Il presente testo è un semplice strumento di documentazione e non produce alcun effetto giuridico. Le istituzioni dell'Unione non assumono alcuna responsabilità per i suoi contenuti. Le versioni facenti fede degli atti pertinenti, compresi i loro preamboli, sono quelle pubblicate nella Gazzetta ufficiale dell'Unione europea e disponibili in EUR-Lex. Tali testi ufficiali sono direttamente accessibili attraverso i link inseriti nel presente documento

►**B** **REGOLAMENTO DI ESECUZIONE (UE) 2016/799 DELLA COMMISSIONE**

del 18 marzo 2016

che applica il regolamento (UE) n. 165/2014 del Parlamento europeo e del Consiglio recante le prescrizioni per la costruzione, il collaudo, il montaggio, il funzionamento e la riparazione dei tachigrafi e dei loro componenti

(Testo rilevante ai fini del SEE)

(GU L 139 del 26.5.2016, pag. 1)

Rettificato da:

►**C1** Rettifica, GU L 146 del 3.6.2016, pag. 31 (2016/799)
►**C2** Rettifica, GU L 27 dell'1.2.2017, pag. 169 (2016/799)

▼B

REGOLAMENTO DI ESECUZIONE (UE) 2016/799 DELLA COMMISSIONE

del 18 marzo 2016

che applica il regolamento (UE) n. 165/2014 del Parlamento europeo e del Consiglio recante le prescrizioni per la costruzione, il collaudo, il montaggio, il funzionamento e la riparazione dei tachigrafi e dei loro componenti

(Testo rilevante ai fini del SEE)

Articolo 1

Oggetto e campo di applicazione

1. Il presente regolamento reca le disposizioni necessarie all'applicazione uniforme dei seguenti aspetti riguardanti i tachigrafi:

a) registrazione della posizione del veicolo in determinati punti nel corso del periodo di lavoro giornaliero del conducente;

b) diagnosi precoce remota di eventuali manomissioni o uso improprio dei tachigrafi intelligenti;

c) interfaccia con i sistemi di trasporto intelligenti;

d) le prescrizioni amministrative e tecniche per le procedure di omologazione dei tachigrafi, compresi i meccanismi di sicurezza.

2. La costruzione, il collaudo, l'installazione, l'ispezione, il funzionamento e la riparazione dei tachigrafi intelligenti e dei loro componenti soddisfano le prescrizioni tecniche di cui all'allegato 1C del presente regolamento.

3. Per quanto riguarda la costruzione, il collaudo, l'installazione, l'ispezione, il funzionamento e la riparazione, i tachigrafi diversi dai tachigrafi intelligenti continuano a soddisfare le prescrizioni dell'allegato 1 o dell'allegato 1B, secondo i casi, del regolamento (CEE) n. 3821/85 del Consiglio ([1]).

4. A norma dell'articolo 10 *quinquies* della direttiva 96/53/CE, il dispositivo di diagnosi precoce remota trasmette anche i dati sul peso forniti da un sistema di pesatura interno di bordo, ai fini della rapida individuazione delle frodi.

Articolo 2

Definizioni

Ai fini del presente regolamento si applicano le definizioni di cui all'articolo 2 del regolamento (UE) n. 165/2014.

Si applicano inoltre le seguenti definizioni:

1) «tachigrafo digitale» o «tachigrafo di prima generazione», un tachigrafo digitale diverso da un tachigrafo intelligente;

2) «dispositivo esterno del GNSS», un dispositivo comprendente il ricevitore GNSS, quando l'unità elettronica di bordo non è un'unità singola, nonché gli altri componenti necessari per proteggere la comunicazione dei dati sulla posizione al resto dell'unità elettronica di bordo;

([1]) Regolamento (CEE) n. 3821/85 del Consiglio, del 20 dicembre 1985, relativo all'apparecchio di controllo nel settore dei trasporti su strada (GU L 370 del 31.12.1985, pag. 8).

▼B

3) «fascicolo informativo», il fascicolo completo, in forma elettronica o cartacea, contenente tutte le informazioni fornite dal fabbricante o dal suo mandatario all'autorità di omologazione ai fini dell'omologazione di un tachigrafo o di un suo componente, compresi i certificati di cui all'articolo 12, paragrafo 3, del regolamento (UE) n. 165/2014, i risultati delle prove di cui all'allegato 1C del presente regolamento, nonché disegni, fotografie e altri documenti pertinenti;

4) «fascicolo di omologazione», il fascicolo informativo, in formato elettronico o cartaceo, più i documenti aggiunti dall'autorità di omologazione al fascicolo informativo nello svolgimento delle proprie funzioni, compresa la scheda di omologazione CE del tachigrafo o di un suo componente aggiunta alla fine della procedura di omologazione;

5) «indice del fascicolo di omologazione», il documento in cui è elencato il contenuto numerato del fascicolo di omologazione, che ne identifica tutte le parti pertinenti. Il formato di tale documento distingue le fasi successive della procedura di omologazione CE, incluse le date delle revisioni e degli aggiornamenti del fascicolo;

6) «dispositivo di diagnosi precoce remota», le dotazioni dell'unità elettronica di bordo utilizzate per svolgere controlli su strada mirati;

7) «tachigrafo intelligente» o «tachigrafo di seconda generazione», un tachigrafo digitale conforme agli articoli 8, 9 e 10 del regolamento (UE) n. 165/2014, nonché all'allegato 1C del presente regolamento;

8) «componente del tachigrafo» o «componente», uno dei seguenti elementi: l'unità elettronica di bordo, il sensore di movimento, la carta tachigrafica, il foglio di registrazione, il dispositivo esterno del GNSS e il dispositivo di diagnosi precoce remota;

9) «autorità di omologazione», l'autorità di uno Stato membro preposta all'omologazione del tachigrafo o dei suoi componenti, alla procedura di autorizzazione, al rilascio e, se del caso, alla revoca delle schede di omologazione, che agisce in qualità di punto di contatto per le autorità di omologazione degli altri Stati membri e che garantisce che i fabbricanti adempiano i loro obblighi relativamente alla conformità alle prescrizioni del presente regolamento.

Articolo 3

Servizi basati sulla localizzazione

1. I fabbricanti garantiscono la compatibilità dei tachigrafi intelligenti con i servizi di posizionamento offerti dai sistemi Galileo e EGNOS (il servizio europeo di copertura per la navigazione geostazionaria).

2. Oltre ai sistemi di cui al paragrafo 1, i fabbricanti possono anche scegliere di assicurare la compatibilità con altri sistemi di navigazione satellitare.

▼B

Articolo 4

Procedura di omologazione di un tachigrafo e dei componenti di un tachigrafo

1. Il fabbricante o il suo mandatario presenta una domanda di omologazione di un tachigrafo o di uno dei suoi componenti o di un gruppo di componenti alle autorità di omologazione designate da ciascuno Stato membro. Tale domanda consiste in un fascicolo informativo contenente le informazioni relative a ciascuno dei componenti interessati, comprese, se del caso, le schede di omologazione di altri componenti necessari per completare il tachigrafo, nonché ogni altro documento pertinente.

2. Uno Stato membro rilascia l'omologazione per i tachigrafi, i componenti o i gruppi di componenti conformi alle prescrizioni amministrative e tecniche di cui all'articolo 1, paragrafo 2 o 3, secondo i casi. In tal caso l'autorità di omologazione rilascia al richiedente una scheda di omologazione conforme al modello di cui all'allegato II del presente regolamento.

3. L'autorità di omologazione può chiedere al fabbricante o al suo mandatario di fornire ulteriori informazioni.

4. Il fabbricante o il suo mandatario mette a disposizione delle autorità di omologazione, nonché degli organismi responsabili del rilascio dei certificati di cui all'articolo 12, paragrafo 3, del regolamento (UE) n. 165/2014, tutti i tachigrafi o i relativi componenti necessari a garantire lo svolgimento soddisfacente della procedura di omologazione.

5. Qualora il fabbricante o il suo mandatario chieda l'omologazione di determinati componenti o gruppi di componenti di un tachigrafo, egli fornisce alle autorità di omologazione gli altri componenti, già omologati, nonché le altre parti necessarie per la costruzione del tachigrafo completo, al fine di consentire loro di effettuare le prove necessarie.

Articolo 5

Modifiche delle omologazioni

1. Il fabbricante o il suo mandatario informa senza indugio le autorità di omologazione che hanno rilasciato l'omologazione iniziale, in merito alle eventuali modifiche del software o dell'hardware del tachigrafo o della natura dei materiali usati per la sua fabbricazione che sono registrati nel fascicolo informativo e presenta una domanda di modifica dell'omologazione.

2. Le autorità di omologazione possono rivedere o estendere un'omologazione esistente oppure rilasciare una nuova omologazione, secondo la natura e le caratteristiche delle modifiche.

Si procede a una «revisione» quando l'autorità di omologazione ritiene che le modifiche del software o dell'hardware del tachigrafo o della natura dei materiali usati per la sua fabbricazione siano di lieve entità. In tali casi, l'autorità di omologazione rilascia i documenti rivisti del fascicolo informativo, precisando la natura delle modifiche apportate e la data della loro approvazione. Una versione aggiornata del fascicolo informativo in una forma consolidata, accompagnata da una descrizione dettagliata delle modifiche apportate, è sufficiente a soddisfare questa prescrizione.

▼B

Si procede a un'«estensione» quando l'autorità di omologazione ritiene che le modifiche del software o dell'hardware del tachigrafo o della natura dei materiali usati per la sua fabbricazione siano sostanziali. In tali casi, l'autorità di omologazione può ritenere necessario che siano effettuate nuove prove e ne informa il fabbricante o il suo mandatario. Se i risultati di tali prove sono soddisfacenti, l'autorità di omologazione rilascia una scheda di omologazione rivista recante un numero che identifica l'estensione rilasciata. La scheda di omologazione riporta il motivo dell'estensione e la data del rilascio.

3. L'indice del fascicolo informativo indica la data dell'ultima estensione o dell'ultima revisione dell'omologazione o la data dell'ultimo consolidamento della versione aggiornata dell'omologazione.

4. Una nuova omologazione è necessaria quando le modifiche richieste del tachigrafo omologato o dei suoi componenti comporterebbero il rilascio di un nuovo certificato di sicurezza o di interoperabilità.

Articolo 6

Entrata in vigore

Il presente regolamento entra in vigore il ventesimo giorno successivo alla pubblicazione nella *Gazzetta ufficiale dell'Unione europea*.

Esso si applica a decorrere dal 2 marzo 2016.

Tuttavia, gli allegati si applicano a decorrere dal 2 marzo 2019, ad eccezione dell'appendice 16 che si applica a decorrere dal 2 marzo 2016.

Il presente regolamento è obbligatorio in tutti i suoi elementi e direttamente applicabile in ciascuno degli Stati membri.

▼B

ALLEGATO IC

Requisiti per la costruzione, il collaudo, il montaggio e il controllo

INTRODUZIONE

1 DEFINIZIONI

2 CARATTERISTICHE GENERALI E FUNZIONI DELL'APPARECCHIO DI CONTROLLO

2.1 Caratteristiche generali

2.2 Funzioni

2.3 Modalità di funzionamento

2.4 Sicurezza

3 REQUISITI DI COSTRUZIONE E FUNZIONAMENTO DELL'APPARECCHIO DI CONTROLLO

3.1 Controllo dell'inserimento e dell'estrazione delle carte

3.2 Misurazione della velocità, della posizione e della distanza

3.2.1 Misurazione della distanza percorsa

3.2.2 Misurazione della velocità

3.2.3 Misurazione della posizione

3.3 Misurazione del tempo

3.4 Controllo delle attività del conducente

3.5 Controllo delle condizioni di guida

3.6 Immissioni da parte del conducente

3.6.1 Immissione del luogo in cui inizia e/o termina il periodo di lavoro giornaliero

3.6.2 Immissione manuale delle attività del conducente e consenso del conducente per l'interfaccia ITS

3.6.3 Immissione di condizioni particolari

3.7 Gestione dei blocchi di un'impresa

3.8 Verifica delle attività di controllo

3.9 Rilevamento di anomalie e/o guasti

3.9.1 Anomalia «Inserimento di una carta non valida»

3.9.2 Anomalia «Conflitto di carte»

3.9.3 Anomalia «Sovrapposizione di orari»

3.9.4 Anomalia «Guida in assenza di una carta adeguata»

3.9.5 Anomalia «Inserimento carta durante la guida»

3.9.6 Anomalia «Chiusura errata ultima sessione carta»

3.9.7 Anomalia «Superamento della velocità»

3.9.8 Anomalia «Interruzione dell'alimentazione di energia»

3.9.9 Anomalia «Errore di comunicazione con il dispositivo di comunicazione remota»

3.9.10 Anomalia «Assenza di informazioni sulla posizione provenienti dal ricevitore GNSS»

▼B

3.9.11	Anomalia «Errore di comunicazione con il dispositivo GNSS esterno»
3.9.12	Anomalia «Errore dati di marcia»
3.9.13	Anomalia «Dati contrastanti sul movimento del veicolo»
3.9.14	Anomalia «Tentata violazione della sicurezza»
3.9.15	Anomalia «Conflitto di orari»
3.9.16	Guasto «Carta»
3.9.17	Guasto «Apparecchio di controllo»
3.10	Prove incorporate e prove automatiche
3.11	Lettura della memoria di dati
3.12	Registrazione e memorizzazione nella memoria di dati
3.12.1	Dati di identificazione dell'apparecchio
3.12.1.1	Dati di identificazione dell'unità elettronica di bordo
3.12.1.2	Dati di identificazione del sensore di movimento
3.12.1.3	Dati di identificazione dei sistemi globali di navigazione satellitare
3.12.2	Chiavi e certificati
3.12.3	Dati relativi all'inserimento e all'estrazione della carta del conducente o dell'officina
3.12.4	Dati relativi all'attività del conducente
3.12.5	Luoghi e posizioni dove iniziano e terminano i periodi di lavoro giornalieri e/o dove il periodo di guida continuo raggiunge le 3 ore
3.12.6	Dati relativi all'odometro
3.12.7	Dati dettagliati relativi alla velocità
3.12.8	Dati relativi alle anomalie
3.12.9	Dati relativi ai guasti
3.12.10	Dati relativi alla taratura
3.12.11	Dati relativi alla regolazione dell'ora
3.12.12	Dati relativi alle attività di controllo
3.12.13	Dati relativi ai blocchi di un'impresa
3.12.14	Dati relativi al trasferimento
3.12.15	Dati relativi a condizioni particolari
3.12.16	Dati della carta tachigrafica
3.13	Lettura delle carte tachigrafiche
3.14	Registrazione e memorizzazione nelle carte tachigrafiche
3.14.1	Registrazione e memorizzazione nelle carte tachigrafiche di prima generazione
3.14.2	Registrazione e memorizzazione nelle carte tachigrafiche di seconda generazione
3.15	Visualizzazione
3.15.1	Visualizzazione predefinita
3.15.2	Visualizzazione degli avvisi

▼B

3.15.3	Accesso guidato da menù
3.15.4	Visualizzazione di altre informazioni
3.16	Stampa
3.17	Avvisi
3.18	Trasferimento di dati a un dispositivo esterno
3.19	Comunicazione remota per controlli su strada mirati
3.20	Trasmissione di dati ad altri dispositivi esterni
3.21	Taratura
3.22	Verifica della taratura su strada
3.23	Regolazione dell'ora
3.24	Caratteristiche prestazionali
3.25	Materiali
3.26	Iscrizioni
4	REQUISITI DI COSTRUZIONE E FUNZIONAMENTO DELLE CARTE TACHIGRAFICHE
4.1	Dati visibili
4.2	Sicurezza
4.3	Norme
4.4	Specifiche ambientali ed elettriche
4.5	Memorizzazione dei dati
4.5.1	File elementari per l'identificazione e la gestione della carta
4.5.2	Identificazione della carta a circuito integrato
4.5.2.1	Identificazione del chip
4.5.2.2	DIR (presente solo nelle carte tachigrafiche di seconda generazione)
4.5.2.3	Informazioni ATR (opzionali, presenti solo nelle carte tachigrafiche di seconda generazione)
4.5.2.4	Informazioni di lunghezza estesa (opzionali, presenti solo nelle carte tachigrafiche di seconda generazione)
4.5.3	Carta del conducente
4.5.3.1	Applicazione del tachigrafo (accessibile alle unità elettroniche di bordo di prima e seconda generazione)
4.5.3.1.1	Identificazione dell'applicazione
4.5.3.1.2	Chiavi e certificati
4.5.3.1.3	Identificazione della carta
4.5.3.1.4	Identificazione del titolare della carta
4.5.3.1.5	Trasferimento dei dati della carta
4.5.3.1.6	Informazioni sulla patente di guida
4.5.3.1.7	Dati relativi alle anomalie
4.5.3.1.8	Dati relativi ai guasti
4.5.3.1.9	Dati relativi all'attività del conducente

▼B

4.5.3.1.10	Dati relativi ai veicoli impiegati
4.5.3.1.11	Luogo in cui inizia e/o termina il periodo di lavoro giornaliero
4.5.3.1.12	Dati relativi alla sessione della carta
4.5.3.1.13	Dati relativi alle attività di controllo
4.5.3.1.14	Dati relativi a condizioni particolari
4.5.3.2	Applicazione del tachigrafo di seconda generazione (non accessibile alle unità elettroniche di bordo di prima generazione)
4.5.3.2.1	Identificazione dell'applicazione
4.5.3.2.2	Chiavi e certificati
4.5.3.2.3	Identificazione della carta
4.5.3.2.4	Identificazione del titolare della carta
4.5.3.2.5	Trasferimento dei dati della carta
4.5.3.2.6	Informazioni sulla patente di guida
4.5.3.2.7	Dati relativi alle anomalie
4.5.3.2.8	Dati relativi ai guasti
4.5.3.2.9	Dati relativi all'attività del conducente
4.5.3.2.10	Dati relativi ai veicoli impiegati
4.5.3.2.11	Luogo e posizione in cui inizia e/o termina il periodo di lavoro giornaliero
4.5.3.2.12	Dati relativi alla sessione della carta
4.5.3.2.13	Dati relativi alle attività di controllo
4.5.3.2.14	Dati relativi a condizioni particolari
4.5.3.2.15	Dati relativi alle unità elettroniche di bordo usate
4.5.3.2.16	Dati relativi al luogo in cui si raggiungono le tre ore di guida ininterrotta
4.5.4	Carta dell'officina
4.5.4.1	Applicazione del tachigrafo (accessibile alle unità elettroniche di bordo di prima e seconda generazione)
4.5.4.1.1	Identificazione dell'applicazione
4.5.4.1.2	Chiavi e certificati
4.5.4.1.3	Identificazione della carta
4.5.4.1.4	Identificazione del titolare della carta
4.5.4.1.5	Trasferimento dei dati della carta
4.5.4.1.6	Dati relativi a taratura e regolazione dell'ora
4.5.4.1.7	Dati relativi ad anomalie e guasti
4.5.4.1.8	Dati relativi all'attività del conducente
4.5.4.1.9	Dati relativi ai veicoli impiegati
4.5.4.1.10	Dati relativi all'inizio e/o al termine del periodo di lavoro giornaliero
4.5.4.1.11	Dati relativi alla sessione della carta
4.5.4.1.12	Dati relativi alle attività di controllo

▼B

4.5.4.1.13	Dati relativi a condizioni particolari
4.5.4.2	Applicazione del tachigrafo di seconda generazione (non accessibile alle unità elettroniche di bordo di prima generazione)
4.5.4.2.1	Identificazione dell'applicazione
4.5.4.2.2	Chiavi e certificati
4.5.4.2.3	Identificazione della carta
4.5.4.2.4	Identificazione del titolare della carta
4.5.4.2.5	Trasferimento dei dati della carta
4.5.4.2.6	Dati relativi a taratura e regolazione dell'ora
4.5.4.2.7	Dati relativi ad anomalie e guasti
4.5.4.2.8	Dati relativi all'attività del conducente
4.5.4.2.9	Dati relativi ai veicoli impiegati
4.5.4.2.10	Dati relativi all'inizio e/o al termine del periodo di lavoro giornaliero
4.5.4.2.11	Dati relativi alla sessione della carta
4.5.4.2.12	Dati relativi alle attività di controllo
4.5.4.2.13	Dati relativi alle unità elettroniche di bordo usate
4.5.4.2.14	Dati relativi al luogo in cui si raggiungono le tre ore di guida ininterrotta
4.5.4.2.15	Dati relativi a condizioni particolari
4.5.5	Carta di controllo
4.5.5.1	Applicazione del tachigrafo (accessibile alle unità elettroniche di bordo di prima e seconda generazione)
4.5.5.1.1	Identificazione dell'applicazione
4.5.5.1.2	Chiavi e certificati
4.5.5.1.3	Identificazione della carta
4.5.5.1.4	Identificazione del titolare della carta
4.5.5.1.5	Dati relativi alle attività di controllo
4.5.5.2	Applicazione del tachigrafo di seconda generazione (non accessibile alle unità elettroniche di bordo di prima generazione)
4.5.5.2.1	Identificazione dell'applicazione
4.5.5.2.2	Chiavi e certificati
4.5.5.2.3	Identificazione della carta
4.5.5.2.4	Identificazione del titolare della carta
4.5.5.2.5	Dati relativi alle attività di controllo
4.5.6	Carta dell'azienda
4.5.6.1	Applicazione del tachigrafo (accessibile alle unità elettroniche di bordo di prima e seconda generazione)
4.5.6.1.1	Identificazione dell'applicazione
4.5.6.1.2	Chiavi e certificati
4.5.6.1.3	Identificazione della carta

▼B

4.5.6.1.4	Identificazione del titolare della carta
4.5.6.1.5	Dati relativi alle attività dell'impresa
4.5.6.2	Applicazione del tachigrafo di seconda generazione (non accessibile alle unità elettroniche di bordo di prima generazione)
4.5.6.2.1	Identificazione dell'applicazione
4.5.6.2.2	Chiavi e certificati
4.5.6.2.3	Identificazione della carta
4.5.6.2.4	Identificazione del titolare della carta
4.5.6.2.5	Dati relativi alle attività dell'impresa
5	MONTAGGIO DELL'APPARECCHIO DI CONTROLLO
5.1	Montaggio
5.2	Targhetta di montaggio
5.3	Sigilli
6	VERIFICHE, CONTROLLI E RIPARAZIONI
6.1	Autorizzazione di installatori, officine e costruttori di veicoli
6.2	Verifica degli strumenti nuovi o riparati
6.3	Controllo in sede di montaggio
6.4	Controlli periodici
6.5	Determinazione degli errori
6.6	Riparazioni
7	RILASCIO DELLA CARTA
8	OMOLOGAZIONE DELL'APPARECCHIO DI CONTROLLO E DELLE CARTE TACHIGRAFICHE
8.1	Prescrizioni generali
8.2	Certificato di sicurezza
8.3	Certificato funzionale
8.4	Certificato di interoperabilità
8.5	Scheda di omologazione
8.6	Procedura eccezionale: primi certificati di interoperabilità per gli apparecchi di controllo e le carte tachigrafiche di 2ª generazione

INTRODUZIONE

Il sistema tachigrafico digitale di prima generazione è in uso dal 1º maggio 2006 e può essere utilizzato fino alla fine del proprio ciclo di vita per il trasporto interno. Per il trasporto internazionale invece, 15 anni dopo l'entrata in vigore del presente regolamento della Commissione, tutti i veicoli devono essere dotati di un tachigrafo intelligente di seconda generazione conforme, introdotto dal presente regolamento.

Il presente allegato reca i requisiti degli apparecchi di controllo e delle carte tachigrafiche di seconda generazione. A decorrere dalla data della sua introduzione, sui veicoli immatricolati per la prima volta si dovranno montare gli apparecchi di controllo di seconda generazione e per essi dovranno essere rilasciate le carte tachigrafiche di seconda generazione.

Al fine di agevolare l'introduzione del sistema tachigrafico di seconda generazione:

▼B

— le carte tachigrafiche di seconda generazione devono essere progettate per poter essere utilizzate anche nelle unità elettroniche di bordo di prima generazione,

— e non sarà richiesta la sostituzione delle carte tachigrafiche di prima generazione in corso di validità alla data di introduzione.

Ciò consentirà ai conducenti di mantenere la propria carta del conducente unica e di utilizzare con essa entrambi i sistemi.

Gli apparecchi di controllo di seconda generazione devono tuttavia essere tarati utilizzando unicamente carte dell'officina di seconda generazione.

Il presente allegato contiene tutti i requisiti relativi all'interoperabilità tra il sistema tachigrafico di prima e quello di seconda generazione.

L'appendice 15 specifica ulteriormente come gestire la coesistenza dei due sistemi.

Elenco delle appendici

App 1: DIZIONARIO DEI DATI

App 2: SPECIFICHE RIGUARDANTI LE CARTE TACHIGRAFICHE

App 3: PITTOGRAMMI

App 4: STAMPE

App 5: DISPOSITIVO DI VISUALIZZAZIONE

App 6: CONNETTORE ANTERIORE PER LA TARATURA E IL TRASFERIMENTO DEI DATI

App 7: PROTOCOLLI DI TRASFERIMENTO DEI DATI

App 8: PROTOCOLLO DI TARATURA

App 9: OMOLOGAZIONE ED ELENCO DELLE PROVE MINIME PRESCRITTE

App 10: REQUISITI DI SICUREZZA

App 11: MECCANISMI COMUNI DI SICUREZZA

App 12: POSIZIONAMENTO BASATO SUL SISTEMA GLOBALE DI NAVIGAZIONE SATELLITARE (GNSS)

App 13: INTERFACCIA ITS

App 14: FUNZIONE DI COMUNICAZIONE REMOTA

App 15: MIGRAZIONE: GESTIONE DELLA COESISTENZA DI DIVERSE GENERAZIONI DI APPARECCHIATURE

App 16: ADATTATORE PER VEICOLI DELLE CATEGORIE M1 E N1

1 DEFINIZIONI

Ai sensi del presente allegato, s'intende per:

a) «attivazione»,

la fase in cui il tachigrafo diventa pienamente operativo e in grado di assolvere tutte le sue funzioni, comprese quelle di sicurezza, tramite l'uso di una carta dell'officina;

b) «autenticazione»,

la funzione di identificazione e verifica dell'identità indicata;

c) «autenticità»,

la caratteristica di un'informazione di provenire da una fonte di cui si può verificare l'identità;

d) «prova incorporata»,

le prove effettuate su richiesta, azionate dall'operatore o da un apparecchio esterno;

▼B

e) «giorno di calendario»,

una giornata che va dalle ore 00:00 alle ore 24:00. Tutti i giorni di calendario si riferiscono all'ora UTC (tempo universale coordinato);

f) «taratura» del tachigrafo intelligente,

l'aggiornamento o la conferma dei parametri del veicolo da conservare nella memoria di dati. Tali parametri comprendono l'identificazione del veicolo (VIN, VRN e Stato membro di immatricolazione) e le caratteristiche del veicolo [w, k, l, dimensioni degli pneumatici, regolazione del limitatore di velocità (se applicabile), ora corrente (UTC), valore corrente dell'odometro]. Durante la taratura di un apparecchio di controllo, anche i tipi e gli identificativi di tutti i sigilli di omologazione pertinenti devono essere registrati nella memoria di dati.

Qualsiasi aggiornamento o conferma esclusivamente dell'ora UTC sono considerati una regolazione dell'ora e non una taratura, purché non siano in contrasto con il requisito 409.

La taratura di un apparecchio di controllo richiede l'impiego di una carta dell'officina;

g) «numero della carta»,

un numero di 16 caratteri alfanumerici che identifica in modo inequivocabile una carta tachigrafica all'interno di uno Stato membro. Il numero della carta comprende un codice di serie (se applicabile), un codice di sostituzione e un codice di rinnovo della stessa.

Una carta è quindi identificata in modo inequivocabile dal codice dello Stato membro di rilascio e dal numero della carta;

h) «codice di serie della carta»,

il 14^{o} carattere alfanumerico del numero della carta inteso a differenziare le diverse carte rilasciate ad un'impresa, un'officina o un'autorità di controllo autorizzate ad ottenere più carte tachigrafiche. L'impresa, l'officina o l'autorità di controllo sono identificate in modo inequivocabile dai primi 13 caratteri del numero della carta;

i) «codice di rinnovo della carta»,

il 16^{o} carattere alfanumerico del numero della carta, che viene aumentato di un'unità ad ogni rinnovo della carta tachigrafica;

j) «codice di sostituzione della carta»,

il 15^{o} carattere alfanumerico del numero della carta, che viene aumentato di un'unità ad ogni sostituzione della carta tachigrafica;

k) «coefficiente caratteristico del veicolo»,

la caratteristica numerica che esprime il valore del segnale di uscita emesso dalla parte del veicolo collegata all'apparecchio di controllo (asse o albero di uscita del cambio) quando il veicolo percorre la distanza di un chilometro in condizioni normali di prova, come definite nel requisito 414. Il coefficiente caratteristico è espresso in impulsi per chilometro (w = … imp/km);

l) «carta dell'azienda»,

una carta tachigrafica rilasciata dalle autorità di uno Stato membro a un'impresa di trasporto stradale che deve usare veicoli muniti di tachigrafo, che identifica l'impresa di trasporto e consente la visualizzazione, il trasferimento e la stampa dei dati archiviati nel tachigrafo che sono stati bloccati da tale impresa di trasporto;

▼B

m) «costante dell'apparecchio di controllo»,

la caratteristica numerica che esprime il valore del segnale di entrata necessario per ottenere l'indicazione e la registrazione della distanza percorsa di 1 chilometro. La costante è espressa in impulsi per chilometro (k = … imp/km);

n) «periodo di guida continuo», calcolato all'interno dell'apparecchio di controllo come [1]:

il periodo di guida continuo è calcolato come la somma corrente dei periodi di guida accumulati da un determinato conducente, a partire dal termine del suo ultimo periodo di DISPONIBILITÀ o di INTERRUZIONE/RIPOSO o NON NOTO [2] di 45 minuti o più [questo periodo può essere ripartito come prescritto dal regolamento (CE) n. 561/2006 del Parlamento europeo e del Consiglio [3]]. I calcoli tengono conto, a seconda della necessità, delle attività precedenti memorizzate sulla carta del conducente. Qualora il conducente non abbia inserito la sua carta, i calcoli si basano sulle registrazioni nella memoria di dati riferite al periodo corrente durante il quale la carta non era inserita e relative alla sede (slot) pertinente;

o) «carta di controllo»,

una carta tachigrafica rilasciata dalle autorità di uno Stato membro a un'autorità di controllo nazionale competente, che identifica l'organismo di controllo e, facoltativamente, l'agente di controllo, e consente l'accesso ai dati archiviati nella memoria di dati, nelle carte del conducente e, facoltativamente, nelle carte dell'officina, per la lettura, la stampa e/o il trasferimento.

Essa dà accesso anche alla funzione di verifica della taratura su strada e ai dati del lettore della comunicazione remota a fini di diagnosi precoce;

p) «periodo cumulato di interruzione», calcolato all'interno dell'apparecchio di controllo come [1]:

il periodo cumulato di interruzione della guida è calcolato come la somma corrente dei periodi di DISPONIBILITÀ o di INTERRUZIONE/RIPOSO o NON NOTI [2] di 15 minuti o più accumulati da un determinato conducente, a partire dal termine del suo ultimo periodo di DISPONIBILITÀ o di INTERRUZIONE/RIPOSO o NON NOTO [2] di 45 minuti o più [questo periodo può essere ripartito come prescritto dal regolamento (CE) n. 561/2006].

I calcoli tengono conto, a seconda della necessità, delle attività precedenti memorizzate sulla carta del conducente. I periodi non noti di durata negativa (inizio del periodo non noto > termine del periodo non noto), dovuti a sovrapposizioni di orari tra due diversi apparecchi di controllo, non sono presi in considerazione.

---

[1] Questo metodo di calcolo del periodo di guida continuo e del periodo cumulato di interruzione consente all'apparecchio di controllo di calcolare gli avvisi relativi al periodo di guida continuo. Esso non pregiudica l'interpretazione giuridica di tali periodi. Ai fini del calcolo del periodo di guida continuo e del periodo cumulato di interruzione si possono utilizzare metodi alternativi per sostituire le presenti definizioni qualora risultino superate a seguito di modifiche di altri atti legislativi pertinenti.

[2] I periodi NON NOTI corrispondono ai periodi durante i quali la carta del conducente non era inserita in un apparecchio di controllo e per i quali non è stata effettuata l'immissione manuale delle attività del conducente.

[3] Regolamento (CE) n. 561/2006 del Parlamento europeo e del Consiglio, del 15 marzo 2006, relativo all'armonizzazione di alcune disposizioni in materia sociale nel settore dei trasporti su strada e che modifica i regolamenti del Consiglio (CEE) n. 3821/85 e (CE) n. 2135/98 e abroga il regolamento (CEE) n. 3820/85 del Consiglio (GU L 102 dell'11.4.2006, pag. 1).

▼B

Qualora il conducente non abbia inserito la sua carta, i calcoli si basano sulle registrazioni nella memoria di dati riferite al periodo corrente durante il quale la carta non era inserita e relative alla sede (slot) pertinente;

q) «memoria di dati»,

un dispositivo elettronico di memorizzazione di dati, incorporato nell'apparecchio di controllo;

r) «firma digitale»,

i dati aggiunti a un blocco di dati o una trasformazione crittografica dello stesso, che consentono al destinatario del blocco di dati di verificarne l'autenticità e l'integrità;

s) «trasferimento»,

la copia, unitamente alla firma digitale, di una parte o di una serie completa di file di dati, registrati nella memoria di dati dell'unità elettronica di bordo (VU) o nella memoria di una carta tachigrafica, a condizione che tale procedura non modifichi o cancelli i dati memorizzati.

I fabbricanti delle unità elettroniche di bordo (tachigrafo intelligente) e i fabbricanti delle apparecchiature destinate al trasferimento di file di dati devono adottare tutti i provvedimenti ragionevoli per garantire che il trasferimento dei dati in questione avvenga in modo da causare ritardi minimi all'attività delle imprese di trasporto o dei conducenti.

Il trasferimento del file relativo alla velocità può non essere necessario per stabilire la conformità al regolamento (CE) n. 561/2006, ma può essere usato per altri scopi, ad esempio per accertare le cause di un incidente;

t) «carta del conducente»,

una carta tachigrafica rilasciata dalle autorità di uno Stato membro a un determinato conducente, che lo identifica e consente l'archiviazione dei dati sulla sua attività;

u) «circonferenza effettiva delle ruote»,

la media delle distanze percorse da ciascuna delle ruote che imprimono il movimento al veicolo (ruote motrici) durante una rotazione completa. La misurazione di queste distanze deve essere effettuata in condizioni normali di prova, come definite nel requisito 414, ed è espressa come: «l = … mm». I costruttori di veicoli possono sostituire la misurazione di queste distanze con un calcolo teorico che tenga conto della ripartizione del peso sugli assi, con veicolo a vuoto in normali condizioni di marcia ([1]). I metodi di tale calcolo teorico devono essere approvati da un'autorità competente degli Stati membri e tale approvazione può avvenire solo prima dell'attivazione del tachigrafo;

v) «anomalia»,

un'operazione anomala rilevata dal tachigrafo intelligente, potenzialmente risultante da un tentativo di frode;

w) «dispositivo GNSS esterno»,

un dispositivo comprendente il ricevitore GNSS, quando l'unità elettronica di bordo non è un'unità singola, nonché gli altri componenti necessari per proteggere la comunicazione dei dati sulla posizione al resto delle unità elettroniche di bordo;

([1]) Regolamento (UE) n. 1230/2012 della Commissione, del 12 dicembre 2012, che attua il regolamento (CE) n. 661/2009 del Parlamento europeo e del Consiglio per quanto riguarda i requisiti di omologazione per le masse e le dimensioni dei veicoli a motore e dei loro rimorchi e che modifica la direttiva 2007/46/CE del Parlamento europeo e del Consiglio (GU L 353 del 21.12.2012, pag. 31), come modificata da ultimo.

▼B

x) «guasto»,

un'operazione anomala rilevata dal tachigrafo intelligente, che può essere dovuta al cattivo funzionamento o al guasto di un apparecchio;

y) «ricevitore GNSS»,

un dispositivo elettronico che riceve ed elabora digitalmente i segnali di uno o più sistemi globali di navigazione satellitare (in inglese GNSS) per fornire informazioni sulla posizione, la velocità e l'ora;

z) «montaggio»,

il montaggio di un tachigrafo su un veicolo;

aa) «interoperabilità»,

la capacità dei sistemi e dei processi industriali e commerciali sottostanti di scambiare dati e di condividere informazioni;

bb) «interfaccia»,

strumento posto tra sistemi, che fornisce i mezzi attraverso i quali detti sistemi possono collegarsi e interagire;

cc) «posizione»,

coordinate geografiche del veicolo in un dato momento;

dd) «sensore di movimento»,

una parte del tachigrafo che fornisce un segnale rappresentativo della velocità del veicolo e/o della distanza percorsa;

ee) «carta non valida»,

una carta individuata come difettosa oppure la cui autenticazione iniziale è stata respinta o la cui data di inizio di validità non è ancora stata raggiunta o la cui data di scadenza è stata superata;

ff) «standard aperto»,

uno standard definito in un documento contenente le relative specifiche disponibile gratuitamente o a un prezzo simbolico, che può essere copiato, divulgato o usato a titolo gratuito o previo pagamento di un importo simbolico;

gg) «escluso dal campo di applicazione»,

la circostanza in cui non è prescritto l'uso dell'apparecchio di controllo, secondo le disposizioni del regolamento (CE) n. 561/2006;

hh) «superamento della velocità»,

il superamento della velocità autorizzata del veicolo, definito come ogni periodo di durata superiore a 60 secondi durante il quale la velocità misurata del veicolo supera il limite del valore di regolazione del limitatore di velocità stabilito dalla direttiva 92/6/CEE del Consiglio ([1]), come modificata da ultimo;

ii) «controllo periodico»,

un insieme di operazioni effettuate per verificare il corretto funzionamento del tachigrafo, la corrispondenza tra le impostazioni e i parametri del veicolo e l'assenza di un eventuale collegamento del tachigrafo a dispositivi di manipolazione;

([1]) Direttiva 92/6/CEE del Consiglio, del 10 febbraio 1992, concernente il montaggio e l'impiego di limitatori di velocità per talune categorie di autoveicoli nella Comunità (GU L 57 del 2.3.1992, pag. 27).

▼B

jj) «stampante»,

un componente dell'apparecchio di controllo che stampa i dati memorizzati;

kk) «comunicazione remota a fini di diagnosi precoce»,

la comunicazione tra il dispositivo di comunicazione remota a fini di diagnosi precoce e il lettore della comunicazione remota a fini di diagnosi precoce durante i controlli su strada mirati al fine di individuare a distanza eventuali manomissioni o usi impropri dell'apparecchio di controllo;

ll) «dispositivo di comunicazione remota»,

le dotazioni dell'unità elettronica di bordo utilizzate per svolgere controlli su strada mirati;

mm) «lettore della comunicazione remota a fini di diagnosi precoce»,

il sistema utilizzato per i controlli su strada mirati dagli agenti preposti;

nn) «rinnovo»,

il rilascio di una nuova carta tachigrafica quando una carta esistente raggiunge il termine del suo periodo di validità o non funziona correttamente e viene restituita alle autorità di rilascio. Il rinnovo implica sempre la certezza che due carte valide non coesistano;

oo) «riparazione»,

qualunque riparazione di un sensore di movimento, di un'unità elettronica di bordo o di un cavo che comporti l'interruzione dell'alimentazione di energia o del suo collegamento ad altri componenti del tachigrafo o l'apertura del sensore di movimento o dell'unità elettronica di bordo;

pp) «sostituzione della carta»,

il rilascio di una carta tachigrafica in sostituzione di una carta esistente, dichiarata smarrita, rubata o non funzionante, che non viene restituita alle autorità di rilascio. La sostituzione implica sempre il rischio che possano coesistere due carte valide;

qq) «certificazione della sicurezza»,

la procedura, condotta da un organismo di certificazione di criteri comuni, volta a certificare che l'apparecchio di controllo (o un suo componente) o la carta tachigrafica in esame soddisfano i requisiti di sicurezza definiti nei rispettivi profili di protezione;

rr) «prova automatica»,

le prove cicliche ed automatiche effettuate dall'apparecchio di controllo per rilevare eventuali guasti;

ss) «misurazione del tempo»,

una registrazione digitale permanente del tempo (data e ora) universale coordinato (UTC);

tt) «regolazione dell'ora»,

una regolazione automatica dell'ora ad intervalli regolari ed entro un margine di tolleranza massimo di un minuto o una regolazione effettuata durante la taratura;

uu) «dimensioni degli pneumatici»,

l'indicazione delle dimensioni degli pneumatici (ruote motrici esterne), in conformità alla direttiva 92/23/CEE, del Consiglio ([1]), come modificata da ultimo;

([1]) Direttiva 92/23/CEE del Consiglio, del 31 marzo 1992, relativa ai pneumatici dei veicoli a motore e dei loro rimorchi nonché al loro montaggio (GU L 129 del 14.5.1992, pag. 95).

▼B

vv) «identificazione del veicolo»,

i numeri che identificano il veicolo: il numero di immatricolazione del veicolo (VRN), con indicazione dello Stato membro di immatricolazione, e il numero di identificazione del veicolo (VIN) ([1]);

ww) «settimana», ai fini dei calcoli interni dell'apparecchio di controllo,

il periodo compreso tra le ore 00:00 UTC del lunedì e le ore 24:00 UTC della domenica;

xx) «carta dell'officina»,

una carta tachigrafica rilasciata dalle autorità di uno Stato membro al personale designato di un produttore di tachigrafi, un installatore, un costruttore di veicoli o un'officina approvati da tale Stato membro, che identifica il titolare della carta e consente il collaudo, la taratura e l'attivazione dei tachigrafi e/o il trasferimento di dati dai medesimi;

yy) «adattatore»,

un dispositivo, che fornisce un segnale costantemente rappresentativo della velocità del veicolo e/o della distanza percorsa, diverso da quello utilizzato per il rilevamento del movimento indipendente, e che:

— è montato e utilizzato soltanto sui veicoli delle categorie M1 e N1 (quali definiti nell'allegato II della direttiva 2007/46/CE del Parlamento europeo e del Consiglio ([2]), come modificata da ultimo) messi in circolazione dal 1° maggio 2006,

— è montato nei casi in cui non è meccanicamente possibile montare alcun altro tipo di sensore di movimento esistente altrimenti conforme alle disposizioni del presente allegato e delle appendici da 1 a 15 dello stesso,

— è montato tra l'unità elettronica di bordo e il punto in cui gli impulsi relativi alla velocità/distanza sono generati da sensori integrati o interfacce alternative,

— visto dall'unità elettronica di bordo, l'adattatore funziona come se un sensore di movimento, conforme alle disposizioni del presente allegato e delle appendici da 1 a 16 dello stesso, fosse collegato all'unità elettronica di bordo.

L'uso dell'adattatore nei veicoli sopra descritti deve consentire il montaggio e il corretto utilizzo di un'unità elettronica di bordo conforme a tutti i requisiti del presente allegato.

Per tali veicoli il tachigrafo intelligente comprende i cavi, l'adattatore e l'unità elettronica di bordo;

([1]) Direttiva 76/114/CEE del Consiglio, del 18 dicembre 1975, per il ravvicinamento delle legislazioni degli Stati membri relative alle targhette ed alle iscrizioni regolamentari nonché alla loro posizione e modo di fissaggio per i veicoli a motore e i loro rimorchi (GU L 24 del 30.1.1976, pag. 1).

([2]) Direttiva 2007/46/CE del Parlamento europeo e del Consiglio, del 5 settembre 2007, che istituisce un quadro per l'omologazione dei veicoli a motore e dei loro rimorchi, nonché dei sistemi, componenti ed entità tecniche destinati a tali veicoli («direttiva quadro») (GU L 263 del 9.10.2007, pag. 1).

▼B

zz) «integrità dei dati»,

l'accuratezza e la coerenza dei dati memorizzati, indicata dall'assenza di qualsiasi cambiamento dei dati tra due aggiornamenti di un registro di dati. L'integrità implica che i dati siano una copia conforme della versione originale, ad esempio che non siano stati danneggiati durante la scrittura su una carta tachigrafica o un dispositivo apposito e la lettura da essi o durante la trasmissione tramite qualsiasi canale di comunicazione;

aaa) «riservatezza dei dati»,

l'insieme delle misure tecniche adottate per garantire la corretta attuazione dei principi enunciati nella direttiva 95/46/CE, del Parlamento europeo e del Consiglio ([1]), come pure di quelli previsti nella direttiva 2002/58/CE del Parlamento europeo e del Consiglio ([2]);

bbb) «sistema tachigrafico intelligente»,

l'apparecchio di controllo, le carte tachigrafiche e l'insieme di tutte le apparecchiature che interagiscono direttamente o indirettamente durante la loro costruzione, installazione, uso, collaudo e controllo, come le carte, il lettore della comunicazione remota e qualsiasi altro dispositivo per il trasferimento dei dati, l'analisi dei dati, la taratura, la creazione, la gestione o l'introduzione di elementi di sicurezza, ecc.;

ccc) «data di introduzione»,

36 mesi dopo l'entrata in vigore delle disposizioni dettagliate di cui all'articolo 11 del regolamento (UE) n. 165/2014 del Parlamento europeo e del Consiglio ([3]).

È questa la data a partire dalla quale i veicoli immatricolati per la prima volta:

— *devono essere dotati di un tachigrafo collegato a un servizio di posizionamento basato su un sistema di navigazione satellitare,*

— *devono essere in grado di comunicare i dati per i controlli su strada mirati alle autorità di controllo competenti, mentre il veicolo è in movimento,*

— *e possono essere muniti di interfacce standardizzate che consentono di usare i dati registrati o generati dal tachigrafo digitale nel modo funzionamento, mediante un dispositivo esterno;*

ddd) «profilo di protezione»,

un documento, utilizzato come parte del processo di certificazione secondo criteri comuni, che fornisce le specifiche indipendenti dall'attuazione dei requisiti di sicurezza per la garanzia di sicurezza delle informazioni;

([1]) Direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (GU L 281 del 23.11.1995, pag. 31).

([2]) Direttiva 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche) (GU L 201 del 31.7.2002, pag. 37).

([3]) Regolamento (UE) n. 165/2014 del Parlamento europeo e del Consiglio, del 4 febbraio 2014, relativo ai tachigrafi nel settore dei trasporti su strada, che abroga il regolamento (CEE) n. 3821/85 del Consiglio relativo all'apparecchio di controllo nel settore dei trasporti su strada e modifica il regolamento (CE) n. 561/2006 del Parlamento europeo e del Consiglio relativo all'armonizzazione di alcune disposizioni in materia sociale nel settore dei trasporti su strada (GU L 60 del 28.2.2014, pag. 1).

▼B

eee) «accuratezza del GNSS»,

nel contesto della registrazione della posizione dal sistema globale di navigazione satellitare (GNSS) con i tachigrafi, il valore dell'HDOP (*Horizontal Dilution of Precision*), calcolato come il valore HDOP minimo tra quelli raccolti sui sistemi GNSS disponibili.

2 CARATTERISTICHE GENERALI E FUNZIONI DELL'APPARECCHIO DI CONTROLLO

2.1 **Caratteristiche generali**

L'apparecchio di controllo ha la finalità di registrare, memorizzare, visualizzare, stampare e trasmettere dati relativi alle attività del conducente.

I veicoli su cui è montato un apparecchio di controllo conforme alle disposizioni del presente allegato devono essere muniti di un indicatore di velocità e di un odometro. Tali funzioni possono essere incorporate nell'apparecchio di controllo.

1) L'apparecchio di controllo comprende i cavi, un sensore di movimento e un'unità elettronica di bordo.

2) L'interfaccia tra i sensori di movimento e le unità elettroniche di bordo deve soddisfare le prescrizioni specificate nell'appendice 11.

3) L'unità elettronica di bordo deve essere collegata a uno o più sistemi globali di navigazione satellitare, come specificato nell'appendice 12.

4) L'unità elettronica di bordo deve comunicare con i lettori della comunicazione remota a fini di diagnosi precoce, come specificato nell'appendice 14.

5) L'unità elettronica di bordo può comprendere un'interfaccia ITS, specificata nell'appendice 13.

L'apparecchio di controllo può essere collegato ad altri dispositivi attraverso interfacce supplementari e/o l'interfaccia ITS opzionale.

6) L'eventuale presenza nell'apparecchio di controllo di altre funzioni o altri dispositivi, omologati o meno, o il loro collegamento ad esso non deve interferire direttamente o indirettamente con il funzionamento corretto e sicuro dell'apparecchio di controllo e con le disposizioni del presente regolamento.

Gli utilizzatori dell'apparecchio di controllo sono identificati dall'apparecchio per mezzo di carte tachigrafiche.

7) L'apparecchio di controllo fornisce diritti di accesso selettivi ai dati e alle funzioni, a seconda del tipo e/o dell'identità dell'utilizzatore.

L'apparecchio di controllo registra e memorizza dati nella sua memoria di dati, nel dispositivo di comunicazione remota e sulle carte tachigrafiche.

Queste operazioni sono effettuate in conformità alla direttiva 95/46/CE, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati [1], alla direttiva 2002/58/CE, del 12 luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche [2] e all'articolo 7 del regolamento (UE) n. 165/2014.

[1] GU L 281 del 23.11.1995, pag. 31.
[2] GU L 201 del 31.7.2002, pag. 37.

▼B

2.2 **Funzioni**

8) L'apparecchio di controllo deve garantire le seguenti funzioni:

— controllo dell'inserimento e dell'estrazione delle carte,

— misurazione della velocità, della distanza e della posizione,

— misurazione del tempo,

— controllo delle attività del conducente,

— controllo delle condizioni di guida,

— immissioni manuali da parte del conducente:

— luogo in cui inizia e/o termina il periodo di lavoro giornaliero,

— attività del conducente,

— condizioni particolari,

— gestione dei blocchi di un'impresa,

— verifica delle attività di controllo,

— rilevamento di anomalie e/o guasti,

— prove incorporate e prove automatiche,

— lettura della memoria di dati,

— registrazione e memorizzazione nella memoria di dati,

— lettura delle carte tachigrafiche,

— registrazione e memorizzazione nelle carte tachigrafiche,

— visualizzazione,

— stampa,

— avvisi,

— trasferimento di dati su dispositivi esterni,

— comunicazione remota per controlli su strada mirati,

— trasmissione di dati a dispositivi aggiuntivi,

— taratura,

— verifica su strada della taratura,

— regolazione dell'ora.

2.3 **Modalità di funzionamento**

9) L'apparecchio di controllo deve prevedere quattro modalità di funzionamento:

— modo funzionamento,

— modo controllo,

— modo taratura,

— modo azienda.

10) L'apparecchio di controllo deve passare alla modalità di funzionamento sotto riportata, a seconda delle carte tachigrafiche in corso di validità inserite nelle interfacce. Al fine di determinare la modalità di funzionamento, la generazione della carta tachigrafica è irrilevante, purché la carta inserita sia valida. Una carta dell'officina di prima generazione deve essere sempre considerata non valida quando è inserita in un'unità elettronica di bordo di seconda generazione.

▼B

Modalità di funzionamento		Sede (slot) del conducente				
		Carta assente	Carta del conducente	Carta di controllo	Carta dell'officina	Carta dell'azienda
Sede (slot) del secondo conducente	Carta assente	Funzionamento	Funzionamento	Controllo	Taratura	Azienda
	Carta del conducente	Funzionamento	Funzionamento	Controllo	Taratura	Azienda
	Carta di controllo	Controllo	Controllo	Controllo (*)	Funzionamento	Funzionamento
	Carta dell'officina	Taratura	Taratura	Funzionamento	Taratura (*)	Funzionamento
	Carta dell'azienda	Azienda	Azienda	Funzionamento	Funzionamento	Azienda (*)

(*) In questi casi l'apparecchio di controllo deve usare solo la carta tachigrafica inserita nella sede (slot) del conducente.

11) L'apparecchio di controllo deve ignorare le carte non valide inserite, fatta salva la possibilità di visualizzare, stampare o trasferire i dati memorizzati su una carta scaduta.

12) Tutte le funzioni elencate al punto 2.2 devono essere disponibili in ogni modalità di funzionamento, con le seguenti eccezioni:

— la funzione di taratura è accessibile solo nel modo taratura,

— la funzione di verifica della taratura su strada è accessibile solo nel modo controllo,

— la funzione di gestione dei blocchi di un'impresa è disponibile solo nel modo azienda,

— la verifica delle attività di controllo è disponibile solo nel modo controllo,

— la funzione di trasferimento dati non è disponibile nel modo funzionamento (fatto salvo quanto disposto nel requisito 193), fatta eccezione per il trasferimento dei dati di una carta del conducente quando nessun'altra carta è inserita nell'unità elettronica di bordo.

13) L'apparecchio di controllo può trasmettere qualsiasi dato al dispositivo di visualizzazione, alla stampante o a interfacce esterne, con le seguenti eccezioni:

— nel modo funzionamento, deve essere omessa ogni identificazione personale (cognome e nome/i) non corrispondente a una carta tachigrafica inserita e va parzialmente omesso (un carattere sì e uno no, da sinistra a destra) ogni numero di carta non corrispondente a una carta tachigrafica inserita,

— nel modo azienda, i dati relativi al conducente (requisiti 102, 105 e 108) possono essere estratti soltanto per i periodi per cui non esista un blocco o nessun'altra azienda (identificata dai primi 13 caratteri del numero della carta dell'azienda) ne abbia attivato uno,

— se nell'apparecchio di controllo non è inserita una carta, si possono trasmettere solo i dati relativi al conducente riferiti al giorno corrente e agli 8 giorni di calendario precedenti,

— i dati personali provenienti dall'unità elettronica di bordo non devono essere trasmessi tramite l'interfaccia ITS dell'unità elettronica di bordo, salvo previa verifica che il conducente cui i dati si riferiscono abbia dato il proprio consenso,

▼B

— le unità elettroniche di bordo hanno un periodo di validità in condizioni di funzionamento normali di 15 anni, che inizia con la data del rilascio dei relativi certificati, ma possono essere utilizzate per ulteriori 3 mesi, solo per il trasferimento dei dati.

2.4 **Sicurezza**

La sicurezza del sistema è intesa a proteggere la memoria di dati in modo da impedire l'accesso non autorizzato, la manipolazione dei dati e rilevarne eventuali tentativi, nonché da proteggere l'integrità e l'autenticità dei dati scambiati tra sensore di movimento e unità elettronica di bordo, l'integrità e l'autenticità dei dati scambiati tra l'apparecchio di controllo e le carte tachigrafiche, l'integrità e l'autenticità dei dati scambiati tra l'apparecchio di controllo e il dispositivo GNSS esterno, la riservatezza, l'integrità e l'autenticità dei dati scambiati per finalità di controllo tramite la comunicazione remota a fini di diagnosi precoce e da verificare l'integrità e l'autenticità dei dati trasferiti.

14) Al fine di garantire la sicurezza del sistema, i seguenti componenti devono soddisfare i requisiti di sicurezza specificati nei rispettivi profili di protezione, come richiesto nell'appendice 10:

— unità elettronica di bordo,

— carta tachigrafica,

— sensore di movimento,

— dispositivo GNSS esterno (questo profilo è necessario e applicabile solo per la variante esterna del GNSS).

3 REQUISITI DI COSTRUZIONE E FUNZIONAMENTO DELL'APPARECCHIO DI CONTROLLO

3.1 **Controllo dell'inserimento e dell'estrazione delle carte**

15) L'apparecchio di controllo deve rilevare ogni inserimento ed estrazione di carte nelle relative interfacce.

16) All'atto dell'inserimento, l'apparecchio di controllo deve verificare se la carta inserita è una carta tachigrafica in corso di validità ed in tal caso identificarne il tipo e la generazione.

Se una carta con lo stesso numero e un codice di rinnovo maggiore è già stata inserita nell'apparecchio di controllo, la carta è dichiarata non valida.

Se una carta con lo stesso numero e lo stesso codice di rinnovo, ma con un codice di sostituzione maggiore è già stata inserita nell'apparecchio di controllo, la carta è dichiarata non valida.

17) Le carte tachigrafiche di prima generazione devono essere considerate non valide dall'apparecchio di controllo dopo che la possibilità di utilizzare carte tachigrafiche di prima generazione è stata preclusa da un'officina, in conformità all'appendice 15 (req. MIG003).

18) Le carte dell'officina di prima generazione inserite nell'apparecchio di controllo di seconda generazione devono essere considerate non valide.

▼B

19) L'apparecchio di controllo deve essere realizzato in modo tale che le carte tachigrafiche vengano bloccate in posizione quando sono inserite correttamente nelle relative interfacce.

20) Le carte tachigrafiche devono poter essere estratte solo a veicolo fermo e dopo la memorizzazione dei dati pertinenti nelle carte stesse. L'estrazione della carta deve richiedere l'intervento fisico dell'utilizzatore.

3.2 **Misurazione della velocità, della posizione e della distanza**

21) Il sensore di movimento (eventualmente incorporato nell'adattatore) è la principale fonte di misurazione della velocità e della distanza.

22) Questa funzione deve misurare costantemente ed essere in grado di fornire il valore dell'odometro corrispondente alla distanza totale percorsa dal veicolo utilizzando gli impulsi provenienti dal sensore di movimento.

23) Questa funzione deve misurare costantemente ed essere in grado di fornire la velocità del veicolo utilizzando gli impulsi provenienti dal sensore di movimento.

24) La funzione di misurazione della velocità deve inoltre segnalare se il veicolo è in marcia o fermo. Il veicolo va considerato in marcia non appena la funzione rileva più di 1 imp/sec per almeno 5 secondi sul sensore di movimento, in caso contrario il veicolo si considera fermo.

25) I dispositivi che visualizzano la velocità (tachimetro) e la distanza totale percorsa (odometro), montati su ogni veicolo munito di un apparecchio di controllo conforme alle prescrizioni del presente regolamento, devono soddisfare i requisiti relativi alle tolleranze massime fissati nel presente allegato (cfr. punti 3.2.1 e 3.2.2).

26) Al fine di individuare una manipolazione dei dati di movimento, le informazioni provenienti dal sensore di movimento devono essere confermate dalle informazioni sul movimento del veicolo provenienti dal ricevitore GNSS e facoltativamente da altre fonti indipendenti dal sensore di movimento.

27) Questa funzione deve misurare la posizione del veicolo al fine di consentire la registrazione automatica:

— delle posizioni dove il conducente e/o il secondo conducente iniziano il loro periodo di lavoro giornaliero;

— delle posizioni dove il periodo di guida continuo del conducente raggiunge un multiplo di tre ore;

— delle posizioni dove il conducente e/o il secondo conducente terminano il loro periodo di lavoro giornaliero.

3.2.1 *Misurazione della distanza percorsa*

28) La distanza percorsa può essere misurata:

— a marcia avanti e a marcia indietro oppure

— unicamente a marcia avanti.

29) L'apparecchio di controllo deve misurare la distanza da 0 a 9 999 999,9 km.

▼B

30) La distanza misurata deve rispettare le tolleranze seguenti (distanze di almeno 1 000 m):

— ± 1 % prima del montaggio,

— ± 2 % all'atto del montaggio e del controllo periodico,

— ± 4 % durante l'impiego.

31) La distanza misurata deve avere una risoluzione maggiore o uguale a 0,1 km.

3.2.2 *Misurazione della velocità*

32) L'apparecchio di controllo deve misurare la velocità tra 0 e 220 km/h.

33) Per garantire una tolleranza massima sulla velocità visualizzata di ± 6 km/h durante l'impiego, tenuto conto di:

— una tolleranza di ± 2 km/h per le variazioni in ingresso (variazioni degli pneumatici, …),

— una tolleranza di ± 1 km/h per le misurazioni effettuate durante il montaggio o i controlli periodici,

l'apparecchio di controllo deve misurare la velocità, per velocità comprese tra 20 e 180 km/h e per coefficienti caratteristici del veicolo compresi tra 4 000 e 25 000 imp/km, con una tolleranza di ± 1 km/h (a velocità costante).

Nota: la risoluzione della memorizzazione dei dati apporta una tolleranza supplementare di ± 0,5 km/h alla velocità memorizzata dall'apparecchio di controllo.

34) La velocità deve essere misurata correttamente, rispettando le tolleranze normali, entro 2 secondi dalla fine di una variazione di velocità, quando il tasso di variazione di velocità è inferiore o uguale a $2 m/s^2$.

35) La misurazione della velocità deve avere una risoluzione pari a 1 km/h o migliore.

3.2.3 *Misurazione della posizione*

36) L'apparecchio di controllo deve misurare la posizione assoluta del veicolo utilizzando il ricevitore GNSS.

37) La posizione assoluta è misurata in coordinate geografiche di latitudine e longitudine in gradi e minuti con una risoluzione di 1/10 di minuto.

3.3 **Misurazione del tempo**

38) La funzione di misurazione del tempo deve misurare costantemente ed indicare data e ora UTC in formato digitale.

39) La data e l'ora UTC vanno usate per datare tutti i dati dell'apparecchio di controllo (registrazioni, scambio di dati) e per tutti i documenti stampati di cui all'appendice 4 «Documenti stampati».

40) Al fine di visualizzare l'ora locale, deve poter essere possibile regolare l'ora visualizzata in intervalli di mezz'ora. Non devono essere possibili regolazioni diverse dai multipli positivi o negativi della mezz'ora.

41) Lo sfasamento dell'ora non deve superare ± 2 secondi al giorno in condizioni di omologazione, in assenza di regolazioni dell'ora.

▼B

42) L'ora misurata deve avere una risoluzione pari a 1 secondo o migliore.

43) La misurazione dell'ora non deve essere compromessa da un'interruzione dell'alimentazione esterna inferiore a 12 mesi in condizioni di omologazione.

3.4 **Controllo delle attività del conducente**

44) Questa funzione deve controllare costantemente e separatamente le attività di un conducente e di un secondo conducente.

45) Le attività del conducente sono GUIDA, LAVORO, DISPONIBILITÀ e INTERRUZIONE/RIPOSO.

46) Il conducente e/o il secondo conducente devono poter selezionare manualmente LAVORO, DISPONIBILITÀ o INTERRUZIONE/RIPOSO.

47) Quando il veicolo è in marcia, devono essere automaticamente selezionati GUIDA per il conducente e DISPONIBILITÀ per il secondo conducente.

48) Quando il veicolo si arresta, deve essere automaticamente selezionato LAVORO per il conducente.

49) Il primo passaggio di attività a RIPOSO o DISPONIBILITÀ che si verifica entro 120 secondi dalla selezione automatica di LAVORO dovuta all'arresto del veicolo va considerato avvenuto al momento dell'arresto del veicolo (annullando eventualmente il passaggio a LAVORO).

50) Questa funzione deve trasmettere i cambi di attività alle funzioni di registrazione con una risoluzione di un minuto.

51) Dato un intervallo di un minuto, se GUIDA è registrata come attività del minuto immediatamente precedente e del minuto immediatamente successivo, l'intero minuto va considerato come GUIDA.

52) Dato un intervallo di un minuto non considerato come GUIDA in base al requisito 051, l'intero minuto va considerato come attività dello stesso tipo di quella continua di maggiore durata verificatasi entro tale minuto (o, nel caso di più attività di pari durata, dell'ultima di esse).

53) Questa funzione deve controllare inoltre costantemente il periodo di guida continuo e il periodo cumulato di interruzione del conducente.

3.5 **Controllo delle condizioni di guida**

54) Questa funzione deve controllare costantemente ed automaticamente le condizioni di guida.

55) La condizione di guida EQUIPAGGIO deve essere selezionata quando nell'apparecchio sono inserite due carte del conducente in corso di validità; in ogni altro caso deve essere selezionata la condizione di guida SINGOLA.

3.6 **Immissioni da parte del conducente**

3.6.1 *Immissione del luogo in cui inizia e/o termina il periodo di lavoro giornaliero*

56) Questa funzione deve consentire l'immissione del luogo in cui, secondo il conducente e/o il secondo conducente, il suo periodo di lavoro giornaliero inizia e/o termina.

▼B

57) Per luogo s'intende lo Stato e inoltre, se del caso, la regione, che sono immessi o confermati manualmente.

58) All'atto dell'estrazione di una carta del conducente, l'apparecchio di controllo deve invitare il conducente (o il secondo conducente) ad immettere il «luogo in cui termina il periodo di lavoro giornaliero».

59) Il conducente deve quindi immettere il luogo in cui si trova il veicolo in quel momento, che è considerato come un dato temporaneo.

60) I luoghi in cui iniziano e/o terminano i periodi di lavoro giornalieri devono poter essere immessi mediante comandi dei menù. Se durante un intervallo di un minuto viene immesso più di uno di tali dati, va conservata esclusivamente la registrazione dell'ultima immissione di inizio e dell'ultima immissione di fine effettuata in tale intervallo.

3.6.2 *Immissione manuale delle attività del conducente e consenso del conducente per l'interfaccia ITS*

61) All'atto dell'inserimento della carta del conducente (o dell'officina), ed esclusivamente in tale momento, l'apparecchio di controllo deve consentire l'immissione manuale di attività. L'immissione manuale di attività deve essere effettuata utilizzando i valori dell'ora locale e della data del fuso orario (regolazione UTC) impostato in quel momento per l'unità elettronica di bordo.

Al momento di inserire una carta del conducente o dell'officina, il titolare della carta deve veder comparire le seguenti informazioni:

— la data e l'ora dell'ultima estrazione della carta;

— facoltativamente: la regolazione dell'ora locale impostata per l'unità elettronica di bordo.

All'atto del primo inserimento di una carta del conducente o dell'officina sconosciuta all'unità elettronica di bordo, il titolare della carta deve essere invitato a dare il proprio consenso alla trasmissione di dati personali connessi al tachigrafo tramite l'interfaccia ITS opzionale.

In qualsiasi momento il consenso del conducente (o dell'officina) può essere abilitato o disabilitato mediante comandi del menù, purché la carta del conducente (dell'officina) sia inserita.

L'immissione di attività deve essere possibile, ma con le seguenti restrizioni:

— i tipi di attività devono essere: LAVORO, DISPONIBILITÀ e INTERRUZIONE/RIPOSO;

— le ore di inizio e di fine per ciascuna attività devono rientrare esclusivamente nel periodo compreso tra l'ultima estrazione della carta e l'inserimento della carta in corso;

— non deve essere consentita la sovrapposizione reciproca nel tempo delle attività.

L'immissione manuale deve essere possibile, se richiesta, all'atto del primo inserimento di una carta del conducente (o dell'officina) precedentemente inutilizzata.

▼B

La procedura di immissione manuale dei dati sulle attività deve comprendere tutte le fasi consecutive necessarie per inserire, per ciascuna attività, il tipo, l'ora di inizio e l'ora di fine. Per ogni parte del periodo compreso tra l'ultima estrazione della carta e l'inserimento della carta in corso, il titolare della carta deve avere la possibilità di non dichiarare alcuna attività.

Nel corso dell'immissione manuale di attività correlate all'inserimento della carta, il titolare della carta, se del caso, deve avere la possibilità di indicare:

— il luogo in cui si è concluso il precedente periodo giornaliero di lavoro associato all'ora corrispondente (che va a sostituire il dato inserito al momento dell'ultima estrazione della carta);

— il luogo in cui ha inizio il periodo giornaliero di lavoro in corso associato all'ora corrispondente.

Se il titolare della carta non immette alcun luogo di inizio o fine del periodo di lavoro, durante le immissioni manuali associate all'inserimento della carta ciò è da considerarsi una dichiarazione del fatto che il suo periodo di lavoro non è cambiato dall'ultima estrazione della carta. La successiva immissione di un luogo in cui termina un periodo di lavoro giornaliero precedente va allora a sovrascrivere il dato temporaneo immesso al momento dell'ultima estrazione della carta.

Se viene inserito un luogo, l'informazione relativa deve essere registrata nella carta tachigrafica pertinente.

Le immissioni manuali devono interrompersi:

— in caso di estrazione della carta, oppure

— se il veicolo è in movimento e la carta è inserita nella sede (slot) del conducente.

Sono consentite ulteriori interruzioni, ad esempio dopo un periodo di inattività dell'utente. In caso di interruzione delle immissioni manuali, l'apparecchio di controllo deve convalidare tutte le indicazioni complete di luogo e attività già inserite (che indichino senza ambiguità un luogo e un'ora o un tipo di attività e un'ora di inizio e di fine).

Qualora venga inserita una seconda carta del conducente o dell'officina mentre è in corso l'immissione manuale di dati di attività relative alla carta precedentemente inserita, tale immissione manuale deve poter essere completata prima che abbia inizio l'immissione manuale dei dati relativi alla seconda carta.

Il titolare della carta deve avere la possibilità di effettuare l'immissione manuale di dati secondo la seguente procedura minima:

— Immissione manuale di attività in ordine cronologico per il periodo compreso tra l'ultima estrazione della carta e l'inserimento in corso.

— L'ora di inizio della prima attività deve essere fissato al momento dell'estrazione della carta. Per ciascuna immissione di dati successiva, l'ora di inizio deve essere fissata in modo da seguire immediatamente l'ora di fine dell'immissione di dati precedente. Per ciascuna attività devono essere selezionati il tipo e l'ora di fine.

▼B

La procedura è completata quando l'ora in cui termina un'attività inserita manualmente corrisponde all'ora di inserimento della carta. L'apparecchio di controllo può quindi consentire facoltativamente al titolare della carta di modificare ogni attività inserita manualmente, fino alla convalida mediante un apposito comando. Successivamente tali modifiche non devono più essere consentite.

3.6.3 *Immissione di condizioni particolari*

62) L'apparecchio di controllo deve consentire al conducente di inserire, in tempo reale, le due condizioni particolari seguenti:

— «ESCLUSO DAL CAMPO DI APPLICAZIONE» (inizio, fine)

— «ATTRAVERSAMENTO MEDIANTE TRAGHETTO/TRENO» (inizio, fine).

Un «ATTRAVERSAMENTO MEDIANTE TRAGHETTO/TRENO» non deve potersi verificare in presenza della condizione «ESCLUSO DAL CAMPO DI APPLICAZIONE».

Se presente, la condizione «ESCLUSO DAL CAMPO DI APPLICAZIONE» deve essere eliminata automaticamente dall'apparecchio di controllo quando viene inserita o estratta una carta del conducente.

L'eventuale condizione «ESCLUSO DAL CAMPO DI APPLICAZIONE» deve impedire i seguenti avvisi e le seguenti anomalie:

— guida in assenza di una carta adeguata;

— avvisi relativi al periodo di guida continuo.

L'indicatore (flag) di inizio dell'ATTRAVERSAMENTO MEDIANTE TRAGHETTO/TRENO deve essere impostato prima di spegnere il motore sul traghetto/treno.

Un ATTRAVERSAMENTO MEDIANTE TRAGHETTO/TRENO attivo deve terminare quando si verifica uno dei seguenti casi:

— il conducente termina manualmente l'ATTRAVERSAMENTO MEDIANTE TRAGHETTO/TRENO,

— il conducente espelle la sua carta.

Un ATTRAVERSAMENTO MEDIANTE TRAGHETTO/TRENO attivo deve terminare quando non è più valido sulla base delle regole indicate nel regolamento (CE) n. 561/2006.

3.7 **Gestione dei blocchi di un'impresa**

63) Questa funzione deve consentire di gestire i blocchi previsti da un'impresa per limitare a se stessa l'accesso ai dati nel modo azienda.

64) I blocchi di un'impresa consistono in una data/ora di inizio (attivazione blocco) e in una data/ora di termine (disattivazione blocco), associate all'identificazione dell'impresa risultante dal numero della carta dell'azienda (all'attivazione del blocco).

65) I blocchi possono essere attivati o disattivati solo in tempo reale.

66) Il blocco deve poter essere disattivato solo dall'impresa il cui blocco è attivo (identificata dai primi 13 caratteri del numero della carta dell'azienda) oppure

67) la disattivazione del blocco deve avvenire automaticamente quando un'altra impresa attiva un blocco.

▼B

68) Nel caso in cui un'impresa attivi un blocco e che il blocco precedente fosse della stessa impresa, allora si riterrà che il blocco precedente non sia stato disattivato e che sia tuttora attivato.

3.8 **Verifica delle attività di controllo**

69) Questa funzione deve verificare le attività di controllo «VISUALIZZAZIONE, STAMPA, TRASFERIMENTO dati della VU e della carta» e «TARATURA SU STRADA» nel modo controllo.

70) Essa deve inoltre verificare le attività di «CONTROLLO SUPERAMENTO DELLA VELOCITÀ» nel modo controllo. Un controllo del superamento della velocità si considera avvenuto quando, nel modo controllo, l'informazione «superamento della velocità» viene inviata alla stampante o al dispositivo di visualizzazione oppure quando i dati relativi ad «anomalie e guasti» vengono trasferiti dalla memoria di dati della VU.

3.9 **Rilevamento di anomalie e/o guasti**

71) Questa funzione deve rilevare le anomalie e/o i guasti seguenti:

3.9.1 *Anomalia «Inserimento di una carta non valida»*

72) Questa anomalia deve attivarsi all'inserimento di una carta non valida, all'inserimento di una carta del conducente già sostituita e/o quando una carta inserita in corso di validità scade.

3.9.2 *Anomalia «Conflitto di carte»*

73) Questa anomalia deve attivarsi quando si verifica una combinazione di carte in corso di validità indicata con X nella tabella seguente:

Conflitto di carte		Sede (slot) del conducente				
		Carta assente	Carta del conducente	Carta di controllo	Carta dell'officina	Carta dell'azienda
Sede (slot) del secondo conducente	Carta assente					
	Carta del conducente				X	
	Carta di controllo			X	X	X
	Carta dell'officina		X	X	X	X
	Carta dell'azienda			X	X	X

3.9.3 *Anomalia «Sovrapposizione di orari»*

74) Questa anomalia deve attivarsi quando la data/ora dell'ultima estrazione di una carta del conducente, letta sulla carta, è successiva alla data/ora corrente dell'apparecchio di controllo in cui è inserita la carta.

3.9.4 *Anomalia «Guida in assenza di una carta adeguata»*

75) Questa anomalia deve attivarsi per ogni combinazione valida di carte tachigrafiche indicata con X nella tabella seguente, quando l'attività del conducente passa a GUIDA o quando si verifica un cambio di modalità di funzionamento mentre l'attività del conducente è GUIDA:

▼B

Guida in assenza di una carta adeguata		Sede (slot) del conducente				
		Carta assente (o carta non valida)	Carta del conducente	Carta di controllo	Carta dell'officina	Carta dell'azienda
Sede (slot) del secondo conducente	Carta assente (o carta non valida)	X		X		X
	Carta del conducente	X		X	X	X
	Carta di controllo	X	X	X	X	X
	Carta dell'officina	X	X	X		X
	Carta dell'azienda	X	X	X	X	X

3.9.5 *Anomalia «Inserimento carta durante la guida»*

76) Questa anomalia deve attivarsi quando una carta tachigrafica viene inserita in qualsiasi sede, mentre l'attività del conducente è GUIDA.

3.9.6 *Anomalia «Chiusura errata ultima sessione carta»*

77) Questa anomalia deve attivarsi quando all'inserimento della carta l'apparecchio di controllo rileva che, nonostante le prescrizioni di cui al punto 3.1, la sessione precedente della carta non è stata chiusa in modo corretto (la carta è stata estratta prima che tutti i dati pertinenti fossero memorizzati sulla carta stessa). Questa anomalia deve attivarsi solo per le carte del conducente e dell'officina.

3.9.7 *Anomalia «Superamento della velocità»*

78) Questa anomalia deve attivarsi ad ogni superamento della velocità autorizzata.

3.9.8 *Anomalia «Interruzione dell'alimentazione di energia»*

79) Quando l'apparecchio non si trova nel modo taratura o nel modo controllo, questa anomalia deve attivarsi nel caso di un'interruzione dell'alimentazione del sensore di movimento e/o dell'unità elettronica di bordo di durata superiore a 200 millisecondi. La soglia di interruzione deve essere definita dal fabbricante. La caduta di alimentazione dovuta all'avviamento del motore del veicolo non deve attivare questa anomalia.

3.9.9 *Anomalia «Errore di comunicazione con il dispositivo di comunicazione remota»*

80) Questa anomalia deve attivarsi, **quando non è attivo il modo taratura**, quando il dispositivo di comunicazione remota non riconosce l'avvenuta ricezione dei dati della comunicazione remota inviati dall'unità elettronica di bordo per più di tre tentativi.

3.9.10 *Anomalia «Assenza di informazioni sulla posizione provenienti dal ricevitore GNSS»*

81) Questa anomalia deve attivarsi, **quando non è attivo il modo taratura**, in caso di assenza di informazioni sulla posizione provenienti dal ricevitore GNSS (sia interno che esterno) per più di tre ore di periodo di guida cumulato.

3.9.11 *Anomalia «Errore di comunicazione con il dispositivo GNSS esterno»*

82) Questa anomalia deve attivarsi, **quando non è attivo il modo taratura**, in caso di interruzione della comunicazione tra il dispositivo GNSS esterno e l'unità elettronica di bordo per più di 20 minuti consecutivi, quando il veicolo è in movimento.

▼B

3.9.12 *Anomalia «Errore dati di marcia»*

83) Questa anomalia deve attivarsi, **quando non è attivo il modo taratura**, in caso di interruzione del normale flusso di dati tra il sensore di movimento e l'unità elettronica di bordo e/o nel caso di un errore di integrità dei dati o di autenticazione dei dati durante lo scambio di dati tra il sensore di movimento e l'unità elettronica di bordo.

3.9.13 *Anomalia «Dati contrastanti sul movimento del veicolo»*

84) Questa anomalia deve attivarsi, **quando non è attivo il modo taratura**, nel caso in cui le informazioni sul movimento calcolate dal sensore di movimento siano contraddette dalle informazioni sul movimento calcolate dal ricevitore GNSS interno o dal dispositivo GNSS esterno e, facoltativamente, da altre fonti indipendenti, come specificato nell'appendice 12. Questa anomalia non deve attivarsi durante un attraversamento mediante traghetto/treno, una condizione «ESCLUSO DAL CAMPO DI APPLICAZIONE» o quando le informazioni sulla posizione provenienti dal ricevitore GNSS non sono disponibili.

3.9.14 *Anomalia «Tentata violazione della sicurezza»*

85) Questa anomalia deve attivarsi, quando non è attivo il modo taratura, in caso di ogni altra anomalia che influisca sulla sicurezza del sensore di movimento e/o dell'unità elettronica di bordo e/o del dispositivo GNSS esterno, come richiesto nell'appendice 10.

3.9.15 *Anomalia «Conflitto di orari»*

86) Questa anomalia deve attivarsi, **quando non è attivo il modo taratura**, quando la VU rileva una discrepanza di più di 1 minuto tra l'orario della funzione di misurazione del tempo dell'unità elettronica di bordo e l'orario proveniente dal ricevitore GNSS. Questa anomalia è registrata unitamente al valore dell'orologio interno dell'unità elettronica di bordo e con un meccanismo automatico di regolazione dell'ora. Dopo che si è attivata un'anomalia «Conflitto di orari», la VU non attiva altre anomalie dello stesso tipo per le successive 12 ore. Questa anomalia non deve attivarsi qualora nei precedenti 30 giorni non fosse rilevabile nessun segnale GNSS valido dal ricevitore GNSS. Tuttavia, quando le informazioni sulla posizione provenienti dal ricevitore GNSS sono nuovamente disponibili, deve avere luogo la regolazione automatica dell'ora.

3.9.16 *Guasto «Carta»*

87) Questo guasto deve attivarsi in caso di funzionamento difettoso della carta tachigrafica.

3.9.17 *Guasto «Apparecchio di controllo»*

88) Questo guasto deve attivarsi, quando non è attivo il modo taratura, in ciascuno dei casi seguenti:

— guasto interno della VU

— guasto della stampante

— guasto del dispositivo di visualizzazione

— guasto nel trasferimento di dati

— guasto del sensore

— guasto del ricevitore GNSS o del dispositivo GNSS esterno

— guasto del dispositivo di comunicazione remota

▼B

3.10 **Prove incorporate e prove automatiche**

89) L'apparecchio di controllo deve rilevare automaticamente i guasti mediante le prove automatiche e le prove incorporate, secondo la tabella seguente:

Sottoinsieme da sottoporre a prova	Prova automatica	Prova incorporata
Software		Integrità
Memoria di dati	Accesso	Accesso, integrità dei dati
Dispositivi di interfaccia della carta	Accesso	Accesso
Tastiera		Controllo manuale
Stampante	(a discrezione del fabbricante)	Stampa
Schermo		Controllo visivo
Trasferimento dati (effettuato solo durante il trasferimento dati)	Funzionamento corretto	
Sensore	Funzionamento corretto	Funzionamento corretto
Dispositivo di comunicazione remota	Funzionamento corretto	Funzionamento corretto
Dispositivo GNSS	Funzionamento corretto	Funzionamento corretto

3.11 **Lettura della memoria di dati**

90) L'apparecchio di controllo deve essere in grado di leggere ogni dato memorizzato nella sua memoria di dati.

3.12 **Registrazione e memorizzazione nella memoria di dati**

Agli effetti del presente punto:

— per «365 giorni» s'intende 365 giorni di calendario di attività media del conducente su un veicolo. L'attività media giornaliera su un veicolo è intesa come almeno 6 conducenti o secondi conducenti, 6 cicli di inserimento ed estrazione della carta e 256 cambi di attività. «365 giorni» comprende quindi almeno 2 190 conducenti (o secondi conducenti), 2 190 cicli di inserimento ed estrazione della carta e 93 440 cambi di attività,

— il numero medio di posizioni per ciascun giorno è inteso come almeno 6 posizioni in cui inizia il periodo di lavoro giornaliero, 6 posizioni in cui il periodo di guida continuo del conducente raggiunge un multiplo di tre ore e 6 posizioni in cui termina il periodo di lavoro giornaliero, per cui «365 giorni» comprende almeno 6 570 posizioni,

— se non diversamente specificato, i tempi sono registrati con una risoluzione di un minuto,

— i valori dell'odometro sono registrati con una risoluzione di un chilometro,

— le velocità sono registrate con una risoluzione di 1 km/h,

— le posizioni (latitudini e longitudini) sono registrate in gradi e minuti, con una risoluzione di 1/10 di minuto, con il tempo di acquisizione e l'accuratezza del GNSS correlati.

▼B

91) I dati memorizzati nella memoria di dati non devono essere compromessi da un'interruzione dell'alimentazione esterna di durata inferiore a dodici mesi in condizioni di omologazione. Inoltre, i dati archiviati nel dispositivo esterno di comunicazione remota, come definito nell'appendice 14, non devono essere compromessi da un'interruzione dell'alimentazione di durata inferiore a 28 giorni.

92) L'apparecchio di controllo deve essere in grado di registrare e memorizzare implicitamente o esplicitamente nella sua memoria di dati le informazioni sotto elencate.

3.12.1 *Dati di identificazione dell'apparecchio*

3.12.1.1 Dati di identificazione dell'unità elettronica di bordo

93) L'apparecchio di controllo deve essere in grado di memorizzare nella sua memoria di dati i seguenti dati di identificazione dell'unità elettronica di bordo:

— nome del fabbricante,

— indirizzo del fabbricante,

— codice componente,

— numero di serie,

— generazione della VU,

— capacità di utilizzare carte tachigrafiche di prima generazione,

— numero di versione del software,

— data di installazione della versione del software,

— anno di fabbricazione dell'apparecchio,

— numero di omologazione.

94) I dati di identificazione dell'unità elettronica di bordo sono registrati e memorizzati una sola volta dal fabbricante dell'unità, eccetto i dati relativi al software e il numero di omologazione, che si possono modificare in caso di aggiornamento del software, e la capacità di utilizzare carte tachigrafiche di prima generazione.

3.12.1.2 Dati di identificazione del sensore di movimento

95) Il sensore di movimento deve essere in grado di memorizzare nella sua memoria i seguenti dati di identificazione:

— nome del fabbricante,

— numero di serie,

— numero di omologazione,

— identificativo del componente di sicurezza incorporato (per es., codice componente del chip/processore interno),

— identificativo del sistema operativo (per es., numero di versione del software).

96) I dati di identificazione del sensore di movimento sono registrati e memorizzati una sola volta dal fabbricante del sensore.

97) L'unità elettronica di bordo deve essere in grado di registrare e memorizzare nella sua memoria di dati i dati seguenti relativi agli ultimi 20 abbinamenti dei sensori di movimento (se in un giorno di calendario avvengono più abbinamenti, si registrano solo il primo e l'ultimo):

▼B

Per ciascuno di tali abbinamenti si devono registrare i dati seguenti:

— dati di identificazione del sensore di movimento:

— numero di serie

— numero di omologazione

— dati di abbinamento al sensore di movimento:

— data dell'abbinamento.

3.12.1.3 Dati di identificazione dei sistemi globali di navigazione satellitare

98) Il dispositivo GNSS esterno deve essere in grado di memorizzare nella sua memoria i seguenti dati di identificazione:

— nome del fabbricante,

— numero di serie,

— numero di omologazione,

— identificativo del componente di sicurezza incorporato (per es., codice componente del chip/processore interno),

— identificativo del sistema operativo (per es., numero di versione del software).

99) I dati di identificazione sono registrati e memorizzati una sola volta nel dispositivo GNSS esterno dal fabbricante dello stesso.

100) L'unità elettronica di bordo deve essere in grado di registrare e memorizzare nella sua memoria di dati i dati seguenti relativi agli ultimi 20 accoppiamenti dei dispositivi GNSS esterni (se in un giorno di calendario avvengono più accoppiamenti, si registrano solo il primo e l'ultimo).

Per ciascuno di tali accoppiamenti devono essere registrati i dati seguenti:

— dati di identificazione del dispositivo GNSS esterno:

— numero di serie,

— numero di omologazione,

— dati di accoppiamento al dispositivo GNSS esterno:

— data dell'accoppiamento

3.12.2 *Chiavi e certificati*

101) L'apparecchio di controllo deve essere in grado di memorizzare una serie di chiavi crittografiche e di certificati, come specificato nell'appendice 11, parti A e B.

3.12.3 *Dati relativi all'inserimento e all'estrazione della carta del conducente o dell'officina*

102) Per ogni ciclo di inserimento ed estrazione dall'apparecchio di una carta del conducente o dell'officina, l'apparecchio di controllo deve registrare e memorizzare nella sua memoria di dati:

— cognome e nome/i del titolare della carta, memorizzati nella carta stessa,

— numero della carta, Stato membro che l'ha rilasciata e data di scadenza, memorizzati nella carta stessa,

— generazione della carta,

▼B

— data e ora di inserimento,

— valore dell'odometro del veicolo all'atto dell'inserimento,

— sede (slot) in cui è inserita la carta,

— data e ora di estrazione,

— valore dell'odometro del veicolo all'atto dell'estrazione,

— le seguenti informazioni relative al veicolo usato in precedenza dal conducente, memorizzate nella carta:

  — VRN e Stato membro di immatricolazione,

  — generazione della VU (se disponibile),

  — data e ora di estrazione della carta,

— un indicatore (flag) che segnali se, all'atto dell'inserimento della carta, il titolare della carta abbia o meno inserito manualmente le attività.

103) La memoria di dati deve essere in grado di conservare tali informazioni per almeno 365 giorni.

104) Qualora si esaurisca la capacità di memorizzazione, i dati nuovi devono sostituire quelli meno recenti.

3.12.4 *Dati relativi all'attività del conducente*

105) L'apparecchio di controllo deve registrare e memorizzare nella sua memoria di dati, ogniqualvolta si verifichi un cambio di attività del conducente e/o del secondo conducente e/o ogniqualvolta si verifichi una variazione della condizione di guida e/o ogniqualvolta venga inserita o estratta una carta del conducente o dell'officina:

— la condizione di guida (EQUIPAGGIO, SINGOLA),

— la sede (slot) (CONDUCENTE, SECONDO CONDUCENTE),

— la condizione della carta nella relativa sede (slot) (INSERITA, NON INSERITA),

— l'attività (GUIDA, DISPONIBILITÀ, LAVORO, INTERRUZIONE/RIPOSO),

— la data e l'ora del cambio.

INSERITA significa che una carta del conducente o dell'officina in corso di validità è inserita nella sede (slot). NON INSERITA significa il contrario, cioè che nella sede non è inserita una carta del conducente o dell'officina in corso di validità (per es., è inserita una carta dell'azienda oppure non è inserita alcuna carta).

I dati relativi all'attività inseriti manualmente dal conducente non vengono registrati nella memoria di dati.

106) La memoria di dati deve essere in grado di conservare i dati relativi all'attività del conducente per almeno 365 giorni.

107) Qualora si esaurisca la capacità di memorizzazione, i dati nuovi devono sostituire quelli meno recenti.

▼B

3.12.5 *Luoghi e posizioni dove iniziano e terminano i periodi di lavoro giornalieri e/o dove il periodo di guida continuo raggiunge le 3 ore*

108) L'apparecchio di controllo deve registrare e memorizzare nella sua memoria di dati:

— i luoghi e le posizioni dove il conducente e/o il secondo conducente iniziano il loro periodo di lavoro giornaliero;

— le posizioni dove il periodo di guida continuo del conducente raggiunge un multiplo di tre ore;

— i luoghi e le posizioni dove il conducente e/o il secondo conducente terminano il loro periodo di lavoro giornaliero.

109) Quando la posizione del veicolo non è rilevabile dal ricevitore GNSS in quei momenti, l'apparecchio di controllo deve utilizzare la posizione disponibile più recente e la relativa data e ora.

110) Insieme a ciascun luogo o posizione, l'apparecchio di controllo deve registrare e memorizzare nella sua memoria di dati:

— il numero di carta del conducente (o del secondo conducente) e lo Stato membro che l'ha rilasciata,

— la generazione della carta,

— la data e l'ora d'immissione dei dati,

— il tipo di immissione (inizio, fine o 3 ore di periodo di guida continuo),

— l'accuratezza del GNSS, la data e l'ora pertinenti, se applicabili,

— il valore dell'odometro del veicolo.

111) La memoria di dati deve essere in grado di conservare per almeno 365 giorni i luoghi e le posizioni in cui i periodi di lavoro giornalieri iniziano e terminano e/o in cui il periodo di guida continuo raggiunge le 3 ore.

112) Qualora si esaurisca la capacità di memorizzazione, i dati nuovi devono sostituire quelli meno recenti.

3.12.6 *Dati relativi all'odometro*

113) L'apparecchio di controllo deve registrare nella sua memoria di dati il valore dell'odometro del veicolo e la data di registrazione alla mezzanotte di ogni giorno di calendario.

114) La memoria di dati deve essere in grado di memorizzare i valori dell'odometro registrati a mezzanotte per almeno 365 giorni di calendario.

115) Qualora si esaurisca la capacità di memorizzazione, i dati nuovi devono sostituire quelli meno recenti.

3.12.7 *Dati dettagliati relativi alla velocità*

116) L'apparecchio di controllo deve registrare e memorizzare nella sua memoria di dati la velocità istantanea del veicolo e la data e l'ora di registrazione ogni secondo per almeno le ultime 24 ore di marcia del veicolo.

3.12.8 *Dati relativi alle anomalie*

Agli effetti del presente punto, l'ora deve essere registrata con una risoluzione di 1 secondo.

117) L'apparecchio di controllo deve registrare e memorizzare nella sua memoria di dati i dati sottoelencati per ogni anomalia rilevata, in base alle seguenti regole di memorizzazione:

▼B

Anomalia	Regole di memorizzazione	Dati da registrare per ogni anomalia
Inserimento di una carta non valida	— le 10 anomalie più recenti.	— data e ora dell'anomalia, — tipo, numero, Stato membro di rilascio e generazione della carta o delle carte che hanno dato origine all'anomalia. — numero di anomalie simili nel giorno in questione.
Conflitto di carte	— le 10 anomalie più recenti.	— data e ora di inizio dell'anomalia, — data e ora di fine dell'anomalia, — tipo, numero, Stato membro di rilascio e generazione delle due carte che hanno dato origine al conflitto.
Guida in assenza di una carta adeguata	— l'anomalia di maggiore durata per ciascuno degli ultimi 10 giorni in cui si è verificata, — le 5 anomalie di maggiore durata nel corso degli ultimi 365 giorni.	— data e ora di inizio dell'anomalia, — data e ora di fine dell'anomalia, — tipo, numero, Stato membro di rilascio e generazione delle carte inserite all'inizio e/o alla fine dell'anomalia, — numero di anomalie simili nel giorno in questione.
Inserimento della carta durante la guida	— l'ultima anomalia per ciascuno degli ultimi 10 giorni in cui si è verificata,	— data e ora dell'anomalia, — tipo, numero, Stato membro di rilascio e generazione della carta o delle carte, — numero di anomalie simili nel giorno in questione.

Chiusura errata dell'ultima sessione della carta	— le 10 anomalie più recenti.	— data e ora dell'inserimento della carta,
		— tipo, numero, Stato membro di rilascio e generazione della carta o delle carte,
		— dati relativi all'ultima sessione letti sulla carta:
		  — data e ora dell'inserimento della carta,
		  — VRN, Stato membro di immatricolazione e generazione della VU.

Superamento della velocità (1)	— l'anomalia più grave per ciascuno degli ultimi 10 giorni in cui si è verificata (cioè quella con la più alta velocità media), — le 5 anomalie più gravi nel corso degli ultimi 365 giorni, — la prima anomalia verificatasi dopo l'ultima taratura.	— data e ora di inizio dell'anomalia, — data e ora di fine dell'anomalia, — velocità massima misurata durante l'anomalia, — media aritmetica della velocità misurata durante l'anomalia, — tipo, numero, Stato membro di rilascio e generazione della carta del conducente (se applicabili), — numero di anomalie simili nel giorno in questione.

▼B

Anomalia	Regole di memorizzazione	Dati da registrare per ogni anomalia
Interruzione dell'alimentazione di energia (2)	— l'anomalia di maggiore durata per ciascuno degli ultimi 10 giorni in cui si è verificata, — le 5 anomalie di maggiore durata nel corso degli ultimi 365 giorni.	— data e ora di inizio dell'anomalia, — data e ora di fine dell'anomalia, — tipo, numero, Stato membro di rilascio e generazione delle carte inserite all'inizio e/o alla fine dell'anomalia, — numero di anomalie simili nel giorno in questione.
Errore di comunicazione con il dispositivo di comunicazione remota	— l'anomalia di maggiore durata per ciascuno degli ultimi 10 giorni in cui si è verificata, — le 5 anomalie di maggiore durata nel corso degli ultimi 365 giorni.	— data e ora di inizio dell'anomalia, — data e ora di fine dell'anomalia, — tipo, numero, Stato membro di rilascio e generazione delle carte inserite all'inizio e/o alla fine dell'anomalia, — numero di anomalie simili nel giorno in questione.
Assenza di informazioni sulla posizione provenienti dal ricevitore GNSS	— l'anomalia di maggiore durata per ciascuno degli ultimi 10 giorni in cui si è verificata, — le 5 anomalie di maggiore durata nel corso degli ultimi 365 giorni.	— data e ora di inizio dell'anomalia, — data e ora di fine dell'anomalia, — tipo, numero, Stato membro di rilascio e generazione delle carte inserite all'inizio e/o alla fine dell'anomalia, — numero di anomalie simili nel giorno in questione.
Errore dei dati di movimento	— l'anomalia di maggiore durata per ciascuno degli ultimi 10 giorni in cui si è verificata, — le 5 anomalie di maggiore durata nel corso degli ultimi 365 giorni.	— data e ora di inizio dell'anomalia, — data e ora di fine dell'anomalia, — tipo, numero, Stato membro di rilascio e generazione delle carte inserite all'inizio e/o alla fine dell'anomalia, — numero di anomalie simili nel giorno in questione.
Dati contrastanti sul movimento del veicolo	— l'anomalia di maggiore durata per ciascuno degli ultimi 10 giorni in cui si è verificata, — le 5 anomalie di maggiore durata nel corso degli ultimi 365 giorni.	— data e ora di inizio dell'anomalia, — data e ora di fine dell'anomalia, — tipo, numero, Stato membro di rilascio e generazione delle carte inserite all'inizio e/o alla fine dell'anomalia, — numero di anomalie simili nel giorno in questione.
Tentativi di violazione della sicurezza	— le ultime 10 anomalie per ogni tipo di anomalia.	— data e ora di inizio dell'anomalia, — data e ora di fine dell'anomalia (se pertinenti), — tipo, numero, Stato membro di rilascio e generazione delle carte inserite all'inizio e/o alla fine dell'anomalia, — tipo di anomalia.

▼B

Anomalia	Regole di memorizzazione	Dati da registrare per ogni anomalia
Dati contrastanti sull'ora	— l'anomalia di maggiore durata per ciascuno degli ultimi 10 giorni in cui si è verificata, — le 5 anomalie di maggiore durata nel corso degli ultimi 365 giorni.	— data e ora dell'apparecchio di controllo, — data e ora del GNSS, — tipo, numero, Stato membro di rilascio e generazione delle carte inserite all'inizio e/o alla fine dell'anomalia, — numero di anomalie simili nel giorno in questione.

(1) L'apparecchio di controllo deve registrare e memorizzare nella sua memoria di dati anche:

— la data e l'ora dell'ultimo CONTROLLO DEL SUPERAMENTO DELLA VELOCITÀ,

— la data e l'ora del primo superamento della velocità successivo a tale CONTROLLO DEL SUPERAMENTO DELLA VELOCITÀ,

— il numero di anomalie per superamento della velocità verificatesi dall'ultimo CONTROLLO DEL SUPERAMENTO DELLA VELOCITÀ.

(2) Questi dati si possono registrare solo al ripristino dell'alimentazione di energia, l'ora può essere nota con un'accuratezza al minuto.

3.12.9 *Dati relativi ai guasti*

Agli effetti del presente punto, l'ora deve essere registrata con una risoluzione di 1 secondo.

118) L'apparecchio di controllo deve cercare di registrare e memorizzare nella sua memoria di dati i dati sottoelencati per ciascun guasto rilevato, in base alle seguenti regole di memorizzazione:

Guasto	Regole di memorizzazione	Dati da registrare per ciascun guasto
Guasto della carta	— gli ultimi 10 guasti della carta del conducente.	— data e ora di inizio del guasto, — data e ora di fine del guasto, — tipo, numero, Stato membro di rilascio e generazione della carta o delle carte.
Guasti dell'apparecchio di controllo	— gli ultimi 10 guasti per ogni tipo di guasto, — il primo guasto dopo l'ultima taratura.	— data e ora di inizio del guasto, — data e ora di fine del guasto, — tipo di guasto, — tipo, numero, Stato membro di rilascio e generazione delle carte inserite all'inizio e/o alla fine del guasto.

3.12.10 *Dati relativi alla taratura*

119) L'apparecchio di controllo deve registrare e memorizzare nella sua memoria di dati le informazioni relative a:

— i parametri di taratura noti al momento dell'attivazione,

▼B

— la prima taratura successiva all'attivazione,

— la prima taratura sul veicolo in cui è montato (identificato dal VIN),

— le ultime 20 tarature (se si effettuano diverse tarature nello stesso giorno di calendario, si devono memorizzare soltanto la prima e l'ultima del giorno).

120) Per ciascuna di tali tarature si devono registrare i dati seguenti:

— scopo della taratura (attivazione, primo montaggio, montaggio, controllo periodico),

— denominazione e indirizzo dell'officina,

— numero di carta dell'officina, Stato membro di rilascio della carta e data di scadenza della carta,

— identificazione del veicolo,

— parametri aggiornati o confermati: w, k, l, dimensioni degli pneumatici, regolazione del limitatore di velocità, odometro (vecchio e nuovo valore), data e ora (vecchio e nuovo valore),

— i tipi e gli identificativi di tutti i sigilli apposti.

121) Inoltre, l'apparecchio di controllo deve registrare e memorizzare nella sua memoria di dati la sua eventuale capacità di utilizzare le carte tachigrafiche di prima generazione (ancora attivate o meno).

122) Il sensore di movimento deve registrare e memorizzare nella sua memoria i seguenti dati di montaggio del sensore stesso:

— primo abbinamento con una VU (data, ora, numero di omologazione della VU, numero di serie della VU),

— ultimo abbinamento con una VU (data, ora, numero di omologazione della VU, numero di serie della VU).

123) Il dispositivo GNSS esterno deve registrare e memorizzare nella sua memoria i seguenti dati di montaggio del dispositivo stesso:

— primo accoppiamento con una VU (data, ora, numero di omologazione della VU, numero di serie della VU),

— ultimo accoppiamento con una VU (data, ora, numero di omologazione della VU, numero di serie della VU).

3.12.11 *Dati relativi alla regolazione dell'ora*

124) L'apparecchio di controllo deve registrare e memorizzare nella sua memoria di dati i dati relativi alle regolazioni dell'ora effettuate in modo taratura al di fuori di un ciclo ordinario di taratura (def. f):

— l'ultima regolazione dell'ora,

— le 5 regolazioni dell'ora di maggiore portata.

125) Per ciascuna di tali regolazioni dell'ora devono essere registrati i dati seguenti:

— data e ora, vecchio valore,

— data e ora, nuovo valore,

— denominazione e indirizzo dell'officina,

— numero di carta dell'officina, Stato membro di rilascio, generazione e data di scadenza della carta.

▼B

3.12.12 *Dati relativi alle attività di controllo*

126) L'apparecchio di controllo deve registrare e memorizzare nella sua memoria di dati i dati seguenti relativi alle ultime 20 attività di controllo:

— data e ora del controllo,

— numero della carta di controllo, Stato membro di rilascio e generazione della carta,

— tipo di controllo (visualizzazione e/o stampa e/o trasferimento dati VU e/o trasferimento dati carta e/o verifica della taratura su strada).

127) Nel caso del trasferimento, si devono registrare anche le date del giorno meno recente e del giorno più recente cui si riferiscono i dati trasferiti.

3.12.13 *Dati relativi ai blocchi di un'impresa*

128) L'apparecchio di controllo deve registrare e memorizzare nella sua memoria di dati i dati seguenti relativi agli ultimi 255 blocchi di un'impresa:

— data e ora di attivazione del blocco,

— data e ora di disattivazione del blocco,

— numero della carta dell'azienda, Stato membro di rilascio e generazione della carta,

— denominazione e indirizzo dell'impresa.

I dati precedentemente bloccati mediante un blocco rimosso dalla memoria a seguito del raggiungimento dei limiti di cui sopra devono essere considerati non bloccati.

3.12.14 *Dati relativi al trasferimento*

129) L'apparecchio di controllo deve registrare e memorizzare nella sua memoria di dati i dati seguenti, relativi all'ultimo trasferimento della memoria di dati su un dispositivo esterno in modo azienda o taratura:

— data e ora del trasferimento,

— numero della carta dell'azienda o dell'officina, Stato membro di rilascio e generazione della carta,

— denominazione dell'impresa o dell'officina.

3.12.15 *Dati relativi a condizioni particolari*

130) L'apparecchio di controllo deve registrare e memorizzare nella sua memoria di dati i dati seguenti, relativi a condizioni particolari:

— data e ora di immissione,

— tipo di condizione particolare.

131) La memoria di dati deve essere in grado di conservare i dati relativi alle condizioni particolari per almeno 365 giorni (nell'ipotesi che in media si apra e si chiuda 1 condizione al giorno). Qualora si esaurisca la capacità di memorizzazione, i dati nuovi devono sostituire quelli meno recenti.

3.12.16 *Dati della carta tachigrafica*

132) L'apparecchio di controllo deve essere in grado di memorizzare i dati seguenti, relativi alle diverse carte tachigrafiche che sono state utilizzate nella VU:

— il numero della carta tachigrafica e il suo numero di serie,

— il fabbricante della carta tachigrafica,

▼B

— il tipo di carta tachigrafica,

— la versione della carta tachigrafica.

133) L'apparecchio di controllo deve essere in grado di memorizzare almeno 88 di tali registrazioni.

3.13 **Lettura delle carte tachigrafiche**

134) L'apparecchio di controllo deve essere in grado di leggere dalle carte tachigrafiche di prima e seconda generazione, se del caso, i dati necessari a:

— identificare il tipo di carta, il titolare della carta, il veicolo usato in precedenza, la data e l'ora dell'ultima estrazione della carta e l'attività selezionata in quel momento,

— verificare che l'ultima sessione della carta sia stata chiusa in modo corretto,

— calcolare il periodo di guida continuo del conducente, il periodo cumulato di interruzione e i periodi cumulati di guida per la settimana corrente e per quella precedente,

— stampare i documenti relativi ai dati registrati su una carta del conducente,

— trasferire i dati di una carta del conducente su un dispositivo esterno.

Questo requisito si applica unicamente alle carte tachigrafiche di prima generazione, se il loro utilizzo non è stato precluso da un'officina.

135) In caso di errore di lettura, l'apparecchio di controllo deve riprovare, un massimo di tre volte, ad inviare il medesimo comando di lettura; quindi, se l'errore persiste, deve dichiarare la carta guasta e non valida.

3.14 **Registrazione e memorizzazione nelle carte tachigrafiche**

3.14.1 *Registrazione e memorizzazione nelle carte tachigrafiche di prima generazione*

136) Purché l'uso delle carte tachigrafiche di prima generazione non sia stato precluso da un'officina, l'apparecchio di controllo deve registrare e memorizzare i dati esattamente come farebbe un apparecchio di controllo di prima generazione.

137) L'apparecchio di controllo deve impostare i «dati relativi alla sessione della carta» nella carta del conducente o dell'officina immediatamente dopo l'inserimento della carta.

138) L'apparecchio di controllo deve aggiornare i dati memorizzati in una carta valida del conducente, dell'officina, dell'azienda e/o di controllo con tutti i dati necessari relativi al periodo durante il quale la carta è inserita e al titolare della carta. I dati memorizzati in tali carte sono specificati nella sezione 4.

139) L'apparecchio di controllo deve aggiornare i dati relativi all'attività del conducente e ai luoghi (come specificato ai punti 4.5.3.1.9 e 4.5.3.1.11) memorizzati su una carta valida del conducente e/o dell'officina con i dati relativi all'attività e ai luoghi inseriti manualmente dal titolare della carta.

140) Tutte le anomalie non definite per le apparecchiature di controllo di prima generazione non devono essere memorizzate sulle carte del conducente e dell'officina.

▼B

141) L'aggiornamento dei dati delle carte tachigrafiche deve avvenire in modo tale che, all'occorrenza e tenuto conto della capacità di memorizzazione effettiva della carta, i nuovi dati sostituiscano quelli meno recenti.

142) In caso di errore di scrittura, l'apparecchio di controllo deve riprovare, un massimo di tre volte, ad inviare il medesimo comando di scrittura; quindi, se l'errore persiste, deve dichiarare la carta guasta e non valida.

143) Prima di consentire l'estrazione di una carta del conducente e dopo avere memorizzato nella carta tutti i dati pertinenti, l'apparecchio di controllo deve azzerare i «dati relativi alla sessione della carta».

3.14.2 *Registrazione e memorizzazione nelle carte tachigrafiche di seconda generazione*

144) Le carte tachigrafiche di seconda generazione devono contenere 2 diverse applicazioni della carta, la prima esattamente uguale all'applicazione TACHO delle carte tachigrafiche di prima generazione, mentre la seconda deve essere l'applicazione «TACHO_G2», come specificato nella sezione 4 e nell'appendice 2.

145) L'apparecchio di controllo deve impostare i «dati relativi alla sessione della carta» nella carta del conducente o dell'officina immediatamente dopo l'inserimento della carta.

146) L'apparecchio di controllo deve aggiornare i dati memorizzati nelle 2 applicazioni di una carta valida del conducente, dell'officina, dell'azienda e/o di controllo con tutti i dati necessari relativi al periodo durante il quale la carta è inserita e al titolare della carta. I dati memorizzati in tali carte sono specificati nella sezione 4.

147) L'apparecchio di controllo deve aggiornare i dati relativi ai luoghi e alle posizioni dell'attività del conducente (come specificato ai punti 4.5.3.1.9, 4.5.3.1.11, 4.5.3.2.9 e 4.5.3.2.11), memorizzati su una carta valida del conducente e/o dell'officina, con i dati relativi all'attività e ai luoghi inseriti manualmente dal titolare della carta.

148) L'aggiornamento dei dati delle carte tachigrafiche deve avvenire in modo tale che, all'occorrenza e tenuto conto della capacità di memorizzazione effettiva della carta, i nuovi dati sostituiscano quelli meno recenti.

149) In caso di errore di scrittura, l'apparecchio di controllo deve riprovare, un massimo di tre volte, ad inviare il medesimo comando di scrittura; quindi, se l'errore persiste, deve dichiarare la carta guasta e non valida.

150) Prima di consentire l'estrazione di una carta del conducente e dopo avere memorizzato nelle 2 applicazioni della carta tutti i dati pertinenti, l'apparecchio di controllo deve azzerare i «dati relativi alla sessione della carta».

3.15 **Visualizzazione**

151) Il dispositivo di visualizzazione deve comprendere almeno 20 caratteri.

152) La dimensione minima prescritta per i caratteri è di 5 mm in altezza e 3,5 mm in larghezza.

153) Il dispositivo di visualizzazione deve gestire i caratteri specificati nell'appendice 1, sezione 4, «Insiemi di caratteri». Il dispositivo di visualizzazione può usare caratteri semplificati (per es. le lettere accentate possono apparire senza l'accento o le lettere minuscole possono apparire come maiuscole).

▼B

154) Il dispositivo di visualizzazione deve essere munito di un'illuminazione adeguata non abbagliante.

155) Le indicazioni devono essere visibili dall'esterno dell'apparecchio di controllo.

156) L'apparecchio di controllo deve essere in grado di visualizzare:

— i dati predefiniti,

— i dati relativi agli avvisi,

— i dati relativi all'accesso guidato da menù,

— altri dati richiesti dall'utilizzatore.

L'apparecchio di controllo può visualizzare altre informazioni, a condizione che siano chiaramente distinte da quelle di cui sopra.

157) Il dispositivo di visualizzazione dell'apparecchio di controllo deve usare i pittogrammi o le combinazioni di pittogrammi elencati nell'appendice 3. Il dispositivo di visualizzazione può prevedere altri pittogrammi o combinazioni di pittogrammi, purché siano chiaramente distinti da quelli summenzionati.

158) Il dispositivo di visualizzazione deve essere sempre acceso durante la marcia del veicolo.

159) L'apparecchio di controllo può prevedere un comando manuale o automatico per spegnere il dispositivo di visualizzazione quando il veicolo non è in marcia.

Il formato di visualizzazione è specificato nell'appendice 5.

3.15.1 *Visualizzazione predefinita*

160) In assenza di altre informazioni da visualizzare, l'apparecchio di controllo deve visualizzare, nell'impostazione predefinita, le seguenti informazioni:

— l'ora locale (risultante dall'ora UTC, con regolazione effettuata dal conducente),

— la modalità di funzionamento,

— l'attività in corso del conducente e del secondo conducente,

— informazioni relative al conducente:

— se l'attività in corso è GUIDA, il periodo di guida continuo in corso e il periodo cumulato di interruzione in corso,

— se l'attività in corso non è GUIDA, la durata di tale attività (a partire dal momento in cui è stata selezionata) e il periodo cumulato di interruzione in corso.

161) La visualizzazione dei dati relativi a ciascun conducente deve essere chiara, semplice ed inequivocabile. Qualora non sia possibile visualizzare contemporaneamente le informazioni relative al conducente e al secondo conducente, l'apparecchio di controllo deve visualizzare per definizione le informazioni relative al conducente e consentire all'utente di visualizzare le informazioni relative al secondo conducente.

162) Qualora la larghezza del dispositivo non consenta di visualizzare per definizione la modalità di funzionamento, ad ogni variazione l'apparecchio di controllo deve visualizzare brevemente la nuova modalità di funzionamento.

▼B

163) L'apparecchio di controllo deve visualizzare brevemente il nome del titolare all'atto dell'inserimento della carta.

164) Qualora si attivi una condizione «ESCLUSO DAL CAMPO DI APPLICAZIONE» o «TRAGHETTO/TRENO», la visualizzazione predefinita deve indicare, mediante l'apposito pittogramma, che tale condizione è attiva (è ammesso che l'attività in corso del conducente non sia indicata nel contempo).

3.15.2 *Visualizzazione degli avvisi*

165) L'apparecchio di controllo deve visualizzare gli avvisi utilizzando principalmente i pittogrammi di cui all'appendice 3, integrati, se necessario, da un codice numerico supplementare. Si può anche aggiungere una descrizione dell'avviso nella lingua abituale del conducente.

3.15.3 *Accesso guidato da menù*

166) L'apparecchio di controllo deve fornire i comandi necessari attraverso un'apposita struttura a menù.

3.15.4 *Visualizzazione di altre informazioni*

167) Deve essere possibile visualizzare selettivamente, su richiesta:

— la data e l'ora UTC e la regolazione dell'ora locale;

— il contenuto di ciascuno dei sei documenti stampati, nello stesso formato dei documenti stessi;

— il periodo di guida continuo e il periodo cumulato di interruzione del conducente;

— il periodo di guida continuo e il periodo cumulato di interruzione del secondo conducente;

— il periodo di guida cumulato del conducente relativo alla settimana in corso e a quella precedente;

— il periodo di guida cumulato del secondo conducente relativo alla settimana in corso e a quella precedente;

informazioni facoltative:

— la durata attuale dell'attività del secondo conducente (a partire dal momento in cui è stata selezionata);

— il periodo di guida cumulato del conducente relativo alla settimana in corso;

— il periodo di guida cumulato del secondo conducente relativo al giorno di lavoro in corso;

— il periodo di guida cumulato del conducente relativo al giorno di lavoro in corso.

168) La visualizzazione del contenuto dei documenti stampati deve essere sequenziale, riga per riga. Qualora la larghezza del dispositivo di visualizzazione sia inferiore a 24 caratteri, l'utilizzatore deve poter ottenere le informazioni complete mediante un sistema adeguato (più righe, scorrimento del testo, ecc.).

Ai fini della visualizzazione si possono omettere le righe dei documenti stampati riservate alle informazioni da riportare a mano.

▼B

3.16 **Stampa**

169) L'apparecchio di controllo deve essere in grado di stampare le seguenti informazioni contenute nella sua memoria di dati e/o nelle carte tachigrafiche, in modo da ottenere i sette documenti stampati seguenti:

— stampa giornaliera delle attività del conducente contenute nella carta,

— stampa giornaliera delle attività del conducente contenute nell'unità elettronica di bordo,

— stampa di anomalie e guasti contenuti nella carta,

— stampa di anomalie e guasti contenuti nell'unità elettronica di bordo,

— stampa dei dati tecnici,

— stampa dei superamenti della velocità,

— cronologia dei dati della carta tachigrafica per una determinata VU (cfr. punto 3.12.16).

Il formato e il contenuto precisi di tali documenti stampati sono specificati nell'appendice 4.

In fondo ai documenti stampati si possono riportare anche altre informazioni.

L'apparecchio di controllo può inoltre fornire altri documenti stampati, purché siano chiaramente distinguibili dai sette documenti summenzionati.

170) I documenti «stampa giornaliera delle attività del conducente contenute nella carta» e «stampa di anomalie e guasti contenuti nella carta» devono essere disponibili solo quando nell'apparecchio di controllo è inserita una carta del conducente o una carta dell'officina. L'apparecchio di controllo deve aggiornare i dati contenuti nella carta prima di iniziare la stampa.

171) Per produrre il documento «stampa giornaliera delle attività del conducente contenute nella carta» o il documento «stampa di anomalie e guasti contenuti nella carta», l'apparecchio di controllo deve:

— selezionare automaticamente la carta del conducente o la carta dell'officina, se solo una delle due è inserita, oppure

— prevedere un comando per selezionare la carta da cui attingere i dati o selezionare la carta inserita nella sede (slot) «conducente», se due di tali carte sono inserite nell'apparecchio di controllo.

172) La stampante deve essere in grado di stampare 24 caratteri per riga.

173) La dimensione minima prescritta per i caratteri è di 2,1 mm in altezza e 1,5 mm in larghezza.

174) La stampante deve poter stampare i caratteri specificati nell'appendice 1, sezione 4, «Insiemi di caratteri».

175) Le stampanti devono essere progettate in modo da fornire i suddetti documenti stampati con un grado di definizione atto ad evitare qualsiasi ambiguità nella lettura.

176) I documenti stampati devono conservare le loro dimensioni e le loro registrazioni in condizioni normali di umidità (10-90 %) e di temperatura.

177) La carta omologata usata per la stampa deve recare il marchio di omologazione pertinente e l'indicazione del tipo o dei tipi di apparecchio di controllo con cui può essere utilizzata.

▼B

178) I documenti stampati devono rimanere chiaramente leggibili e identificabili in condizioni normali di conservazione, per quanto riguarda l'intensità luminosa, l'umidità e la temperatura, per almeno due anni.

179) I documenti stampati devono essere quantomeno conformi alle specifiche di prova di cui all'appendice 9.

180) Deve inoltre essere possibile aggiungere su questi documenti note manoscritte supplementari, come la firma del conducente.

181) L'apparecchio di controllo deve gestire anomalie del tipo «mancanza carta» durante la stampa, riavviando la stampa dall'inizio del documento in seguito al caricamento della carta o continuando la stampa e fornendo un riferimento inequivocabile alla parte già stampata.

3.17 **Avvisi**

182) L'apparecchio di controllo deve inviare un segnale di avviso al conducente quando rileva un'anomalia e/o un guasto.

183) L'avviso di un'anomalia dovuta ad interruzione dell'alimentazione può attivarsi anche solo dopo il ripristino dell'alimentazione stessa.

184) L'apparecchio di controllo deve inviare un segnale di avviso al conducente 15 minuti prima del superamento del periodo massimo di guida continuo consentito e nel momento in cui tale limite viene superato.

185) I segnali di avviso devono essere visivi. Si possono anche prevedere avvisi acustici in aggiunta a quelli visivi.

186) Gli avvisi visivi devono essere chiaramente riconoscibili dall'utente, devono rientrare nel campo visivo del conducente ed essere chiaramente leggibili sia di giorno che di notte.

187) Gli avvisi visivi possono essere incorporati nell'apparecchio di controllo e/o collocati in posizione remota rispetto all'apparecchio di controllo.

188) In quest'ultimo caso devono recare il simbolo «T».

189) Gli avvisi devono avere una durata di almeno 30 secondi, salvo che l'utente con la pressione di uno o più tasti specifici dell'apparecchio di controllo non confermi di averne preso atto. Questa prima conferma non deve annullare la visualizzazione della causa dell'avviso menzionata nel paragrafo successivo.

190) La causa dell'avviso deve essere visualizzata sull'apparecchio di controllo e rimanere visibile fino alla conferma da parte dell'utente mediante l'uso di un apposito tasto o comando dell'apparecchio di controllo.

191) Si possono prevedere altri avvisi, purché non confondano i conducenti in relazione a quelli sopra definiti.

3.18 **Trasferimento di dati a un dispositivo esterno**

192) L'apparecchio di controllo deve essere in grado di trasferire su richiesta i dati contenuti nella sua memoria o in una carta del conducente ad un dispositivo di memorizzazione esterno attraverso il connettore di taratura/trasferimento. L'apparecchio di controllo deve aggiornare i dati contenuti nella carta prima di iniziare il trasferimento.

▼B

193) Inoltre, a titolo facoltativo, in qualsiasi modalità di funzionamento l'apparecchio di controllo può trasferire i dati tramite qualsiasi altro mezzo ad un'impresa autenticata attraverso questo canale. In tal caso, al trasferimento si applicano i diritti di accesso ai dati del modo azienda.

194) Il trasferimento di dati non deve modificare o cancellare i dati memorizzati.

195) L'interfaccia elettrica del connettore di taratura/trasferimento è specificata nell'appendice 6.

196) I protocolli di trasferimento sono specificati nell'appendice 7.

3.19 **Comunicazione remota per controlli su strada mirati**

197) Quando l'accensione è inserita, l'unità elettronica di bordo deve memorizzare ogni 60 secondi nel dispositivo di comunicazione remota i dati più recenti necessari ai fini dei controlli su strada mirati. Tali dati devono essere criptati e firmati come specificato nelle appendici 11 e 14.

198) I dati da controllare a distanza devono essere resi disponibili a lettori di comunicazione remota attraverso una comunicazione senza fili, come specificato nell'appendice 14.

199) I dati necessari ai fini dei controlli su strada mirati devono riguardare:

— l'ultimo tentativo di violazione della sicurezza,

— l'interruzione più lunga dell'alimentazione di energia,

— guasto del sensore,

— errore dei dati di movimento,

— dati contrastanti sul movimento del veicolo,

— guida in assenza di una carta valida,

— inserimento della carta durante la guida,

— dati relativi alla regolazione dell'ora,

— dati relativi alla taratura, comprese le date delle ultime due registrazioni di tarature memorizzate,

— numero d'immatricolazione del veicolo,

— velocità registrata dal tachigrafo.

3.20 **Trasmissione di dati ad altri dispositivi esterni**

200) L'apparecchio di controllo può anche essere munito di interfacce standardizzate che consentano di usare i dati registrati o generati dal tachigrafo nel modo funzionamento o taratura mediante un dispositivo esterno.

Nell'appendice 13 è specificata e standardizzata un'interfaccia ITS opzionale. Altre interfacce simili possono coesistere, purché siano pienamente conformi ai requisiti dell'appendice 13 in termini di elenco minimo dei dati, sicurezza e consenso del conducente.

I seguenti requisiti si applicano ai dati ITS resi disponibili mediante tale interfaccia:

— tali dati sono una serie di dati esistenti scelti dal dizionario di dati del tachigrafo (appendice 1),

▼B

— un sottoinsieme di tali dati scelti è contrassegnato «dati personali»,

— il sottoinsieme «dati personali» è disponibile solo se è abilitato il consenso verificabile del conducente, con cui egli accetta che i propri dati personali possano lasciare la rete del veicolo,

— in qualsiasi momento il consenso del conducente può essere abilitato o disabilitato con i comandi del menù, purché la carta del conducente sia inserita,

— l'insieme e il sottoinsieme di dati sono trasmessi tramite protocollo senza fili Bluetooth nel raggio della cabina del veicolo, con una frequenza di aggiornamento di 1 minuto,

— l'abbinamento del dispositivo esterno con l'interfaccia ITS è protetto da un PIN dedicato e casuale di almeno 4 cifre, registrate e disponibili mediante il dispositivo di visualizzazione di ciascuna unità elettronica di bordo,

— in ogni caso, la presenza dell'interfaccia ITS non deve perturbare o pregiudicare il corretto funzionamento e la sicurezza dell'unità elettronica di bordo.

Si possono trasmettere anche altri dati in aggiunta all'insieme di dati esistenti scelti, considerato l'elenco minimo, a condizione che tali dati non si possano considerare dati personali.

L'apparecchio di controllo deve notificare il consenso del conducente agli altri dispositivi esterni.

Quando l'accensione del veicolo è inserita, tali dati devono essere trasmessi costantemente.

201) Il tachigrafo può continuare ad essere munito dell'interfaccia del collegamento seriale, come specificato nell'allegato 1B del regolamento (CEE) n. 3821/85, come modificato da ultimo, per garantire la compatibilità con le versioni precedenti. In ogni caso, il consenso del conducente è comunque necessario qualora siano trasmessi dati personali.

3.21 **Taratura**

202) La funzione di taratura deve consentire:

— l'accoppiamento automatico del sensore di movimento alla VU,

— l'accoppiamento automatico del dispositivo GNSS esterno alla VU, se del caso,

— l'adattamento digitale della costante dell'apparecchio di controllo (k) al coefficiente caratteristico del veicolo (w),

— la regolazione dell'ora corrente entro il periodo di validità della carta dell'officina inserita,

— la regolazione del valore corrente dell'odometro,

— l'aggiornamento dei dati di identificazione del sensore di movimento memorizzati nella memoria di dati,

— l'aggiornamento, se del caso, dei dati di identificazione del dispositivo GNSS esterno memorizzati nella memoria di dati,

▼B

— l'aggiornamento dei tipi e degli identificativi di tutti i sigilli apposti,

— l'aggiornamento o la conferma di altri parametri noti all'apparecchio di controllo: identificazione del veicolo, w, l, dimensioni degli pneumatici e regolazione del limitatore di velocità, se applicabile.

203) Inoltre, la funzione di taratura deve consentire di eliminare l'utilizzo delle carte tachigrafiche di prima generazione nell'apparecchio di controllo, purché siano soddisfatte le condizioni di cui all'appendice 15.

204) L'abbinamento del sensore di movimento alla VU deve prevedere almeno:

— l'aggiornamento dei dati di montaggio del sensore di movimento in esso contenuti (all'occorrenza),

— la copia, nella memoria di dati della VU, dei dati di identificazione del sensore necessari.

205) L'accoppiamento del dispositivo GNSS esterno alla VU deve prevedere almeno:

— l'aggiornamento dei dati di montaggio del dispositivo GNSS esterno in esso contenuti (all'occorrenza),

— la copia, nella memoria di dati della VU, dei dati di identificazione del dispositivo GNSS esterno necessari, compreso il numero di serie del dispositivo GNSS esterno.

L'accoppiamento deve essere seguito dalla verifica delle informazioni sulla posizione del GNSS.

206) La funzione di taratura deve essere in grado di immettere i dati necessari, attraverso il connettore di taratura/trasferimento, in base al protocollo di taratura definito nell'appendice 8. La funzione di taratura può anche immettere i dati necessari attraverso altri mezzi.

3.22 **Verifica della taratura su strada**

207) La funzione di verifica della taratura su strada deve consentire di leggere il numero di serie del sensore di movimento (eventualmente incorporato nell'adattatore) e il numero di serie del dispositivo GNSS esterno (se del caso), collegati all'unità elettronica di bordo, al momento della richiesta.

208) Tale lettura deve essere possibile almeno sul dispositivo di visualizzazione dell'unità elettronica di bordo con i comandi dei menù.

209) La funzione di verifica della taratura su strada deve anche consentire di controllare la selezione della modalità I/O della linea dei segnali I/O di taratura specificata nell'appendice 6, tramite l'interfaccia della linea K. A ciò si deve provvedere tramite la sessione di regolazione ECU, come specificato nell'appendice 8, Sezione 7 «Controllo degli impulsi di prova — Unità funzionale di controllo dei segnali di entrata/uscita».

3.23 **Regolazione dell'ora**

210) La funzione di regolazione dell'ora deve consentire di regolare automaticamente l'ora corrente. Nell'apparecchio di controllo si devono usare due fonti di misurazione del tempo per regolare l'ora: 1) l'orologio interno della VU); 2) il ricevitore GNSS.

▼B

211) Le impostazioni dell'ora dell'orologio interno della VU devono essere automaticamente ri-regolate ad intervalli di 12 ore al massimo. Se allo scadere dell'intervallo il segnale GNSS non è disponibile, l'impostazione dell'ora deve avvenire non appena la VU può accedere ad un orario valido fornito dal ricevitore GNSS, secondo le condizioni di accensione del veicolo. Il riferimento temporale per l'impostazione automatica dell'ora dell'orologio interno della VU deve essere costituito dal ricevitore GNSS. Un'anomalia «dati contrastanti sull'ora» deve attivarsi quando l'ora corrente si discosta di oltre un (1) minuto dalle informazioni sull'ora fornite dal ricevitore GNSS.

212) La funzione di regolazione dell'ora deve anche consentire la regolazione dell'ora corrente in modo mirato, nel modo taratura.

3.24 **Caratteristiche prestazionali**

213) L'unità elettronica di bordo deve essere in grado di funzionare correttamente nell'intervallo di temperatura compreso tra – 20 °C e 70 °C, il dispositivo GNSS esterno nell'intervallo di temperatura compreso tra – 20 °C e 70 °C e il sensore di movimento nell'intervallo di temperatura compreso tra – 40 °C e 135 °C. Il contenuto della memoria di dati deve conservarsi fino alla temperatura minima di – 40 °C.

214) Il tachigrafo deve essere in grado di funzionare correttamente nell'intervallo di umidità compreso tra 10 % e 90 %.

215) I sigilli utilizzati nel tachigrafo intelligente devono resistere alle stesse condizioni applicabili ai componenti del tachigrafo cui sono apposti.

216) L'apparecchio di controllo deve essere protetto contro la sovratensione, l'inversione di polarità dell'alimentazione e i corto circuiti.

217) I sensori di movimento:

— devono reagire a un campo magnetico che disturbi il rilevamento dei dati di movimento del veicolo. In queste circostanze, l'unità elettronica di bordo del veicolo deve registrare e memorizzare un guasto del sensore (requisito 88); oppure

— devono disporre di un elemento di rilevazione protetto dai campi magnetici o immune agli stessi.

218) L'apparecchio di controllo e il dispositivo GNSS esterno devono essere conformi al regolamento internazionale UNECE n. 10 e devono essere protetti contro le scariche elettrostatiche ed i transitori.

3.25 **Materiali**

219) Tutti gli elementi costitutivi dell'apparecchio di controllo devono essere realizzati con materiali dotati di stabilità e di resistenza meccanica sufficienti e con caratteristiche elettriche e magnetiche stabili.

220) Per le normali condizioni di impiego, tutti gli elementi interni dell'apparecchio devono essere protetti contro l'umidità e la polvere.

221) L'unità elettronica di bordo e il dispositivo GNSS esterno devono soddisfare il grado di protezione IP 40 e il sensore di movimento deve soddisfare il grado di protezione IP 64, secondo la norma IEC 60529:1989 comprese A1:1999 e A2:2013.

222) L'apparecchio di controllo deve essere conforme alle specifiche tecniche applicabili in materia di ergonomia.

▼B

223) L'apparecchio di controllo deve essere protetto contro i danni accidentali.

3.26 **Iscrizioni**

224) Se l'apparecchio di controllo visualizza il valore dell'odometro e la velocità, sul dispositivo di visualizzazione devono figurare le seguenti iscrizioni:

— in prossimità della cifra che indica la distanza, l'unità di misura della distanza espressa dal simbolo «km»,

— in prossimità della cifra che indica la velocità, l'indicazione «km/h».

L'apparecchio di controllo deve inoltre consentire la visualizzazione della velocità in miglia all'ora, nel qual caso l'unità di misura della velocità sarà espressa dall'indicazione «mph». L'apparecchio di controllo deve inoltre consentire la visualizzazione della distanza in miglia, nel qual caso l'unità di misura della distanza sarà espressa dall'indicazione «mi».

225) Una targhetta segnaletica deve essere affissa ad ogni componente distinto dell'apparecchio di controllo e deve riportare le seguenti indicazioni:

— nome ed indirizzo del fabbricante dell'apparecchio,

— codice componente del fabbricante e anno di fabbricazione dell'apparecchio,

— numero di serie dell'apparecchio,

— marchio di omologazione del tipo di apparecchio.

226) Qualora lo spazio fisico non sia sufficiente per riportare tutte le indicazioni summenzionate, sulla targhetta segnaletica devono figurare almeno: il nome o il logo del fabbricante e il codice componente dell'apparecchio.

4 REQUISITI DI COSTRUZIONE E FUNZIONAMENTO DELLE CARTE TACHIGRAFICHE

4.1 **Dati visibili**

Il lato anteriore della carta deve recare:

227) le diciture «Carta del conducente» o «Carta di controllo» o «Carta dell'officina» o «Carta dell'azienda» stampati in carattere maiuscolo nella lingua o nelle lingue ufficiali dello Stato membro che rilascia la carta, a seconda del tipo di carta;

228) il nome dello Stato membro che rilascia la carta (facoltativo);

229) il segno distintivo dello Stato membro che rilascia la carta, stampato in negativo in un rettangolo azzurro e circondato da dodici stelle gialle. I segni distintivi sono i seguenti:

B	Belgio	LV	Lettonia
BG	Bulgaria	L	Lussemburgo
CZ	Repubblica ceca	LT	Lituania
CY	Cipro	M	Malta
DK	Danimarca	NL	Paesi Bassi
D	Germania	A	Austria
EST	Estonia	PL	Polonia

▼B

GR	Grecia	P RO SK SLO	Portogallo Romania Slovacchia Slovenia
E	Spagna	FIN	Finlandia
F HR H	Francia Croazia Ungheria	S	Svezia
IRL	Irlanda	UK	Regno Unito
I	Italia		

230) le informazioni specifiche della carta, nell'ordine seguente:

	Carta del conducente	Carta di controllo	Carta dell'azienda o carta dell'officina
1.	cognome del conducente	denominazione dell'organismo di controllo	denominazione dell'impresa o dell'officina
2.	nome/i del conducente	cognome del controllore (se pertinente)	cognome del titolare della carta (se pertinente)
3.	data di nascita del conducente	nome/i del controllore (se pertinente)	nome/i del titolare della carta (se pertinente)
4.a	data di inizio validità della carta		
4.b	data di fine validità della carta		
4.c	denominazione dell'autorità che rilascia la carta (può essere stampata sul retro);		
4.d	un numero diverso da quello di cui alla voce 5, a fini amministrativi (facoltativo);		
5.a	numero della patente di guida (alla data di rilascio della carta del conducente)	—	—
5.b	numero della carta		
6.	fotografia del conducente	fotografia del controllore (facoltativa)	fotografia dell'installatore (facoltativa)
7.	firma del titolare (facoltativa)		
8.	luogo di residenza abituale o indirizzo postale del titolare (facoltativo)	indirizzo postale dell'organismo di controllo	indirizzo postale dell'azienda o dell'officina

231) le date devono essere indicate nel formato «gg/mm/aaaa» o «gg.mm.aaaa» (giorno, mese, anno).

Il retro della carta deve recare:

232) la spiegazione delle voci numerate che appaiono sul lato anteriore della carta;

▼B

233) se del caso e con l'assenso specifico scritto del titolare, anche altre informazioni che non si riferiscono alla gestione della carta, purché tale aggiunta non modifichi in alcun modo l'impiego del modello come carta tachigrafica.

234) Le carte tachigrafiche devono essere stampate con i seguenti colori di fondo predominanti:

— carta del conducente: bianco,

— carta di controllo: blu,

— carta dell'officina: rosso,

— carta dell'azienda: giallo.

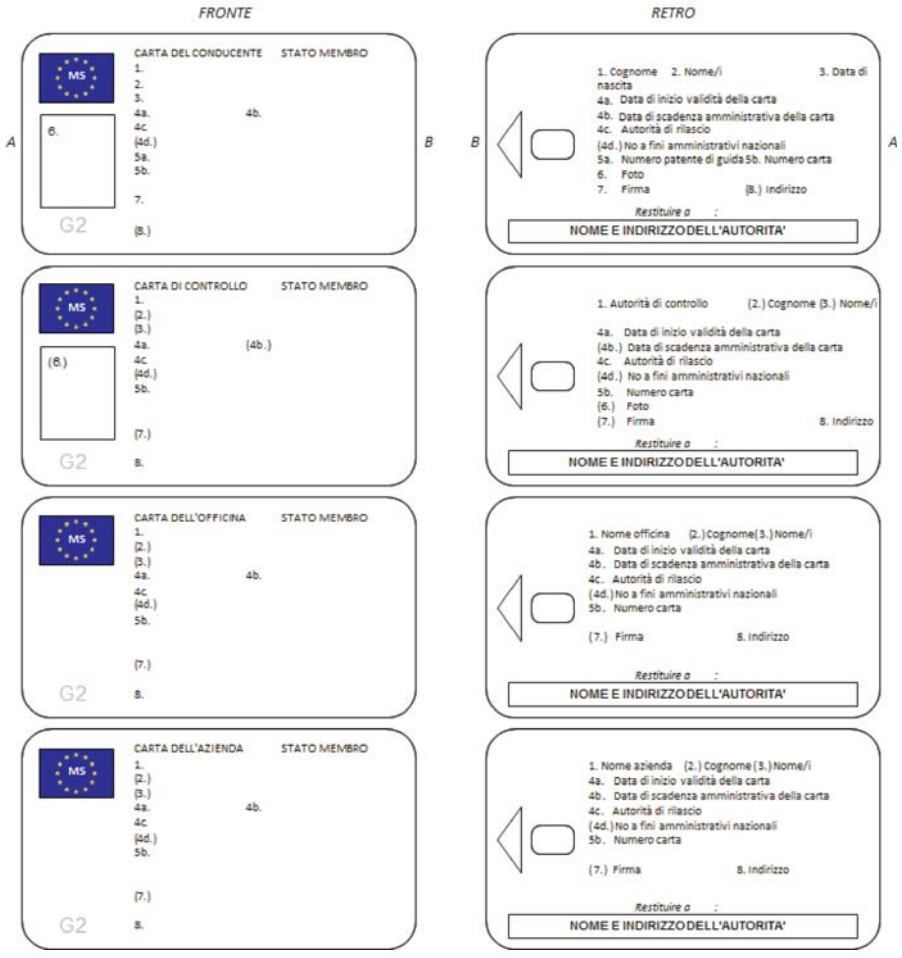
235) Le carte tachigrafiche devono avere almeno le caratteristiche seguenti ai fini della protezione contro la falsificazione e la manomissione:

— stampa policroma del fondo di sicurezza finemente arabescato,

— nell'area della foto, sovrapposizione del fondo di sicurezza e della fotografia,

— almeno una linea bicromatica microstampata.

MODELLO DI CARTE TACHIGRAFICHE DELL'UE



▼B

236) Previa consultazione della Commissione, gli Stati membri possono aggiungere colori o iscrizioni, quali simboli nazionali e caratteristiche di sicurezza, fatte salve le altre disposizioni del presente allegato.

237) Le carte temporanee di cui all'articolo 26, paragrafo 4, del regolamento (UE) n. 165/2014 devono essere conformi alle disposizioni del presente allegato.

4.2 **Sicurezza**

La sicurezza del sistema è intesa a proteggere l'integrità e l'autenticità dei dati scambiati tra le carte e l'apparecchio di controllo e l'integrità e l'autenticità dei dati trasferiti dalle carte, a consentire determinate operazioni di scrittura sulle carte solo all'apparecchio di controllo, a decriptare alcuni dati, ad escludere ogni possibilità di falsificazione dei dati memorizzati sulle carte, ad impedire la manomissione e a rilevarne eventuali tentativi.

238) Al fine di garantire la sicurezza del sistema, le carte tachigrafiche devono soddisfare i requisiti di sicurezza specificati nelle appendici 10 e 11.

239) Le carte tachigrafiche devono poter essere lette da altri apparecchi, come i personal computer.

4.3 **Norme**

240) Le carte tachigrafiche devono essere conformi alle norme seguenti:

— ISO/IEC 7810 Carte di identificazione — Caratteristiche fisiche,

— ISO/IEC 7816 Carte di identificazione — Carte a circuiti integrati:

  — Parte 1: Caratteristiche fisiche,

  — Parte 2: Dimensioni e posizione dei contatti (ISO/IEC 7816-2:2007),

  — Parte 3: Interfaccia elettrica e protocolli di trasmissione (ISO/IEC 7816-3:2006),

  — Parte 4: Organizzazione, sicurezza e comandi per gli scambi (ISO/IEC 7816-4:2013 + Cor 1:2014),

  — Parte 6: Elementi di dati interindustriali per gli scambi (ISO/IEC 7816-6:2004 + Cor 1:2006),

  — Parte 8: Comandi per le operazioni di sicurezza (ISO/IEC 7816-8:2004).

— Le carte tachigrafiche devono essere sottoposte a prova in conformità alla norma ISO/IEC 10373-3:2010 Carte di identificazione — Metodi di prova — Parte 3: Carte a circuiti integrati con contatti e relative interfacce.

4.4 **Specifiche ambientali ed elettriche**

241) Le carte tachigrafiche devono essere in grado di funzionare correttamente in tutte le condizioni climatiche abituali nel territorio della Comunità e almeno nell'intervallo di temperatura compreso tra – 25 °C e + 70 °C, con picchi occasionali fino a + 85 °C, dove per «occasionale» s'intende non superiore a 4 ore per volta e non superiore a 100 volte nell'intero periodo di durata della carta.

242) Le carte devono poter funzionare correttamente con un'umidità compresa tra 10 e 90 %.

▼B

243) Le carte tachigrafiche devono essere in grado di funzionare correttamente per un periodo di cinque anni, se impiegate nel rispetto delle specifiche ambientali ed elettriche.

244) Durante il funzionamento, le carte tachigrafiche devono essere conformi al regolamento UNECE n. 10, relativo alla compatibilità elettromagnetica, e devono essere protette contro le scariche elettrostatiche.

4.5 **Memorizzazione dei dati**

Agli effetti del presente punto:

— se non diversamente specificato, i tempi sono registrati con una risoluzione di un minuto,

— i valori dell'odometro sono registrati con una risoluzione di un chilometro,

— le velocità sono registrate con una risoluzione di 1 km/h,

— le posizioni (latitudini e longitudini) sono registrate in gradi e minuti, con una risoluzione di 1/10 di minuto.

Le funzioni, i comandi e le strutture logiche delle carte tachigrafiche, che soddisfano i requisiti di memorizzazione dei dati, sono specificati nell'appendice 2.

Se non diversamente specificato, la memorizzazione dei dati nelle carte tachigrafiche deve essere organizzata in modo che i nuovi dati sostituiscano quelli più datati, nel caso in cui lo spazio della memoria previsto per quelle registrazioni specifiche sia esaurito.

245) Il presente punto specifica la capacità minima di memorizzazione per i file di dati destinati alle diverse applicazioni. Le carte tachigrafiche devono essere in grado di indicare all'apparecchio di controllo la capacità effettiva di memorizzazione di tali file di dati.

246) Gli eventuali dati supplementari che possono essere memorizzati nelle carte tachigrafiche, relativi ad altre applicazioni eventualmente supportate dalla carta, devono essere memorizzati in conformità alla direttiva 95/46/CE, alla direttiva 2002/58/CE e all'articolo 7 del regolamento (UE) n. 165/2014.

247) Ogni file principale (MF) di ciascuna carta tachigrafica deve contenere fino a cinque file elementari (EF), ai fini della gestione della carta e dell'identificazione dell'applicazione e del chip, e due file dedicati (DF):

— DF Tachograph, che contiene l'applicazione accessibile alle unità elettroniche di bordo di prima generazione, che è presente anche nelle carte tachigrafiche di prima generazione,

— DF Tachograph_G2, che contiene l'applicazione accessibile solo alle unità elettroniche di bordo di seconda generazione, che è presente solo nelle carte tachigrafiche di seconda generazione.

Informazioni dettagliate sulla struttura delle carte tachigrafiche sono riportate nell'appendice 2.

4.5.1 *File elementari per l'identificazione e la gestione della carta*

4.5.2 *Identificazione della carta a circuito integrato*

248) Le carte tachigrafiche devono essere in grado di memorizzare i seguenti dati di identificazione delle carte intelligenti:

— arresto dell'orologio,

▼B

— numero di serie della carta (compresi i riferimenti di fabbricazione),

— numero di omologazione della carta,

— identificazione personalizzata della carta (ID),

— identificazione dell'assemblatore della carta,

— identificativo del circuito integrato.

4.5.2.1 Identificazione del chip

249) Le carte tachigrafiche devono essere in grado di memorizzare i seguenti dati di identificazione del circuito integrato:

— numero di serie del circuito integrato,

— riferimenti di fabbricazione del circuito integrato.

4.5.2.2 DIR (presente solo nelle carte tachigrafiche di seconda generazione)

250) Le carte tachigrafiche devono essere in grado di memorizzare gli oggetti dei dati di identificazione dell'applicazione specificati nell'appendice 2.

4.5.2.3 Informazioni ATR (opzionali, presenti solo nelle carte tachigrafiche di seconda generazione)

251) Le carte tachigrafiche devono essere in grado di memorizzare il seguente oggetto di dati informativi di lunghezza estesa:

— nel caso in cui la carta tachigrafica supporti i campi di lunghezza estesa, l'oggetto di dati informativi di lunghezza estesa specificato nell'appendice 2.

4.5.2.4 Informazioni di lunghezza estesa (opzionali, presenti solo nelle carte tachigrafiche di seconda generazione)

252) Le carte tachigrafiche devono essere in grado di memorizzare i seguenti oggetti di dati informativi di lunghezza estesa:

— nel caso in cui la carta tachigrafica supporti i campi di lunghezza estesa, gli oggetti di dati informativi di lunghezza estesa specificati nell'appendice 2.

4.5.3 *Carta del conducente*

4.5.3.1 Applicazione del tachigrafo (accessibile alle unità elettroniche di bordo di prima e seconda generazione)

4.5.3.1.1 Identificazione dell'applicazione

253) La carta del conducente deve essere in grado di memorizzare i seguenti dati di identificazione dell'applicazione:

— identificazione dell'applicazione del tachigrafo,

— identificazione del tipo di carta tachigrafica.

4.5.3.1.2 Chiavi e certificati

254) La carta del conducente deve essere in grado di memorizzare una serie di chiavi crittografiche e di certificati, come specificato nell'appendice 11, parte A.

▼B

4.5.3.1.3 Identificazione della carta

255) La carta del conducente deve essere in grado di memorizzare i seguenti dati di identificazione della carta:

— numero della carta,

— Stato membro di rilascio, denominazione dell'autorità di rilascio, data di rilascio,

— data di inizio validità della carta, data di scadenza della carta.

4.5.3.1.4 Identificazione del titolare della carta

256) La carta del conducente deve essere in grado di memorizzare i seguenti dati di identificazione del titolare:

— cognome del titolare,

— nome/i del titolare,

— data di nascita,

— lingua abituale.

4.5.3.1.5 Trasferimento dei dati della carta

257) La carta del conducente deve essere in grado di memorizzare i dati seguenti relativi al trasferimento dei dati della carta:

— data e ora dell'ultimo trasferimento di dati della carta (a fini diversi da quelli di controllo).

258) La carta del conducente deve essere in grado di conservare una di tali registrazioni.

4.5.3.1.6 Informazioni sulla patente di guida

259) La carta del conducente deve essere in grado di memorizzare i seguenti dati relativi alla patente di guida:

— Stato membro di rilascio, denominazione dell'autorità di rilascio,

— numero della patente di guida (alla data di rilascio della carta).

4.5.3.1.7 Dati relativi alle anomalie

Agli effetti del presente punto, l'ora deve essere memorizzata con una risoluzione di 1 secondo.

260) La carta del conducente deve essere in grado di memorizzare i dati relativi alle anomalie seguenti, rilevate dall'apparecchio di controllo a carta inserita:

— sovrapposizione di orari (se questa carta è la causa dell'anomalia),

— inserimento della carta durante la guida (se questa carta è l'oggetto dell'anomalia),

— chiusura errata ultima sessione carta (se questa carta è l'oggetto dell'anomalia),

— interruzione dell'alimentazione di energia,

— errore dei dati di movimento,

— tentativi di violazione della sicurezza.

261) Per tali anomalie, la carta del conducente deve essere in grado di memorizzare i dati seguenti:

— codice dell'anomalia,

— data e ora di inizio dell'anomalia (o di inserimento della carta se l'anomalia era in atto in tale momento),

▼B

— data e ora di termine dell'anomalia (o di estrazione della carta se l'anomalia era in atto in tale momento),

— VRN e Stato membro di immatricolazione del veicolo in cui si è verificata l'anomalia.

Nota: per l'anomalia «Sovrapposizione di orari»:

— la data e l'ora di inizio dell'anomalia devono corrispondere alla data e all'ora di estrazione della carta dal veicolo precedente,

— la data e l'ora di termine dell'anomalia devono corrispondere alla data e all'ora di inserimento della carta nel veicolo in uso,

— i dati relativi al veicolo devono corrispondere al veicolo in uso su cui si verifica l'anomalia.

Nota: per l'anomalia «Chiusura errata ultima sessione carta»:

— la data e l'ora di inizio dell'anomalia devono corrispondere alla data e all'ora di inserimento della carta per la sessione chiusa in modo errato,

— la data e l'ora di termine dell'anomalia devono corrispondere alla data e all'ora di inserimento della carta della sessione durante la quale è stata rilevata l'anomalia (sessione in corso),

— i dati relativi al veicolo devono corrispondere al veicolo in cui la sessione è stata chiusa in modo errato.

262) La carta del conducente deve essere in grado di memorizzare i dati relativi alle sei anomalie più recenti di ciascun tipo (vale a dire 36 anomalie).

4.5.3.1.8 Dati relativi ai guasti

Agli effetti del presente punto, l'ora deve essere registrata con una risoluzione di 1 secondo.

263) La carta del conducente deve essere in grado di memorizzare i dati relativi ai guasti seguenti, rilevati dall'apparecchio di controllo a carta inserita:

— guasto della carta (se questa carta è l'oggetto del guasto),

— guasto dell'apparecchio di controllo.

264) Per tali guasti, la carta del conducente deve essere in grado di memorizzare i dati seguenti:

— codice di guasto,

— data e ora di inizio del guasto (o di inserimento della carta se il guasto era in atto in tale momento),

— data e ora di termine del guasto (o di estrazione della carta se il guasto era in atto in tale momento),

— VRN e Stato membro di immatricolazione del veicolo in cui si è verificato il guasto.

265) La carta del conducente deve essere in grado di memorizzare i dati relativi ai dodici guasti più recenti di ciascun tipo (vale a dire 24 guasti).

▼B

4.5.3.1.9 Dati relativi all'attività del conducente

266) La carta del conducente deve essere in grado di memorizzare, per ciascun giorno di calendario in cui viene usata o ogniqualvolta il conducente inserisca manualmente un'attività, i dati seguenti:

— la data,

— un contatore di presenza giornaliera (aumentato di un'unità per ogni giorno di calendario in cui la carta viene usata),

— la distanza totale percorsa dal conducente durante tale giorno,

— la condizione del conducente alle 00h00,

— ad ogni cambio di attività del conducente e/o cambio di condizione di guida e/o inserimento o estrazione della carta:

— la condizione di guida (EQUIPAGGIO, SINGOLA),

— la sede (slot) (CONDUCENTE, SECONDO CONDUCENTE),

— la condizione della carta (INSERITA, NON INSERITA),

— l'attività (GUIDA, DISPONIBILITÀ, LAVORO, INTERRUZIONE/RIPOSO),

— l'ora del cambio.

267) La memoria della carta del conducente deve essere in grado di conservare i dati relativi all'attività del conducente per almeno 28 giorni (l'attività media di un conducente è intesa come 93 cambi di attività al giorno).

268) I dati elencati ai requisiti 261, 264 e 266 devono essere memorizzati in modo da consentire il reperimento delle attività nell'ordine in cui hanno avuto luogo, anche in caso di sovrapposizione di orari.

4.5.3.1.10 Dati relativi ai veicoli impiegati

269) La carta del conducente deve essere in grado di memorizzare, per ogni giorno di calendario in cui viene usata e per ogni periodo di impiego di un determinato veicolo in tale giorno (un periodo di impiego comprende tutti i cicli consecutivi di inserimento/estrazione della carta nel veicolo, dal punto di vista della singola carta), i dati seguenti:

— data e ora del primo impiego del veicolo (cioè il primo inserimento della carta per questo periodo di impiego del veicolo o 00h00 se il periodo di impiego è in corso in tale momento),

— valore dell'odometro del veicolo in tale momento,

— data e ora dell'ultimo impiego del veicolo (cioè l'ultima estrazione della carta per questo periodo di impiego del veicolo o 23h59 se il periodo di impiego è in corso in tale momento),

▼B

— valore dell'odometro del veicolo in tale momento,

— VRN e Stato membro di immatricolazione del veicolo.

270) La carta del conducente deve essere in grado di memorizzare almeno 84 di tali registrazioni.

4.5.3.1.11 Luogo in cui inizia e/o termina il periodo di lavoro giornaliero

271) La carta del conducente deve essere in grado di memorizzare i dati seguenti relativi al luogo in cui inizia e/o termina il periodo di lavoro giornaliero, inseriti dal conducente:

— la data e l'ora dell'immissione (o la data/ora relativa all'immissione, se questa viene effettuata durante la procedura di immissione manuale),

— il tipo di immissione (inizio o termine, condizione di immissione),

— il paese e la regione inseriti,

— il valore dell'odometro del veicolo.

272) La memoria della carta del conducente deve essere in grado di conservare almeno 42 coppie di tali registrazioni.

4.5.3.1.12 Dati relativi alla sessione della carta

273) La carta del conducente deve essere in grado di memorizzare i dati relativi al veicolo che ha aperto la sessione in corso:

— data e ora di apertura della sessione (cioè d'inserimento della carta) con una risoluzione di un secondo,

— VRN e Stato membro di immatricolazione.

4.5.3.1.13 Dati relativi alle attività di controllo

274) La carta del conducente deve essere in grado di memorizzare i dati seguenti, relativi alle attività di controllo:

— data e ora del controllo,

— numero della carta di controllo e Stato membro di rilascio,

— tipo di controllo [visualizzazione e/o stampa e/o trasferimento dati VU e/o trasferimento dati carta (cfr. nota)],

— periodo trasferito, in caso di trasferimento,

— VRN e Stato membro di immatricolazione del veicolo in cui è stato effettuato il controllo.

Nota: il trasferimento dei dati della carta è registrato soltanto se viene effettuato attraverso un apparecchio di controllo.

275) La carta del conducente deve essere in grado di conservare una di tali registrazioni.

4.5.3.1.14 Dati relativi a condizioni particolari

276) La carta del conducente deve essere in grado di memorizzare i dati seguenti, relativi a condizioni particolari immesse a carta inserita [in qualsiasi sede (slot)]:

— data e ora di immissione,

— tipo di condizione particolare.

▼B

277) La carta del conducente deve essere in grado di memorizzare almeno 56 di tali registrazioni.

4.5.3.2 Applicazione del tachigrafo di seconda generazione (non accessibile alle unità elettroniche di bordo di prima generazione)

4.5.3.2.1 Identificazione dell'applicazione

278) La carta del conducente deve essere in grado di memorizzare i seguenti dati di identificazione dell'applicazione:

— identificazione dell'applicazione del tachigrafo,

— identificazione del tipo di carta tachigrafica.

4.5.3.2.2 Chiavi e certificati

279) La carta del conducente deve essere in grado di memorizzare una serie di chiavi crittografiche e di certificati, come specificato nell'appendice 11, parte B.

4.5.3.2.3 Identificazione della carta

280) La carta del conducente deve essere in grado di memorizzare i seguenti dati di identificazione della carta:

— numero della carta,

— Stato membro di rilascio, denominazione dell'autorità di rilascio, data di rilascio,

— data di inizio validità della carta, data di scadenza della carta.

4.5.3.2.4 Identificazione del titolare della carta

281) La carta del conducente deve essere in grado di memorizzare i seguenti dati di identificazione del titolare:

— cognome del titolare,

— nome/i del titolare,

— data di nascita,

— lingua abituale.

4.5.3.2.5 Trasferimento dei dati della carta

282) La carta del conducente deve essere in grado di memorizzare i dati seguenti relativi al trasferimento dei dati della carta:

— data e ora dell'ultimo trasferimento di dati della carta (a fini diversi da quelli di controllo).

283) La carta del conducente deve essere in grado di conservare una di tali registrazioni.

4.5.3.2.6 Informazioni sulla patente di guida

284) La carta del conducente deve essere in grado di memorizzare i seguenti dati relativi alla patente di guida:

— Stato membro di rilascio, denominazione dell'autorità di rilascio,

— numero della patente di guida (alla data di rilascio della carta).

4.5.3.2.7 Dati relativi alle anomalie

Agli effetti del presente punto, l'ora deve essere memorizzata con una risoluzione di 1 secondo.

▼B

285) La carta del conducente deve essere in grado di memorizzare i dati relativi alle anomalie seguenti, rilevate dall'apparecchio di controllo a carta inserita:

— sovrapposizione di orari (se questa carta è la causa dell'anomalia),

— inserimento della carta durante la guida (se questa carta è l'oggetto dell'anomalia),

— chiusura errata ultima sessione carta (se questa carta è l'oggetto dell'anomalia),

— interruzione dell'alimentazione di energia,

— errore di comunicazione con il dispositivo di comunicazione remota,

— assenza di informazioni sulla posizione provenienti dal ricevitore GNSS,

— errore di comunicazione con il dispositivo GNSS esterno,

— errore dei dati di movimento,

— dati contrastanti sul movimento del veicolo,

— tentativi di violazione della sicurezza,

— dati contrastanti sull'ora.

286) Per tali anomalie, la carta del conducente deve essere in grado di memorizzare i dati seguenti:

— codice dell'anomalia,

— data e ora di inizio dell'anomalia (o di inserimento della carta se l'anomalia era in atto in tale momento),

— data e ora di termine dell'anomalia (o di estrazione della carta se l'anomalia era in atto in tale momento),

— VRN e Stato membro di immatricolazione del veicolo in cui si è verificata l'anomalia.

Nota: per l'anomalia «Sovrapposizione di orari»:

— la data e l'ora di inizio dell'anomalia devono corrispondere alla data e all'ora di estrazione della carta dal veicolo precedente,

— la data e l'ora di termine dell'anomalia devono corrispondere alla data e all'ora di inserimento della carta nel veicolo in uso,

— i dati relativi al veicolo devono corrispondere al veicolo in uso su cui si verifica l'anomalia.

Nota: per l'anomalia «Chiusura errata ultima sessione carta»:

— la data e l'ora di inizio dell'anomalia devono corrispondere alla data e all'ora di inserimento della carta per la sessione chiusa in modo errato,

— la data e l'ora di termine dell'anomalia devono corrispondere alla data e all'ora di inserimento della carta della sessione durante la quale è stata rilevata l'anomalia (sessione in corso),

▼B

— i dati relativi al veicolo devono corrispondere al veicolo in cui la sessione è stata chiusa in modo errato.

287) La carta del conducente deve essere in grado di memorizzare i dati relativi alle sei anomalie più recenti di ciascun tipo (vale a dire 66 anomalie).

4.5.3.2.8 Dati relativi ai guasti

Agli effetti del presente punto, l'ora deve essere registrata con una risoluzione di 1 secondo.

288) La carta del conducente deve essere in grado di memorizzare i dati relativi ai guasti seguenti, rilevati dall'apparecchio di controllo a carta inserita:

— guasto della carta (se questa carta è l'oggetto del guasto),

— guasto dell'apparecchio di controllo.

289) Per tali guasti, la carta del conducente deve essere in grado di memorizzare i dati seguenti:

— codice di guasto,

— data e ora di inizio del guasto (o di inserimento della carta se il guasto era in atto in tale momento),

— data e ora di termine del guasto (o di estrazione della carta se il guasto era in atto in tale momento),

— VRN e Stato membro di immatricolazione del veicolo in cui si è verificato il guasto.

290) La carta del conducente deve essere in grado di memorizzare i dati relativi ai dodici guasti più recenti di ciascun tipo (vale a dire 24 guasti).

4.5.3.2.9 Dati relativi all'attività del conducente

291) La carta del conducente deve essere in grado di memorizzare, per ciascun giorno di calendario in cui viene usata o ogniqualvolta il conducente inserisca manualmente un'attività, i dati seguenti:

— la data,

— un contatore di presenza giornaliera (aumentato di un'unità per ogni giorno di calendario in cui la carta viene usata),

— la distanza totale percorsa dal conducente durante tale giorno,

— la condizione del conducente alle 00h00,

— ad ogni cambio di attività del conducente e/o cambio di condizione di guida e/o inserimento o estrazione della carta:

— la condizione di guida (EQUIPAGGIO, SINGOLA),

— la sede (slot) (CONDUCENTE, SECONDO CONDUCENTE),

— la condizione della carta (INSERITA, NON INSERITA),

— l'attività (GUIDA, DISPONIBILITÀ, LAVORO, INTERRUZIONE/RIPOSO),

▼B

— l'ora del cambio.

292) La memoria della carta del conducente deve essere in grado di conservare i dati relativi all'attività del conducente per almeno 28 giorni (l'attività media di un conducente è intesa come 93 cambi di attività al giorno).

293) I dati elencati ai requisiti 286, 289 e 291 devono essere memorizzati in modo da consentire il reperimento delle attività nell'ordine in cui hanno avuto luogo, anche in caso di sovrapposizione di orari.

4.5.3.2.10 Dati relativi ai veicoli impiegati

294) La carta del conducente deve essere in grado di memorizzare, per ogni giorno di calendario in cui viene usata e per ogni periodo di impiego di un determinato veicolo in tale giorno (un periodo di impiego comprende tutti i cicli consecutivi di inserimento/estrazione della carta nel veicolo, dal punto di vista della singola carta), i dati seguenti:

— data e ora del primo impiego del veicolo (cioè il primo inserimento della carta per questo periodo di impiego del veicolo o 00h00 se il periodo di impiego è in corso in tale momento),

— valore dell'odometro del veicolo all'ora di tale primo impiego,

— data e ora dell'ultimo impiego del veicolo (cioè l'ultima estrazione della carta per questo periodo di impiego del veicolo o 23h59 se il periodo di impiego è in corso in tale momento),

— valore dell'odometro del veicolo all'ora di tale ultimo impiego,

— VRN e Stato membro di immatricolazione del veicolo,

— VIN del veicolo.

295) La carta del conducente deve essere in grado di memorizzare almeno 84 di tali registrazioni.

4.5.3.2.11 Luogo e posizione in cui inizia e/o termina il periodo di lavoro giornaliero

296) La carta del conducente deve essere in grado di memorizzare i dati seguenti relativi al luogo in cui inizia e/o termina il periodo di lavoro giornaliero, inseriti dal conducente:

— la data e l'ora dell'immissione (o la data/ora relativa all'immissione, se questa viene effettuata durante la procedura di immissione manuale),

— il tipo di immissione (inizio o termine, condizione di immissione),

— il paese e la regione inseriti,

— il valore dell'odometro del veicolo,

— la posizione del veicolo,

— l'accuratezza del GNSS, la data e l'ora in cui la posizione è stata determinata.

297) La memoria della carta del conducente deve essere in grado di conservare almeno 84 coppie di tali registrazioni.

▼B

4.5.3.2.12 Dati relativi alla sessione della carta

298) La carta del conducente deve essere in grado di memorizzare i dati relativi al veicolo che ha aperto la sessione in corso:

— data e ora di apertura della sessione (cioè d'inserimento della carta) con una risoluzione di un secondo,

— VRN e Stato membro di immatricolazione.

4.5.3.2.13 Dati relativi alle attività di controllo

299) La carta del conducente deve essere in grado di memorizzare i dati seguenti, relativi alle attività di controllo:

— data e ora del controllo,

— numero della carta di controllo e Stato membro di rilascio,

— tipo di controllo [visualizzazione e/o stampa e/o trasferimento dati VU e/o trasferimento dati carta (cfr. nota)],

— periodo trasferito, in caso di trasferimento,

— VRN e Stato membro di immatricolazione del veicolo in cui è stato effettuato il controllo.

Nota: i requisiti di sicurezza prevedono che il trasferimento dei dati della carta sia registrato soltanto se viene effettuato attraverso un apparecchio di controllo.

300) La carta del conducente deve essere in grado di conservare una di tali registrazioni.

4.5.3.2.14 Dati relativi a condizioni particolari

301) La carta del conducente deve essere in grado di memorizzare i dati seguenti, relativi a condizioni particolari immesse a carta inserita [in qualsiasi sede (slot)]:

— data e ora di immissione,

— tipo di condizione particolare.

302) La carta del conducente deve essere in grado di memorizzare almeno 56 di tali registrazioni.

4.5.3.2.15 Dati relativi alle unità elettroniche di bordo usate

303) La carta del conducente deve essere in grado di memorizzare i dati seguenti, relativi alle diverse unità elettroniche di bordo in cui è stata usata la carta:

— la data e l'ora d'inizio del periodo d'impiego dell'unità elettronica di bordo (cioè il primo inserimento della carta nell'unità elettronica di bordo per il periodo),

— il fabbricante dell'unità elettronica di bordo,

— il tipo di unità elettronica di bordo,

— il numero di versione del software dell'unità elettronica di bordo.

304) La carta del conducente deve essere in grado di memorizzare almeno 84 di tali registrazioni.

▼B

4.5.3.2.16 Dati relativi al luogo in cui si raggiungono le tre ore di guida ininterrotta

305) La carta del conducente deve essere in grado di memorizzare i seguenti dati relativi alla posizione del veicolo quando il periodo di guida continuo del conducente raggiunge un multiplo di tre ore:

— la data e l'ora in cui il periodo di guida continuo del titolare della carta raggiunge un multiplo di tre ore;

— la posizione del veicolo,

— l'accuratezza del GNSS, la data e l'ora in cui la posizione è stata determinata.

306) La carta del conducente deve essere in grado di memorizzare almeno 252 di tali registrazioni.

4.5.4 *Carta dell'officina*

4.5.4.1 Applicazione del tachigrafo (accessibile alle unità elettroniche di bordo di prima e seconda generazione)

4.5.4.1.1 Identificazione dell'applicazione

307) La carta dell'officina deve essere in grado di memorizzare i seguenti dati di identificazione dell'applicazione:

— identificazione dell'applicazione del tachigrafo,

— identificazione del tipo di carta tachigrafica.

4.5.4.1.2 Chiavi e certificati

308) La carta dell'officina deve essere in grado di memorizzare una serie di chiavi crittografiche e di certificati, come specificato nell'appendice 11, parte A.

309) La carta dell'officina deve essere in grado di memorizzare un numero di identificazione personale (codice PIN).

4.5.4.1.3 Identificazione della carta

310) La carta dell'officina deve essere in grado di memorizzare i seguenti dati di identificazione della carta:

— numero della carta,

— Stato membro di rilascio, denominazione dell'autorità di rilascio, data di rilascio,

— data di inizio validità della carta, data di scadenza della carta.

4.5.4.1.4 Identificazione del titolare della carta

311) La carta dell'officina deve essere in grado di memorizzare i seguenti dati di identificazione del titolare della carta:

— denominazione dell'officina,

— indirizzo dell'officina,

— cognome del titolare,

— nome/i del titolare,

— lingua abituale.

4.5.4.1.5 Trasferimento dei dati della carta

312) La carta dell'officina deve essere in grado di memorizzare un registro di dati del trasferimento dei dati della carta allo stesso modo della carta del conducente.

▼B

4.5.4.1.6 Dati relativi a taratura e regolazione dell'ora

313) La carta dell'officina deve essere in grado di conservare i dati relativi alle tarature e/o alle regolazioni dell'ora effettuate a carta inserita nell'apparecchio di controllo.

314) Ogni registrazione relativa alla taratura deve essere in grado di contenere i dati seguenti:

— scopo della taratura (attivazione, primo montaggio, montaggio, controllo periodico),

— identificazione del veicolo,

— parametri aggiornati o confermati (w, k, l, dimensioni degli pneumatici, regolazione del limitatore di velocità, odometro (vecchio e nuovo valore), data e ora (vecchio e nuovo valore),

— identificazione dell'apparecchio di controllo (codice componente della VU, numero di serie della VU, numero di serie del sensore di movimento).

315) La carta dell'officina deve essere in grado di memorizzare almeno 88 di tali registrazioni.

316) La carta dell'officina deve contenere un contatore che indichi il numero totale di tarature effettuate con la carta stessa.

317) La carta dell'officina deve contenere un contatore che indichi il numero di tarature effettuate a partire dall'ultimo trasferimento di dati della carta stessa.

4.5.4.1.7 Dati relativi ad anomalie e guasti

318) La carta dell'officina deve essere in grado di memorizzare i registri dei dati delle anomalie e dei guasti allo stesso modo della carta del conducente.

319) La carta dell'officina deve essere in grado di memorizzare i dati relativi alle ultime tre anomalie di ciascun tipo (cioè 18 anomalie) e agli ultimi sei guasti di ciascun tipo (cioè 12 guasti).

4.5.4.1.8 Dati relativi all'attività del conducente

320) La carta dell'officina deve essere in grado di memorizzare i dati relativi all'attività del conducente allo stesso modo della carta del conducente.

321) La carta dell'officina deve essere in grado di conservare tali dati per almeno 1 giorno di attività media del conducente.

4.5.4.1.9 Dati relativi ai veicoli impiegati

322) La carta dell'officina deve essere in grado di memorizzare i dati relativi ai veicoli impiegati allo stesso modo della carta del conducente.

323) La carta dell'officina deve essere in grado di memorizzare almeno 4 di tali registrazioni.

4.5.4.1.10 Dati relativi all'inizio e/o al termine del periodo di lavoro giornaliero

324) La carta dell'officina deve essere in grado di memorizzare i dati relativi all'inizio e/o al termine del periodo di lavoro giornaliero allo stesso modo della carta del conducente.

325) La carta dell'officina deve essere in grado di conservare almeno 3 coppie di tali registrazioni.

▼B

4.5.4.1.11 Dati relativi alla sessione della carta

326) La carta dell'officina deve essere in grado di memorizzare un registro di dati della sessione della carta allo stesso modo della carta del conducente.

4.5.4.1.12 Dati relativi alle attività di controllo

327) La carta dell'officina deve essere in grado di memorizzare i dati relativi alle attività di controllo allo stesso modo della carta del conducente.

4.5.4.1.13 Dati relativi a condizioni particolari

328) La carta dell'officina deve essere in grado di memorizzare i dati relativi a condizioni particolari allo stesso modo della carta del conducente.

329) La carta dell'officina deve essere in grado di memorizzare almeno 2 di tali registrazioni.

4.5.4.2 Applicazione del tachigrafo di seconda generazione (non accessibile alle unità elettroniche di bordo di prima generazione)

4.5.4.2.1 Identificazione dell'applicazione

330) La carta dell'officina deve essere in grado di memorizzare i seguenti dati di identificazione dell'applicazione:

— identificazione dell'applicazione del tachigrafo,

— identificazione del tipo di carta tachigrafica.

4.5.4.2.2 Chiavi e certificati

331) La carta dell'officina deve essere in grado di memorizzare una serie di chiavi crittografiche e di certificati, come specificato nell'appendice 11, parte B.

332) La carta dell'officina deve essere in grado di memorizzare un numero di identificazione personale (codice PIN).

4.5.4.2.3 Identificazione della carta

333) La carta dell'officina deve essere in grado di memorizzare i seguenti dati di identificazione della carta:

— numero della carta,

— Stato membro di rilascio, denominazione dell'autorità di rilascio, data di rilascio,

— data di inizio validità della carta, data di scadenza della carta.

4.5.4.2.4 Identificazione del titolare della carta

334) La carta dell'officina deve essere in grado di memorizzare i seguenti dati di identificazione del titolare della carta:

— denominazione dell'officina,

— indirizzo dell'officina,

— cognome del titolare,

— nome/i del titolare,

— lingua abituale.

4.5.4.2.5 Trasferimento dei dati della carta

335) La carta dell'officina deve essere in grado di memorizzare un registro di dati del trasferimento dei dati della carta allo stesso modo della carta del conducente.

▼B

4.5.4.2.6 Dati relativi a taratura e regolazione dell'ora

336) La carta dell'officina deve essere in grado di conservare i dati relativi alle tarature e/o alle regolazioni dell'ora effettuate a carta inserita nell'apparecchio di controllo.

337) Ogni registrazione relativa alla taratura deve essere in grado di contenere i dati seguenti:

— scopo della taratura (attivazione, primo montaggio, montaggio, controllo periodico),

— identificazione del veicolo,

— parametri aggiornati o confermati (w, k, l, dimensioni degli pneumatici, regolazione del limitatore di velocità, odometro (vecchio e nuovo valore), data e ora (vecchio e nuovo valore),

— identificazione dell'apparecchio di controllo (codice componente della VU, numero di serie della VU, numero di serie del sensore di movimento, numero di serie del dispositivo di comunicazione remota e numero di serie del dispositivo GNSS esterno, se applicabile),

— tipo e identificativo di tutti i sigilli apposti,

— capacità della VU di utilizzare carte tachigrafiche di prima generazione (attivata o meno).

338) La carta dell'officina deve essere in grado di memorizzare almeno 88 di tali registrazioni.

339) La carta dell'officina deve contenere un contatore che indichi il numero totale di tarature effettuate con la carta stessa.

340) La carta dell'officina deve contenere un contatore che indichi il numero di tarature effettuate a partire dall'ultimo trasferimento di dati della carta stessa.

4.5.4.2.7 Dati relativi ad anomalie e guasti

341) La carta dell'officina deve essere in grado di memorizzare i registri dei dati delle anomalie e dei guasti allo stesso modo della carta del conducente.

342) La carta dell'officina deve essere in grado di memorizzare i dati relativi alle ultime tre anomalie di ciascun tipo (cioè 33 anomalie) e agli ultimi sei guasti di ciascun tipo (cioè 12 guasti).

4.5.4.2.8 Dati relativi all'attività del conducente

343) La carta dell'officina deve essere in grado di memorizzare i dati relativi all'attività del conducente allo stesso modo della carta del conducente.

344) La carta dell'officina deve essere in grado di conservare tali dati per almeno 1 giorno di attività media del conducente.

4.5.4.2.9 Dati relativi ai veicoli impiegati

345) La carta dell'officina deve essere in grado di memorizzare i dati relativi ai veicoli impiegati allo stesso modo della carta del conducente.

346) La carta dell'officina deve essere in grado di memorizzare almeno 4 di tali registrazioni.

▼B

4.5.4.2.10 Dati relativi all'inizio e/o al termine del periodo di lavoro giornaliero

347) La carta dell'officina deve essere in grado di memorizzare i dati relativi all'inizio e/o al termine del periodo di lavoro giornaliero allo stesso modo della carta del conducente.

348) La carta dell'officina deve essere in grado di conservare almeno 3 coppie di tali registrazioni.

4.5.4.2.11 Dati relativi alla sessione della carta

349) La carta dell'officina deve essere in grado di memorizzare un registro di dati della sessione della carta allo stesso modo della carta del conducente.

4.5.4.2.12 Dati relativi alle attività di controllo

350) La carta dell'officina deve essere in grado di memorizzare i dati relativi alle attività di controllo allo stesso modo della carta del conducente.

4.5.4.2.13 Dati relativi alle unità elettroniche di bordo usate

351) La carta dell'officina deve essere in grado di memorizzare i dati seguenti, relativi alle diverse unità elettroniche di bordo in cui è stata usata la carta:

— la data e l'ora d'inizio del periodo d'impiego dell'unità elettronica di bordo (cioè il primo inserimento della carta nell'unità elettronica di bordo per il periodo),

— il fabbricante dell'unità elettronica di bordo,

— il tipo di unità elettronica di bordo,

— il numero di versione del software dell'unità elettronica di bordo.

352) La carta dell'officina deve essere in grado di memorizzare almeno 4 di tali registrazioni.

4.5.4.2.14 Dati relativi al luogo in cui si raggiungono le tre ore di guida ininterrotta

353) La carta dell'officina deve essere in grado di memorizzare i seguenti dati relativi alla posizione del veicolo quando il periodo di guida continuo del conducente raggiunge un multiplo di tre ore:

— la data e l'ora in cui il periodo di guida continuo del titolare della carta raggiunge un multiplo di tre ore;

— la posizione del veicolo,

— l'accuratezza del GNSS, la data e l'ora in cui la posizione è stata determinata.

354) La carta dell'officina deve essere in grado di memorizzare almeno 18 di tali registrazioni.

4.5.4.2.15 Dati relativi a condizioni particolari

355) La carta dell'officina deve essere in grado di memorizzare i dati relativi a condizioni particolari allo stesso modo della carta del conducente.

356) La carta dell'officina deve essere in grado di memorizzare almeno 2 di tali registrazioni.

▼B

4.5.5 *Carta di controllo*

4.5.5.1 Applicazione del tachigrafo (accessibile alle unità elettroniche di bordo di prima e seconda generazione)

4.5.5.1.1 Identificazione dell'applicazione

357) La carta di controllo deve essere in grado di memorizzare i seguenti dati di identificazione dell'applicazione:

— identificazione dell'applicazione del tachigrafo,

— identificazione del tipo di carta tachigrafica.

4.5.5.1.2 Chiavi e certificati

358) La carta di controllo deve essere in grado di memorizzare una serie di chiavi crittografiche e di certificati, come specificato nell'appendice 11, parte A.

4.5.5.1.3 Identificazione della carta

359) La carta di controllo deve essere in grado di memorizzare i seguenti dati di identificazione della carta:

— numero della carta,

— Stato membro di rilascio, denominazione dell'autorità di rilascio, data di rilascio,

— data di inizio validità della carta, data di scadenza della carta (se presente).

4.5.5.1.4 Identificazione del titolare della carta

360) La carta di controllo deve essere in grado di memorizzare i seguenti dati di identificazione del titolare:

— denominazione dell'organismo di controllo,

— indirizzo dell'organismo di controllo,

— cognome del titolare,

— nome/i del titolare,

— lingua abituale.

4.5.5.1.5 Dati relativi alle attività di controllo

361) La carta di controllo deve essere in grado di memorizzare i dati seguenti, relativi alle attività di controllo:

— data e ora del controllo,

— tipo di controllo (visualizzazione e/o stampa e/o trasferimento dati VU e/o trasferimento dati carta e/o verifica della taratura su strada),

— periodo cui si riferiscono i dati (se del caso),

— VRN e autorità di immatricolazione del veicolo controllato dello Stato membro,

— numero della carta e Stato membro di rilascio della carta del conducente controllata.

362) La carta di controllo deve essere in grado di conservare almeno 230 di tali registrazioni.

▼B

4.5.5.2 Applicazione del tachigrafo di seconda generazione (non accessibile alle unità elettroniche di bordo di prima generazione)

4.5.5.2.1 Identificazione dell'applicazione

363) La carta di controllo deve essere in grado di memorizzare i seguenti dati di identificazione dell'applicazione:

— identificazione dell'applicazione del tachigrafo,

— identificazione del tipo di carta tachigrafica.

4.5.5.2.2 Chiavi e certificati

364) La carta di controllo deve essere in grado di memorizzare una serie di chiavi crittografiche e di certificati, come specificato nell'appendice 11, parte B.

4.5.5.2.3 Identificazione della carta

365) La carta di controllo deve essere in grado di memorizzare i seguenti dati di identificazione della carta:

— numero della carta,

— Stato membro di rilascio, denominazione dell'autorità di rilascio, data di rilascio,

— data di inizio validità della carta, data di scadenza della carta (se presente).

4.5.5.2.4 Identificazione del titolare della carta

366) La carta di controllo deve essere in grado di memorizzare i seguenti dati di identificazione del titolare:

— denominazione dell'organismo di controllo,

— indirizzo dell'organismo di controllo,

— cognome del titolare,

— nome/i del titolare,

— lingua abituale.

4.5.5.2.5 Dati relativi alle attività di controllo

367) La carta di controllo deve essere in grado di memorizzare i dati seguenti, relativi alle attività di controllo:

— data e ora del controllo,

— tipo di controllo (visualizzazione e/o stampa e/o trasferimento dati VU e/o trasferimento dati carta e/o verifica della taratura su strada),

— periodo cui si riferiscono i dati (se del caso),

— VRN e autorità di immatricolazione del veicolo controllato dello Stato membro,

— numero della carta e Stato membro di rilascio della carta del conducente controllata.

368) La carta di controllo deve essere in grado di conservare almeno 230 di tali registrazioni.

▼B

4.5.6 *Carta dell'azienda*

4.5.6.1 Applicazione del tachigrafo (accessibile alle unità elettroniche di bordo di prima e seconda generazione)

4.5.6.1.1 Identificazione dell'applicazione

369) La carta dell'azienda deve essere in grado di memorizzare i seguenti dati di identificazione dell'applicazione:

— identificazione dell'applicazione del tachigrafo,

— identificazione del tipo di carta tachigrafica.

4.5.6.1.2 Chiavi e certificati

370) La carta dell'azienda deve essere in grado di memorizzare una serie di chiavi crittografiche e di certificati, come specificato nell'appendice 11, parte A.

4.5.6.1.3 Identificazione della carta

371) La carta dell'azienda deve essere in grado di memorizzare i seguenti dati di identificazione della carta:

— numero della carta,

— Stato membro di rilascio, denominazione dell'autorità di rilascio, data di rilascio,

— data di inizio validità della carta, data di scadenza della carta (se presente).

4.5.6.1.4 Identificazione del titolare della carta

372) La carta dell'azienda deve essere in grado di memorizzare i seguenti dati di identificazione del titolare:

— denominazione dell'azienda,

— indirizzo dell'azienda.

4.5.6.1.5 Dati relativi alle attività dell'impresa

373) La carta dell'azienda deve essere in grado di memorizzare i dati seguenti, relativi alle attività dell'impresa:

— data e ora dell'attività,

— tipo di attività (attivazione e/o disattivazione blocco VU e/o trasferimento dati VU e/o trasferimento dati carta),

— periodo cui si riferiscono i dati (se del caso),

— VRN e autorità di immatricolazione del veicolo dello Stato membro,

— numero della carta e Stato membro di rilascio (in caso di trasferimento dei dati della carta).

374) La carta dell'azienda deve essere in grado di conservare almeno 230 di tali registrazioni.

▼B

4.5.6.2 Applicazione del tachigrafo di seconda generazione (non accessibile alle unità elettroniche di bordo di prima generazione)

4.5.6.2.1 Identificazione dell'applicazione

375) La carta dell'azienda deve essere in grado di memorizzare i seguenti dati di identificazione dell'applicazione:

— identificazione dell'applicazione del tachigrafo,

— identificazione del tipo di carta tachigrafica.

4.5.6.2.2 Chiavi e certificati

376) La carta dell'azienda deve essere in grado di memorizzare una serie di chiavi crittografiche e di certificati, come specificato nell'appendice 11, parte B.

4.5.6.2.3 Identificazione della carta

377) La carta dell'azienda deve essere in grado di memorizzare i seguenti dati di identificazione della carta:

— numero della carta,

— Stato membro di rilascio, denominazione dell'autorità di rilascio, data di rilascio,

— data di inizio validità della carta, data di scadenza della carta (se presente).

4.5.6.2.4 Identificazione del titolare della carta

378) La carta dell'azienda deve essere in grado di memorizzare i seguenti dati di identificazione del titolare:

— denominazione dell'azienda,

— indirizzo dell'azienda.

4.5.6.2.5 Dati relativi alle attività dell'impresa

379) La carta dell'azienda deve essere in grado di memorizzare i dati seguenti, relativi alle attività dell'impresa:

— data e ora dell'attività,

— tipo di attività (attivazione e/o disattivazione blocco VU e/o trasferimento dati VU e/o trasferimento dati carta),

— periodo cui si riferiscono i dati (se del caso),

— VRN e autorità di immatricolazione del veicolo dello Stato membro,

— numero della carta e Stato membro di rilascio (in caso di trasferimento dei dati della carta).

380) La carta dell'azienda deve essere in grado di conservare almeno 230 di tali registrazioni.

5 MONTAGGIO DELL'APPARECCHIO DI CONTROLLO

5.1 **Montaggio**

381) Gli apparecchi di controllo nuovi devono essere consegnati agli installatori o ai costruttori di veicoli prima dell'attivazione con tutti i parametri di taratura elencati al punto 3.21 impostati su valori predefiniti corretti e validi. In assenza di un valore corretto, i parametri alfabetici devono essere impostati come stringhe di «?» e i parametri numerici devono essere impostati su «0». La consegna di parti dell'apparecchio di controllo aventi attinenza con la sicurezza può essere limitata se necessario durante la certificazione della sicurezza.

▼B

382) Prima dell'attivazione, l'apparecchio di controllo deve consentire l'accesso alla funzione di taratura anche in modalità di funzionamento diverse dal modo taratura.

383) Prima dell'attivazione, l'apparecchio di controllo non deve registrare né memorizzare i dati menzionati ai punti 3.12.3., 3.12.9. e da 3.12.12 a 3.12.15 incluso.

384) Durante il montaggio, i costruttori di veicoli devono preimpostare tutti i parametri noti.

385) I costruttori di veicoli o gli installatori devono procedere all'attivazione dell'apparecchio di controllo montato sul veicolo al più tardi prima che esso sia adibito agli usi previsti nel regolamento (CE) n. 561/2006.

386) L'attivazione dell'apparecchio di controllo deve avvenire automaticamente al primo inserimento di una carta dell'officina valida in una qualsiasi delle interfacce della carta.

387) Le operazioni specifiche di abbinamento tra il sensore di movimento e l'unità elettronica di bordo, se del caso, devono avvenire automaticamente prima o durante l'attivazione.

388) Analogamente, le operazioni specifiche di accoppiamento tra il dispositivo GNSS esterno e l'unità elettronica di bordo, se del caso, devono avvenire automaticamente prima o durante l'attivazione.

389) Dopo l'attivazione, l'apparecchio di controllo deve essere in grado di funzionare correttamente e riconoscere tutti i diritti di accesso ai dati.

390) Dopo l'attivazione, l'apparecchio di controllo deve comunicare al dispositivo di comunicazione remota i dati protetti necessari ai fini dei controlli su strada mirati.

391) Dopo l'attivazione si devono poter usare tutte le funzioni di registrazione e memorizzazione dell'apparecchio di controllo.

392) Dopo il montaggio occorre procedere alla taratura. La prima taratura non deve necessariamente includere l'inserimento del numero di immatricolazione del veicolo (VRN) qualora esso non sia noto all'officina autorizzata che procede alla taratura. In queste circostanze, ed esclusivamente in tale momento, il proprietario del veicolo può inserire il VRN utilizzando la carta dell'azienda prima di adibire il veicolo agli usi previsti nel regolamento (CE) n. 561/2006 (ad esempio utilizzando i comandi mediante una struttura di menù appropriata dell'interfaccia uomo-macchina dell'unità elettronica di bordo) ([1]). L'aggiornamento o la conferma di tali dati devono essere possibili esclusivamente utilizzando una carta dell'officina.

393) Il montaggio di un dispositivo GNSS esterno richiede l'accoppiamento con l'unità elettronica di bordo e la successiva verifica delle informazioni sulla posizione del GNSS.

394) L'apparecchio di controllo deve essere posizionato a bordo del veicolo in modo tale da consentire al conducente di accedere a tutte le funzioni dal posto di guida.

([1]) GU L 102 dell'11.4.2006, pag. 1.

▼B

5.2 **Targhetta di montaggio**

395) Dopo la verifica dell'apparecchio di controllo in sede di montaggio, deve essere affissa una targhetta di montaggio, incisa o stampata in modo permanente, sull'apparecchio di controllo in un punto chiaramente visibile e facilmente accessibile. Nei casi in cui ciò non sia possibile, la targhetta va affissa in posizione facilmente visibile sul montante «B» del veicolo. Nel caso dei veicoli sprovvisti di montante «B», la targhetta di montaggio va apposta sul telaio della portiera dal lato del conducente del veicolo e deve essere chiaramente visibile in tutti i casi.

Dopo ogni intervento da parte di un installatore o di un'officina autorizzati deve essere apposta una nuova targhetta in sostituzione della precedente.

396) Sulla targhetta devono essere riportate almeno le indicazioni seguenti:

— nome, indirizzo o denominazione commerciale dell'installatore o dell'officina autorizzati,

— coefficiente caratteristico del veicolo, in forma di «w = … imp/km»,

— costante dell'apparecchio di controllo, in forma di «k = … imp/km»,

— circonferenza effettiva degli pneumatici delle ruote, in forma di «l = … mm»,

— dimensioni degli pneumatici,

— data in cui sono stati misurati il coefficiente caratteristico del veicolo e la circonferenza effettiva degli pneumatici delle ruote,

— numero di identificazione del veicolo,

— presenza (o meno) di un dispositivo GNSS esterno,

— numero di serie del dispositivo GNSS esterno,

— numero di serie del dispositivo di comunicazione remota,

— numero di serie di tutti i sigilli apposti,

— parte del veicolo su cui è montato l'adattatore, se presente,

— parte del veicolo su cui è montato il sensore di movimento, se non è collegato alla scatola del cambio o se non viene utilizzato un adattatore,

— descrizione del colore del cavo che collega l'adattatore e la parte del veicolo che fornisce gli impulsi in entrata,

— numero di serie del sensore di movimento incorporato dell'adattatore.

397) Solo per i veicoli M1 e N1 che sono provvisti di adattatore conformemente al regolamento (CE) n. 68/2009 della Commissione ([1]), come modificato da ultimo, e qualora non sia possibile indicare tutte le informazioni necessarie, come indicato nel requisito 396, può essere utilizzata una seconda targhetta aggiuntiva. In questi casi la targhetta aggiuntiva deve recare le informazioni di cui ai quattro ultimi trattini del requisito 396.

([1]) Regolamento (CE) n. 68/2009 della Commissione, del 23 gennaio 2009, che adegua per la nona volta al progresso tecnico il regolamento (CEE) n. 3821/85 del Consiglio relativo all'apparecchio di controllo nel settore dei trasporti su strada (GU L 21 del 24.1.2009, pag. 3).

▼B

La targhetta aggiuntiva, se utilizzata, deve essere apposta a fianco o vicino alla targhetta principale, di cui al requisito 396, e deve avere lo stesso livello di protezione. La seconda targhetta, inoltre, deve recare il nome, l'indirizzo o la denominazione commerciale dell'installatore o dell'officina autorizzati che hanno effettuato il montaggio, nonché la data di quest'ultimo.

5.3 **Sigilli**

398) Le seguenti parti devono essere sigillate:

— qualsiasi connessione che, se scollegata, causerebbe modifiche o perdite di dati non rilevabili (ciò può ad esempio valere per il sensore di movimento montato sul cambio, per l'adattatore per i veicoli delle categorie M1/N1, per il dispositivo GNSS esterno o per l'unità elettronica di bordo),

— la targhetta di montaggio, a meno che non sia affissa in modo da non poter essere rimossa senza distruggere le iscrizioni poste sulla stessa.

399) I sigilli summenzionati possono essere tolti:

— in caso d'emergenza,

— per installare, regolare o riparare un limitatore di velocità o qualsiasi altro dispositivo inteso a migliorare la sicurezza stradale, a condizione che l'apparecchio di controllo continui a funzionare in modo affidabile e corretto e sia risigillato da un installatore o da un'officina autorizzati (conformemente alla sezione 6) immediatamente dopo l'installazione del limitatore di velocità o di un altro dispositivo inteso a migliorare la sicurezza stradale, oppure entro sette giorni negli altri casi.

400) L'eventuale rimozione di questi sigilli deve essere l'oggetto di una giustificazione scritta, tenuta a disposizione dell'autorità competente.

401) I sigilli devono avere un numero di identificazione assegnato dal fabbricante. Tale numero deve essere unico e diverso da qualsiasi altro numero di sigillo assegnato da altri fabbricanti di sigilli.

Questo numero d'identificazione unico è così composto: MM NNNNNN, con iscrizione impossibile da rimuovere, dove MM è l'identificazione unica del fabbricante (registrazione nella banca dati gestita dalla CE) e NNNNNN il valore alfanumerico del sigillo, unico nel settore del fabbricante.

402) I sigilli devono avere uno spazio libero in cui gli installatori, le officine o i costruttori di veicoli autorizzati possono aggiungere un marchio speciale in conformità all'articolo 22, paragrafo 3, del regolamento (UE) n. 165/2014.

Tale marchio non deve coprire il numero di identificazione del sigillo.

403) I fabbricanti di sigilli devono essere registrati in una banca dati dedicata e devono rendere pubblici i loro numeri di identificazione dei sigilli attraverso una procedura che sarà stabilita dalla Commissione europea.

404) Le officine e i costruttori di veicoli autorizzati, nel quadro del regolamento (UE) n. 165/2014, devono usare esclusivamente sigilli dei fabbricanti di sigilli elencati nella banca dati di cui sopra.

▼B

405) I fabbricanti di sigilli e i loro distributori devono conservare i documenti attestanti la completa tracciabilità dei sigilli venduti, da utilizzare nel quadro del regolamento (UE) n. 165/2014, e presentarli alle autorità nazionali competenti ogniqualvolta necessario.

406) I numeri di identificazione unici dei sigilli devono essere visibili sulla targhetta di montaggio.

6 VERIFICHE, CONTROLLI E RIPARAZIONI

I requisiti relativi alle circostanze in cui si possono togliere i sigilli, secondo quanto indicato all'articolo 22, paragrafo 5, del regolamento (UE) n. 165/2014, sono definiti al punto 5.3 del presente allegato.

6.1 **Autorizzazione di installatori, officine e costruttori di veicoli**

Gli Stati membri autorizzano, sottopongono a verifiche regolari e certificano gli organismi incaricati di effettuare:

— il montaggio,

— le verifiche,

— i controlli,

— le riparazioni.

Le carte dell'officina devono essere rilasciate esclusivamente agli installatori e/o alle officine autorizzati ad effettuare l'attivazione e/o la taratura dell'apparecchio di controllo in conformità al presente allegato e che, tranne in casi debitamente motivati:

— non possiedono i requisiti necessari per ottenere una carta dell'azienda,

— e le cui altre attività professionali non costituiscono un rischio potenziale per la sicurezza generale del sistema, secondo quanto previsto all'appendice 10.

6.2 **Verifica degli strumenti nuovi o riparati**

407) Di ogni singolo dispositivo, nuovo o riparato, vanno verificati il corretto funzionamento e l'esattezza delle letture e delle registrazioni, nei limiti fissati ai punti 3.2.1, 3.2.2, 3.2.3 e 3.3 mediante l'apposizione di sigilli, conformemente al punto 5.3, e la taratura.

6.3 **Controllo in sede di montaggio**

408) All'atto del montaggio sul veicolo, l'installazione nel suo complesso (compreso l'apparecchio di controllo) deve essere conforme alle disposizioni relative alle tolleranze massime di cui ai punti 3.2.1, 3.2.2, 3.2.3 e 3.3.

6.4 **Controlli periodici**

409) I controlli periodici degli apparecchi montati nei veicoli devono avere luogo dopo ogni riparazione degli apparecchi stessi, dopo ogni modifica del coefficiente caratteristico del veicolo o della circonferenza effettiva degli pneumatici, dopo un periodo di ora UTC errata di oltre 20 minuti, dopo la modifica del VRN e comunque almeno ogni due anni (24 mesi) a partire dall'ultimo controllo.

410) Si devono controllare:

— lo stato di buon funzionamento dell'apparecchio di controllo, compresa la funzione di memorizzazione di dati nelle carte tachigrafiche e la comunicazione con i lettori di comunicazione remota,

▼B

— la conformità alle disposizioni dei punti 3.2.1 e 3.2.2 relative alle tolleranze massime in sede di montaggio,

— la conformità alle disposizioni dei punti 3.2.3 e 3.3,

— la presenza del marchio di omologazione sull'apparecchio di controllo,

— che siano apposte la targhetta di montaggio, quale definita al requisito 396, e la targhetta segnaletica, quale definita al requisito 225,

— le dimensioni degli pneumatici e la circonferenza effettiva degli pneumatici,

— che l'apparecchio non sia collegato ad alcun dispositivo di manipolazione,

— che i sigilli siano correttamente collocati, in buone condizioni, e che i loro numeri di identificazione siano validi (fabbricante dei sigilli presente nella banca dati della CE) e corrispondano alle iscrizioni sulla targhetta di montaggio (cfr. requisito 401).

411) Se dopo l'ultimo controllo viene constatata una delle anomalie elencate al punto 3.9 (Rilevamento di anomalie e/o guasti) e qualora i fabbricanti del tachigrafo e/o le autorità nazionali ritengano che essa possa comportare rischi per la sicurezza dell'apparecchio, l'officina:

a. raffronta i dati di identificazione del sensore di movimento collegato alla scatola del cambio con quelli del sensore di movimento registrati nell'unità elettronica di bordo ad esso accoppiata;

b. verifica se le informazioni riportate sulla targhetta di montaggio corrispondono a quelle contenute nell'unità elettronica di bordo;

c. verifica se il numero di serie e il numero di omologazione del sensore di movimento, se stampati sul corpo del sensore stesso, corrispondono alle informazioni memorizzate nella memoria di dati dell'apparecchio di controllo;

d. confronta gli eventuali dati di identificazione apposti sulla targhetta segnaletica del dispositivo GNSS esterno con quelli memorizzati nella memoria di dati dell'unità elettronica di bordo.

412) Nelle relazioni di controllo, le officine devono indicare gli eventuali casi di rimozione dei sigilli o di intervento di dispositivi di manipolazione. Le officine devono conservare tali relazioni per almeno 2 anni e metterle a disposizione delle autorità competenti ogniqualvolta queste ultime ne facciano richiesta.

413) Tali controlli devono prevedere una taratura e una sostituzione preventiva dei sigilli la cui apposizione è responsabilità delle officine..

6.5 **Determinazione degli errori**

414) La determinazione degli errori all'atto del montaggio e durante l'uso va effettuata nelle seguenti condizioni, che devono essere considerate normali condizioni di prova:

— veicolo a vuoto, in normali condizioni di marcia,

— pressione degli pneumatici conforme alle indicazioni fornite dal produttore,

▼B

— usura degli pneumatici nei limiti ammessi dalla normativa nazionale in vigore,

— movimento del veicolo:

— il veicolo deve spostarsi, mosso dal proprio motore, in linea retta, su terreno piano, ad una velocità di 50 ± 5 km/h. La misurazione deve essere effettuata su una distanza di almeno 1 000 m.

— A condizione che sia garantita una precisione analoga, la prova può essere effettuata con altri metodi, per esempio su un banco di prova.

6.6 **Riparazioni**

415) Le officine devono essere in grado di trasferire i dati dall'apparecchio di controllo al fine di fornirli alle imprese di trasporti interessate.

416) Qualora il cattivo funzionamento dell'apparecchio di controllo impedisca il trasferimento dei dati registrati in precedenza, anche dopo la riparazione da parte di tali officine autorizzate, queste ultime devono rilasciare alle imprese di trasporti un certificato che attesti l'impossibilità di trasferire i dati. Le officine devono conservare una copia di ogni certificato rilasciato per almeno due anni.

7 RILASCIO DELLA CARTA

Le procedure di rilascio della carta definite dagli Stati membri devono conformarsi ai requisiti seguenti.

417) Al primo rilascio di una carta tachigrafica ad un richiedente, il numero della carta deve contenere un codice di serie (se applicabile), un codice di sostituzione e un codice di rinnovo impostati sullo «0».

418) Il numero della carta di tutte le carte tachigrafiche non personali rilasciate ad un medesimo organismo di controllo, una medesima officina o una medesima impresa di trasporti, deve avere gli stessi primi 13 caratteri ed un diverso codice di serie.

419) Una carta tachigrafica rilasciata in sostituzione di una carta tachigrafica esistente deve avere lo stesso numero della carta sostituita, eccetto per il codice di sostituzione che deve essere aumentato di un'unità (nell'ordine 0, …, 9, A, …, Z).

420) Una carta tachigrafica rilasciata in sostituzione di una carta tachigrafica esistente deve avere la stessa data di scadenza della carta sostituita.

421) Una carta tachigrafica rilasciata in rinnovo di una carta tachigrafica esistente deve avere lo stesso numero della carta rinnovata, eccetto per il codice di sostituzione che deve essere riportato a «0» e il codice di rinnovo che deve essere aumentato di un'unità (nell'ordine 0, …, 9, A, …, Z).

422) In caso di cambio di una carta tachigrafica esistente al fine di modificarne i dati amministrativi, si devono applicare le regole relative al rinnovo, se il cambio è effettuato all'interno dello stesso Stato membro, oppure le regole relative al primo rilascio, se il cambio è effettuato da un altro Stato membro.

423) Per le carte dell'officina o le carte di controllo non personali, nel campo «Cognome del titolare della carta» si deve inserire la denominazione dell'officina o dell'organismo di controllo o il nome dell'installatore o dell'agente di controllo, a discrezione degli Stati membri.

▼B

424) Gli Stati membri devono scambiarsi i dati in forma elettronica per assicurare l'univocità delle carte del conducente da essi emesse conformemente all'articolo 31 del regolamento (UE) n. 165/2014.

8 OMOLOGAZIONE DELL'APPARECCHIO DI CONTROLLO E DELLE CARTE TACHIGRAFICHE

8.1 **Prescrizioni generali**

Agli effetti della presente sezione, con «apparecchio di controllo» s'intendono l'«apparecchio di controllo o i suoi componenti». Non è richiesta l'omologazione del cavo o dei cavi di collegamento tra il sensore di movimento e la VU, il dispositivo GNSS esterno e la VU o il dispositivo di comunicazione remota e la VU. I fogli di carta impiegati dall'apparecchio di controllo devono considerarsi come un componente dell'apparecchio stesso.

Ciascun fabbricante può chiedere l'omologazione del proprio componente con qualsiasi tipo di sensore di movimento, dispositivo GNSS esterno e viceversa, purché ciascun componente sia conforme ai requisiti del presente allegato. In alternativa, i fabbricanti possono anche chiedere l'omologazione dell'apparecchio di controllo.

425) L'apparecchio di controllo deve essere presentato per l'omologazione munito di tutti i dispositivi integrati supplementari.

426) L'omologazione dell'apparecchio di controllo e delle carte tachigrafiche deve comprendere prove riguardanti la sicurezza, prove funzionali e prove di interoperabilità. I risultati positivi di ciascuna di queste prove sono riportati su un apposito certificato.

427) Le autorità di omologazione degli Stati membri non rilasciano nessuna scheda di omologazione finché non siano stati loro presentati:

— un certificato di sicurezza,

— un certificato funzionale

— e un certificato di interoperabilità

per l'apparecchio di controllo o la carta tachigrafica che forma l'oggetto della domanda di omologazione.

428) Eventuali modifiche del software o dell'hardware dell'apparecchio o della natura dei materiali usati per la fabbricazione devono essere notificate prima dell'impiego all'autorità che ha omologato l'apparecchio. Tale autorità conferma al fabbricante l'estensione dell'omologazione oppure richiede un aggiornamento o una conferma del certificato funzionale, del certificato di sicurezza e/o del certificato di interoperabilità pertinenti.

429) Le procedure volte ad aggiornare in situ il software dell'apparecchio di controllo devono essere approvate dall'autorità che ha omologato l'apparecchio di controllo. L'aggiornamento del software non deve modificare o cancellare i dati relativi alle attività del conducente in esso memorizzati. Il software si può aggiornare solo sotto la responsabilità del fabbricante dell'apparecchio.

430) L'omologazione delle modifiche del software volte ad aggiornare un apparecchio di controllo precedentemente omologato non può essere negata qualora tali modifiche si applichino solo a funzioni non specificate nel presente allegato. L'aggiornamento del software di un apparecchio di controllo può escludere l'introduzione di nuovi insiemi di caratteri, qualora non sia tecnicamente fattibile.

▼B

8.2 **Certificato di sicurezza**

431) Il certificato di sicurezza è rilasciato in conformità alle disposizioni dell'appendice 10 del presente allegato. I componenti dell'apparecchio di controllo da certificare sono: unità elettronica di bordo, sensore di movimento, dispositivo GNSS esterno e carte tachigrafiche.

432) Nei casi eccezionali in cui le autorità nazionali di certificazione della sicurezza rifiutino di certificare apparecchiature nuove a causa del carattere superato dei meccanismi di sicurezza, l'omologazione continua a essere rilasciata solo in queste circostanze specifiche ed eccezionali e qualora non esistano soluzioni alternative in conformità al presente regolamento.

433) In questi casi gli Stati membri interessati devono informare sollecitamente la Commissione europea che, entro 12 mesi civili dal rilascio dell'omologazione, avvia una procedura per accertare che la sicurezza sia stata ripristinata ai livelli originali.

8.3 **Certificato funzionale**

434) Ogni richiedente un'omologazione deve presentare all'autorità di omologazione dello Stato membro tutto il materiale e la documentazione ritenuti necessari da tale autorità.

435) I fabbricanti devono fornire i campioni pertinenti dei prodotti da omologare e la relativa documentazione ai laboratori incaricati di eseguire le prove funzionali entro un mese dalla presentazione di una richiesta in tal senso. Gli eventuali costi sono a carico dei soggetti che hanno presentato la richiesta. I laboratori sono tenuti a trattare con riservatezza le informazioni sensibili sotto il profilo commerciale.

436) Il certificato funzionale deve essere rilasciato al fabbricante solo se almeno tutte le prove funzionali specificate nell'appendice 9 hanno dato risultati positivi.

437) L'autorità di omologazione rilascia un certificato funzionale. Tale certificato deve recare, oltre al nome del beneficiario e all'identificazione del modello, un elenco dettagliato delle prove effettuate e dei risultati ottenuti.

438) Il certificato funzionale dei componenti dell'apparecchio di controllo deve indicare inoltre i numeri di omologazione degli altri componenti dell'apparecchio di controllo compatibili omologati sottoposti a prova per ottenere la certificazione dell'apparecchio di controllo.

439) Il certificato funzionale dei componenti dell'apparecchio di controllo deve anche indicare la norma ISO o CEN in conformità alla quale è stata certificata l'interfaccia funzionale.

8.4 **Certificato di interoperabilità**

440) Le prove di interoperabilità sono effettuate da un unico laboratorio sotto l'autorità e la responsabilità della Commissione europea.

441) Il laboratorio registra le richieste di prove di interoperabilità presentate dai fabbricanti nell'ordine cronologico di presentazione.

442) Le richieste sono registrate ufficialmente solo quando il laboratorio dispone:

— dell'intera serie di materiali e documenti necessari per le prove di interoperabilità,

▼B

— del corrispondente certificato di sicurezza,

— del corrispondente certificato funzionale.

La data di registrazione della richiesta viene notificata al fabbricante.

443) Ad eccezione delle circostanze eccezionali di cui al requisito 432, i laboratori non effettuano prove di interoperabilità sugli apparecchi di controllo o sulle carte tachigrafiche sprovvisti di certificato di sicurezza e di certificato funzionale.

444) I fabbricanti che richiedono le prove di interoperabilità si impegnano a lasciare a disposizione del laboratorio incaricato di tali prove l'intera serie di materiali e documenti forniti per l'esecuzione delle prove stesse.

445) Le prove di interoperabilità sono effettuate, in conformità alle disposizioni dell'appendice 9 del presente allegato, con tutti i tipi di apparecchi di controllo e di carte tachigrafiche:

— la cui omologazione è in corso di validità o

— che sono in attesa di omologazione e hanno ottenuto un certificato di interoperabilità valido.

446) Le prove di interoperabilità devono riguardare tutte le generazioni di apparecchi di controllo o di carte tachigrafiche ancora in uso.

447) Il laboratorio rilascia al fabbricante il certificato di interoperabilità solo se tutte le prove di interoperabilità hanno dato risultati positivi.

448) Se le prove di interoperabilità non danno risultati positivi con uno o più apparecchi di controllo o carte tachigrafiche, il certificato di interoperabilità non viene rilasciato al fabbricante finché non sono state apportate le modifiche necessarie a superare tutte le prove di interoperabilità. Il laboratorio identifica la causa del problema con l'aiuto dei fabbricanti interessati da tale mancanza di interoperabilità ed aiuta il richiedente a trovare una soluzione tecnica. Nel caso in cui il fabbricante modifichi il prodotto, spetterà al fabbricante stesso accertare presso le autorità competenti che il certificato di sicurezza e il certificato funzionale siano ancora validi.

449) Il certificato di interoperabilità ha una validità di sei mesi e viene revocato se, al termine di tale periodo, il fabbricante non ha ottenuto la corrispondente scheda di omologazione. Il certificato di interoperabilità viene trasmesso dal fabbricante all'autorità di omologazione dello Stato membro che ha rilasciato il certificato funzionale.

450) Qualsiasi elemento cui si possa ricondurre la mancanza di interoperabilità non deve essere usato a fini di lucro o per accedere ad una posizione dominante.

8.5 **Scheda di omologazione**

451) L'autorità di omologazione di uno Stato membro può rilasciare la scheda di omologazione non appena è in possesso dei tre certificati richiesti.

▼B

452) La scheda di omologazione dei componenti dell'apparecchio di controllo deve anche indicare i numeri di omologazione degli altri componenti interoperabili omologati dell'apparecchio di controllo.

453) L'autorità di omologazione deve trasmettere una copia della scheda di omologazione al laboratorio incaricato delle prove di interoperabilità all'atto del rilascio della stessa al fabbricante.

454) Il laboratorio competente per le prove di interoperabilità deve gestire un sito web pubblico nel quale mantiene aggiornato l'elenco dei modelli di apparecchio di controllo o carta tachigrafica:

— per i quali è stata registrata una richiesta di prove di interoperabilità,

— che abbiano ottenuto un certificato di interoperabilità (anche provvisorio),

— che abbiano ottenuto una scheda di omologazione.

8.6 **Procedura eccezionale: primi certificati di interoperabilità per gli apparecchi di controllo e le carte tachigrafiche di 2ª generazione**

455) Per un periodo di quattro mesi successivi al rilascio del certificato di interoperabilità della prima coppia apparecchio di controllo di 2ª generazione/ carte tachigrafiche di 2ª generazione (carte del conducente, dell'officina, di controllo e dell'azienda), ogni certificato di interoperabilità rilasciato (compresi i primi in assoluto), concernente le richieste presentate durante tale periodo, deve essere considerato provvisorio.

456) Se al termine di tale periodo tutti i prodotti interessati sono reciprocamente interoperabili, i rispettivi certificati di interoperabilità diventano definitivi.

457) Se durante tale periodo si riscontrano mancanze di interoperabilità, il laboratorio incaricato delle prove di interoperabilità identifica le cause dei problemi con l'aiuto di tutti i fabbricanti interessati e li invita ad apportare le modifiche necessarie.

458) Se al termine di tale periodo sussistono ancora problemi di interoperabilità, il laboratorio incaricato delle prove di interoperabilità, con la collaborazione dei fabbricanti interessati e delle autorità di omologazione che hanno rilasciato i corrispondenti certificati funzionali, ricerca le cause della mancanza di interoperabilità e stabilisce le modifiche che ogni fabbricante deve apportare. La ricerca di soluzioni tecniche deve avvenire entro un periodo massimo di due mesi, in seguito al quale, qualora non si trovi una soluzione comune, la Commissione, dopo aver consultato il laboratorio incaricato delle prove di interoperabilità, decide quali apparecchi e quali carte ottengono un certificato definitivo di interoperabilità e ne indica i motivi.

459) Tutte le richieste di prove di interoperabilità, registrate dal laboratorio tra il termine del periodo di quattro mesi successivi al rilascio del primo certificato provvisorio di interoperabilità e la data della decisione della Commissione di cui al requisito 455, sono rinviate fino alla soluzione dei problemi iniziali di interoperabilità. Tali richieste sono quindi evase in ordine cronologico in base alla data di registrazione.

▼B

Appendice 1

DIZIONARIO DEI DATI

INDICE

1. INTRODUZIONE

1.1. Metodo di definizione dei tipi di dati

1.2. Riferimenti

2. DEFINIZIONI DEI TIPI DI DATI

2.1. ActivityChangeInfo

2.2. Address

2.3. AESKey

2.4. AES128Key

2.5. AES192Key

2.6. AES256Key

2.7. BCDString

2.8. CalibrationPurpose

2.9. CardActivityDailyRecord

2.10. CardActivityLengthRange

2.11. CardApprovalNumber

2.12. CardCertificate

2.13. CardChipIdentification

2.14. CardConsecutiveIndex

2.15. CardControlActivityDataRecord

2.16. CardCurrentUse

2.17. CardDriverActivity

2.18. CardDrivingLicenceInformation

2.19. CardEventData

2.20. CardEventRecord

2.21. CardFaultData

2.22. CardFaultRecord

2.23. CardIccIdentification

2.24. CardIdentification

2.25. CardMACertificate

2.26. CardNumber

2.27. CardPlaceDailyWorkPeriod

2.28. CardPrivateKey

2.29. CardPublicKey

▼B

2.30. CardRenewalIndex

2.31. CardReplacementIndex

2.32. CardSignCertificate

2.33. CardSlotNumber

2.34. CardSlotsStatus

2.35. CardSlotsStatusRecordArray

2.36. CardStructureVersion

2.37. CardVehicleRecord

2.38. CardVehiclesUsed

2.39. CardVehicleUnitRecord

2.40. CardVehicleUnitsUsed

2.41. Certificate

2.42. CertificateContent

2.43. CertificateHolderAuthorisation

2.44. CertificateRequestID

2.45. CertificationAuthorityKID

2.46. CompanyActivityData

2.47. CompanyActivityType

2.48. CompanyCardApplicationIdentification

2.49. CompanyCardHolderIdentification

2.50. ControlCardApplicationIdentification

2.51. ControlCardControlActivityData

2.52. ControlCardHolderIdentification

2.53. ControlType

2.54. CurrentDateTime

2.55. CurrentDateTimeRecordArray

2.56. DailyPresenceCounter

2.57. Datef

2.58. DateOfDayDownloaded

2.59. DateOfDayDownloadedRecordArray

2.60. Distance

2.61. DriverCardApplicationIdentification

▼B

2.62. DriverCardHolderIdentification

2.63. DSRCSecurityData

2.64. EGFCertificate

2.65. EmbedderIcAssemblerId

2.66. EntryTypeDailyWorkPeriod

2.67. EquipmentType

2.68. EuropeanPublicKey

2.69. EventFaultRecordPurpose

2.70. EventFaultType

2.71. ExtendedSealIdentifier

2.72. ExtendedSerialNumber

2.73. FullCardNumber

2.74. FullCardNumberAndGeneration

2.75. Generation

2.76. GeoCoordinates

2.77. GNSSAccuracy

2.78. GNSSContinuousDriving

2.79. GNSSContinuousDrivingRecord

2.80. GNSSPlaceRecord

2.81. HighResOdometer

2.82. HighResTripDistance

2.83. HolderName

2.84. InternalGNSSReceiver

2.85. K-ConstantOfRecordingEquipment

2.86. KeyIdentifier

2.87. KMWCKey

2.88. Language

2.89. LastCardDownload

2.90. LinkCertificate

2.91. L-TyreCircumference

2.92. MAC

2.93. ManualInputFlag

2.94. ManufacturerCode

2.95. ManufacturerSpecificEventFaultData

2.96. MemberStateCertificate

▼B

2.97. MemberStateCertificateRecordArray

2.98. MemberStatePublicKey

2.99. Name

2.100. NationAlpha

2.101. NationNumeric

2.102. NoOfCalibrationRecords

2.103. NoOfCalibrationsSinceDownload

2.104. NoOfCardPlaceRecords

2.105. NoOfCardVehicleRecords

2.106. NoOfCardVehicleUnitRecords

2.107. NoOfCompanyActivityRecords

2.108. NoOfControlActivityRecords

2.109. NoOfEventsPerType

2.110. NoOfFaultsPerType

2.111. NoOfGNSSCDRecords

2.112. NoOfSpecificConditionRecords

2.113. OdometerShort

2.114. OdometerValueMidnight

2.115. OdometerValueMidnightRecordArray

2.116. OverspeedNumber

2.117. PlaceRecord

2.118. PreviousVehicleInfo

2.119. PublicKey

2.120. RecordType

2.121. RegionAlpha

2.122. RegionNumeric

2.123. RemoteCommunicationModuleSerialNumber

2.124. RSAKeyModulus

2.125. RSAKeyPrivateExponent

2.126. RSAKeyPublicExponent

2.127. RtmData

2.128. SealDataCard

▼B

2.129. SealDataVu

2.130. SealRecord

2.131. SensorApprovalNumber

2.132. SensorExternalGNSSApprovalNumber

2.133. SensorExternalGNSSCoupledRecord

2.134. SensorExternalGNSSIdentification

2.135. SensorExternalGNSSInstallation

2.136. SensorExternalGNSSOSIdentifier

2.137. SensorExternalGNSSSCIdentifier

2.138. SensorGNSSCouplingDate

2.139. SensorGNSSSerialNumber

2.140. SensorIdentification

2.141. SensorInstallation

2.142. SensorInstallationSecData

2.143. SensorOSIdentifier

2.144. SensorPaired

2.145. SensorPairedRecord

2.146. SensorPairingDate

2.147. SensorSCIdentifier

2.148. SensorSerialNumber

2.149. Signature

2.150. SignatureRecordArray

2.151. SimilarEventsNumber

2.152. SpecificConditionRecord

2.153. SpecificConditions

2.154. SpecificConditionType

2.155. Velocità

2.156. SpeedAuthorised

2.157. SpeedAverage

2.158. SpeedMax

2.159. TachographPayload

2.160. TachographPayloadEncrypted

▼B

2.161. TDesSessionKey

2.162. TimeReal

2.163. TyreSize

2.164. VehicleIdentificationNumber

2.165. VehicleIdentificationNumberRecordArray

2.166. VehicleRegistrationIdentification

2.167. VehicleRegistrationNumber

2.168. VehicleRegistrationNumberRecordArray

2.169. VuAbility

2.170. VuActivityDailyData

2.171. VuActivityDailyRecordArray

2.172. VuApprovalNumber

2.173. VuCalibrationData

2.174. VuCalibrationRecord

2.175. VuCalibrationRecordArray

2.176. VuCardIWData

2.177. VuCardIWRecord

2.178. VuCardIWRecordArray

2.179. VuCardRecord

2.180. VuCardRecordArray

2.181. VuCertificate

2.182. VuCertificateRecordArray

2.183. VuCompanyLocksData

2.184. VuCompanyLocksRecord

2.185. VuCompanyLocksRecordArray

2.186. VuControlActivityData

2.187. VuControlActivityRecord

2.188. VuControlActivityRecordArray

▼B

2.189. VuDataBlockCounter

2.190. VuDetailedSpeedBlock

2.191. VuDetailedSpeedBlockRecordArray

2.192. VuDetailedSpeedData

2.193. VuDownloadablePeriod

2.194. VuDownloadablePeriodRecordArray

2.195. VuDownloadActivityData

2.196. VuDownloadActivityDataRecordArray

2.197. VuEventData

2.198. VuEventRecord

2.199. VuEventRecordArray

2.200. VuFaultData

2.201. VuFaultRecord

2.202. VuFaultRecordArray

2.203. VuGNSSCDRecord

2.204. VuGNSSCDRecordArray

2.205. VuIdentification

2.206. VuIdentificationRecordArray

2.207. VuITSConsentRecord

2.208. VuITSConsentRecordArray

2.209. VuManufacturerAddress

2.210. VuManufacturerName

2.211. VuManufacturingDate

2.212. VuOverSpeedingControlData

2.213. VuOverSpeedingControlDataRecordArray

2.214. VuOverSpeedingEventData

▼B

2.215. VuOverSpeedingEventRecord

2.216. VuOverSpeedingEventRecordArray

2.217. VuPartNumber

2.218. VuPlaceDailyWorkPeriodData

2.219. VuPlaceDailyWorkPeriodRecord

2.220. VuPlaceDailyWorkPeriodRecordArray

2.221. VuPrivateKey

2.222. VuPublicKey

2.223. VuSerialNumber

2.224. VuSoftInstallationDate

2.225. VuSoftwareIdentification

2.226. VuSoftwareVersion

2.227. VuSpecificConditionData

2.228. VuSpecificConditionRecordArray

2.229. VuTimeAdjustmentData

2.230. VuTimeAdjustmentGNSSRecord

2.231. VuTimeAdjustmentGNSSRecordArray

2.232. VuTimeAdjustmentRecord

2.233. VuTimeAdjustmentRecordArray

2.234. WorkshopCardApplicationIdentification

2.235. WorkshopCardCalibrationData

2.236. WorkshopCardCalibrationRecord

2.237. WorkshopCardHolderIdentification

2.238. WorkshopCardPIN

2.239. W-VehicleCharacteristicConstant

2.240. VuPowerSupplyInterruptionRecord

▼B

2.241. VuPowerSupplyInterruptionRecordArray

2.242. VuSensorExternalGNSSCoupledRecordArray

2.243. VuSensorPairedRecordArray

3. DEFINIZIONI DEI CAMPI DI VALORI E DIMENSIONI

4. SET DI CARATTERI

5. CODIFICA

6. IDENTIFICATIVI DI OGGETTO E IDENTIFICATIVI DI APPLICAZIONE

6.1. Identificativi di oggetto

6.2. Identificativi di applicazione

1. INTRODUZIONE

La presente appendice specifica i formati dei dati, gli elementi di dati e le strutture dei dati da usare nell'apparecchio di controllo e nelle carte tachigrafiche.

1.1. Metodo di definizione dei tipi di dati

Nella presente appendice i tipi di dati sono definiti in base al linguaggio Abstract Syntax Notation One (ASN.1). La notazione ASN.1 permette di definire dati semplici e strutturati, senza richiedere una specifica sintassi di trasmissione (regole di codifica), la quale dipende dall'applicazione e dal contesto.

La notazione convenzionale ASN.1 per l'attribuzione di nomi si basa sulla norma ISO/IEC 8824-1. Ciò significa che:

— ove possibile, il significato del tipo di dati è implicitamente noto in funzione del nome attribuito,

— per i tipi di dati composti, costituiti da una combinazione di più tipi di dati, il nome è comunque un'unica sequenza di caratteri alfabetici con la lettera iniziale maiuscola, ma vengono usate lettere maiuscole anche all'interno del nome, che consentono di individuare il significato corrispondente,

— in generale, i nomi dei tipi di dati si riferiscono al nome dei tipi di dati con cui vengono costruiti, all'apparecchio in cui sono memorizzati i dati e alla funzione connessa ai dati.

Se un tipo ASN.1 è già definito nell'ambito di un'altra norma e viene usato nell'apparecchio di controllo, tale tipo ASN.1 è definito nella presente appendice.

Per tenere conto di vari tipi di regole di codifica, alcuni tipi ASN.1 compresi nella presente appendice sono limitati da identificativi del campo di valori. Gli identificativi del campo di valori sono definiti al paragrafo 3 e nell'appendice 2.

1.2. Riferimenti

Nella presente appendice si rimanda alle seguenti norme:

ISO 639	Codice per la rappresentazione dei nomi delle lingue. Prima edizione: 1988.

▼B

ISO 3166	Codici per la rappresentazione dei nomi dei paesi e delle loro suddivisioni — Parte 1: Codici paese, 2013
ISO 3779	Veicoli stradali — Numero di identificazione del veicolo (VIN) — Contenuto e struttura. 2009
ISO/CEI 7816-5	Carte di identificazione — Carte a circuiti integrati — Parte 5: Registrazione dei fornitori di applicazioni. Seconda edizione: 2004.
ISO/CEI 7816-6	Carte di identificazione — Carte a circuiti integrati — Parte 6: Elementi di dati interindustriali per gli scambi, 2004 + rettifica tecnica 1: 2006
ISO/CEI 8824-1	Tecnologia dell'informazione — Abstract Syntax Notation 1 (ASN.1): Descrizione della notazione di base. 2008 + rettifica tecnica 1: 2012 e rettifica tecnica 2: 2014.
ISO/CEI 8825-2	Tecnologia dell'informazione — Regole di codifica ASN.1: Descrizione delle regole di codifica a pacchetto (PER). 2008.
ISO/CEI 8859-1	Tecnologia dell'informazione — Codifica a gruppo singolo di 8 bit di insiemi di caratteri grafici — Parte 1: Alfabeto latino n. 1. Prima edizione: 1998.
ISO/CEI 8859-7	Tecnologia dell'informazione — Codifica a gruppo singolo di 8 bit di insiemi di caratteri grafici — Parte 7: Alfabeto latino/greco. 2003.
ISO 16844-3	Veicoli stradali — Sistemi tachigrafici — Interfaccia del sensore di movimento. 2004 + rettifica tecnica 1: 2006.
TR-03110-3	Orientamenti tecnici TR-03110-3 di BSI/ANSSI, Meccanismi di sicurezza avanzati per i documenti di viaggio a lettura ottica e il token eIDAS- Parte 3: Specifiche comuni, versione 2.20, 3. Febbraio 2015

2. DEFINIZIONI DEI TIPI DI DATI

Per ciascuno dei seguenti tipi di dati, il valore predefinito di un contenuto «non noto» o «non applicabile» è dato dal riempimento dell'elemento di dati con byte 'FF'.

Tutti i tipi di dati sono utilizzati per le applicazioni di prima e seconda generazione, salvo indicazione contraria.

2.1. **ActivityChangeInfo**

Questo tipo di dati consente di codificare, in una parola (word) a due byte, la condizione della sede (slot) alle 00h00 e/o la condizione del conducente alle 00h00 e/o i cambi di attività e/o le variazioni della condizione di guida e/o le variazioni della condizione della carta riguardanti un conducente o un secondo conducente. Questo tipo di dati si riferisce ai requisiti 105, 266, 291, 320, 321, 343 e 344 dell'allegato 1C.

```
ActivityChangeInfo ::= OCTET STRING (SIZE(2))
```

Assegnazione valore — Allineato all'ottetto: 'scpaatttttttttt'B (16 bit)

Per le registrazioni nella memoria di dati (o condizione della sede):

's'B	Sede (slot): '0'B: CONDUCENTE, '1'B: SECONDO CONDUCENTE,

▼B

‘c’B	Condizione di guida:
	‘0’B: SINGOLA,
	‘1’B: EQUIPAGGIO,
‘p’B	Condizione della carta del conducente (o dell'officina) nella relativa sede (slot):
	‘0’B: INSERITA, la carta è inserita,
	‘1’B: NON INSERITA, la carta è assente (o una carta viene estratta),
‘aa’B	Attività:
	‘00’B: INTERRUZIONE/RIPOSO,
	‘01’B: DISPONIBILITÀ,
	‘10’B: LAVORO,
	‘11’B: GUIDA,
‘ttttttttttt’B	Ora della variazione: numero di minuti a partire dalle 00h00 del giorno in questione.

Per le registrazioni nella carta del conducente (o dell'officina) (e per la condizione del conducente):

‘s’B	Sede (slot) (non pertinente se ‘p’ = 1, fatta salva la nota sotto):
	‘0’B: CONDUCENTE,
	‘1’B: SECONDO CONDUCENTE,
‘c’B	Condizione di guida (quando ‘p’ = 0) o
	Condizione attività successiva (quando ‘p’ = 1):
	‘0’B: SINGOLA,
	‘0’B: NON NOTA
	‘1’B: EQUIPAGGIO,
	‘1’B: NOTA (= immissione manuale)
‘p’B	Condizione carta:
	‘0’B: INSERITA, la carta è inserita in un apparecchio di controllo,
	‘1’B: NON INSERITA, la carta è assente (o la carta viene estratta),
‘aa’B	Attività (non pertinente se ‘p’ = 1 e ‘c’ = 0, fatta salva la nota sotto):
	‘00’B: INTERRUZIONE/RIPOSO,
	‘01’B: DISPONIBILITÀ,
	‘10’B: LAVORO,
	‘11’B: GUIDA,
‘ttttttttttt’B	Ora della variazione: numero di minuti a partire dalle 00h00 del giorno in questione.

▼B

Nota per il caso di «estrazione carta»:

Quando la carta viene estratta:

— ‘s’ è pertinente ed indica la sede (slot) da cui viene estratta la carta,

— ‘c’ deve essere impostato su 0,

— ‘p’ deve essere impostato su 1,

— ‘aa’ deve codificare l'attività selezionata in corso al momento dell'estrazione.

In seguito a un'immissione manuale, i bit ‘c’ e ‘aa’ della parola (word) (memorizzata in una carta) possono essere sovrascritti in un secondo tempo per tenere conto dell'immissione.

2.2. **Address**

Un indirizzo.

```
Address ::= SEQUENCE {
   codePage                              INTEGER (0..255),
   address                               OCTET STRING (SIZE(35))
}
```

codePage specifica una serie di caratteri quali definiti nel capitolo 4,

address è un indirizzo codificato usando la serie specifica di caratteri.

2.3. **AESKey**

Seconda generazione:

Una chiave AES con una lunghezza di 128, 192 o 256 bit.

```
AESKey ::= CHOICE {
   aes128Key                             AES128Key,
   aes192Key                             AES192Key,
   aes256Key                             AES256Key
}
```

Assegnazione valore: nessun'altra specificazione.

2.4. **AES128Key**

Seconda generazione:

Una chiave AES128.

```
AES128Key ::= SEQUENCE {
   length                                INTEGER(0..255),
   aes128Key                             OCTET STRING (SIZE(16))
}
```

length indica la lunghezza della chiave AES128 in ottetti.

aes128key è una chiave AES con una lunghezza di 128 bit.

Assegnazione valore:

la lunghezza deve avere il valore 16.

▼B

2.5. **AES192Key**

Seconda generazione:

Una chiave AES192.

```
AES192Key ::= SEQUENCE {
   length                                INTEGER(0..255),
   aes192Key                             OCTET STRING (SIZE(24))
}
```

length indica la lunghezza della chiave AES192 in ottetti.

aes192key è una chiave AES con una lunghezza di 192 bit.

Assegnazione valore:

la lunghezza deve avere il valore 24.

2.6. **AES256Key**

Seconda generazione:

Una chiave AES256.

```
AES256Key ::= SEQUENCE {
   length                                INTEGER(0..255),
   aes256Key                             OCTET STRING (SIZE(32))
}
```

length indica la lunghezza della chiave AES256 in ottetti.

aes256key è una chiave AES con una lunghezza di 256 bit.

Assegnazione valore:

la lunghezza deve avere il valore 32.

2.7. **BCDString**

BCDString si usa per la rappresentazione in codice binario decimale (BCD). Questo tipo di dati è usato per rappresentare una cifra decimale in un semi-ottetto (4 bit). BCDString si basa su ISO/IEC 8824-1 'CharacterStringType'.

```
BCDString ::= CHARACTER STRING (WITH COMPONENTS {
   identification ( WITH COMPONENTS {
   fixed PRESENT }) })
```

BCDString utilizza la notazione «hstring». La prima cifra esadecimale a partire da sinistra è il semi-ottetto più significativo del primo ottetto. Per ottenere un multiplo di ottetti, si devono inserire semi-ottetti a coda zero, secondo la necessità, a partire dalla prima posizione a sinistra del semi-ottetto nel primo ottetto.

Le cifre ammesse sono: 0, 1, .. 9.

2.8. **CalibrationPurpose**

Codice che spiega il motivo per cui è stata registrata una serie di parametri di taratura. Questo tipo di dati si riferisce ai requisiti 097 e 098 dell'allegato 1B e al requisito 119 dell'allegato 1C.

```
CalibrationPurpose ::= OCTET STRING (SIZE(1))
```

▼B

Assegnazione valore:

Prima generazione:

‘00’H	valore riservato,
‘01’H	attivazione: registrazione dei parametri di taratura noti al momento dell'attivazione della VU,
‘02’H	prima installazione: prima taratura della VU in seguito all'attivazione,
‘03’H	installazione: prima taratura della VU nel veicolo in cui è montata,
‘04’H	controllo periodico.

Seconda generazione:

Oltre alla prima generazione, sono utilizzati i valori seguenti:

‘05’H	inserimento del VRN da parte dell'azienda,
‘06’H	regolazione dell'ora senza taratura,

da ‘07’H a ‘7F’H RFU,

da ‘80’H a ‘FF’H Specifico del fabbricante.

2.9. **CardActivityDailyRecord**

Informazioni, memorizzate in una carta, relative all'attività del conducente per un determinato giorno di calendario. Questo tipo di dati si riferisce ai requisiti 266, 291, 320 e 343 dell'allegato 1C.

```
CardActivityDailyRecord ::= SEQUENCE {
   activityPreviousRecordLength         INTEGER(0..CardActivityLengthRange),
   activityRecordLength                 INTEGER(0..CardActivityLengthRange),
   activityRecordDate                   TimeReal,
   activityDailyPresenceCounter         DailyPresenceCounter,
   activityDayDistance                  Distance,
   activityChangeInfo                   SET SIZE(1..1440) OF ActivityChangeInfo
}
```

activityPreviousRecordLength è la lunghezza totale in byte della registrazione giornaliera precedente. Il valore massimo è dato dalla lunghezza della STRINGA DI OTTETTI contenente tali registrazioni (cfr. CardActivityLengthRange, appendice 2, paragrafo 4). Se questa registrazione è la registrazione giornaliera meno recente, il valore di activityPreviousRecordLength dev'essere impostato su 0.

activityRecordLength è la lunghezza totale in byte di questa registrazione. Il valore massimo è dato dalla lunghezza della STRINGA DI OTTETTI contenente tali registrazioni.

activityRecordDate è la data della registrazione.

▼B

activityDailyPresenceCounter è il contatore di presenza giornaliera per la carta nel giorno in questione.

activityDayDistance è la distanza totale percorsa nel giorno in questione.

activityChangeInfo è la serie di dati ActivityChangeInfo per il conducente nel giorno in questione. Può contenere un massimo di 1440 valori (un cambio di attività al minuto). La serie comprende sempre il valore activityChangeInfo relativo alla condizione del conducente alle 00h00.

2.10. **CardActivityLengthRange**

Numero di byte in una carta del conducente o dell'officina, disponibile per memorizzare le registrazioni relative all'attività del conducente.

```
CardActivityLengthRange ::= INTEGER(0..2^16-1)
```

Assegnazione valore: cfr. appendice 2.

2.11. **CardApprovalNumber**

Numero di omologazione della carta.

```
CardApprovalNumber ::= IA5String(SIZE(8))
```

Assegnazione valore:

Il numero di omologazione deve corrispondere a quanto pubblicato sul sito Internet della Commissione europea, vale a dire ad esempio compresi gli eventuali trattini. Il numero di omologazione deve essere allineato a sinistra.

2.12. **CardCertificate**

Prima generazione:

Certificato della chiave pubblica di una carta.

```
CardCertificate ::= Certificate
```

2.13. **CardChipIdentification**

Informazioni, memorizzate in una carta, relative all'identificazione del circuito integrato (IC) della carta (requisito 249 dell'allegato 1C). L'icSerialNumber unitamente all'icManufacturingReferences identifica il chip della carta in modo univoco. L'icSerialNumber di per sé non è sufficiente per identificare univocamente il chip della carta.

```
CardChipIdentification ::= SEQUENCE {
   icSerialNumber                    OCTET STRING (SIZE(4)),
   icManufacturingReferences         OCTET STRING (SIZE(4))
}
```

icSerialNumber è il numero di serie dell'IC.

icManufacturingReferences è l'identificativo specifico del fabbricante dell'IC.

2.14. **CardConsecutiveIndex**

Il codice di serie di una carta [definizione h)].

```
CardConsecutiveIndex ::= IA5String(SIZE(1))
```

Assegnazione valore: (cfr. allegato 1C, capitolo 7)

Ordine di incremento: ‘0, …, 9, A, …, Z, a, …, z’

▼B

2.15. **CardControlActivityDataRecord**

Informazioni, memorizzate in una carta del conducente o dell'officina, relative all'ultimo controllo cui è stato sottoposto il conducente (requisiti 274, 299, 327 e 350 dell'allegato 1C).

```
CardControlActivityDataRecord ::= SEQUENCE {
   controlType                          ControlType,
   controlTime                          TimeReal,
   controlCardNumber                    FullCardNumber,
   controlVehicleRegistration           VehicleRegistrationIdentification,
   controlDownloadPeriodBegin           TimeReal,
   controlDownloadPeriodEnd             TimeReal
}
```

controlType è il tipo di controllo.

controlTime è la data e l'ora del controllo.

controlCardNumber è il FullCardNumber dell'agente che ha effettuato il controllo.

controlVehicleRegistration contiene il VRN e lo Stato membro di immatricolazione del veicolo in cui è stato effettuato il controllo.

controlDownloadPeriodBegin e **controlDownloadPeriodEnd** specificano il periodo trasferito, in caso di trasferimento.

2.16. **CardCurrentUse**

Informazioni sull'uso effettivo della carta (requisiti 273, 298, 326 e 349 dell'allegato 1C).

```
CardCurrentUse ::= SEQUENCE {
   sessionOpenTime                      TimeReal,
   sessionOpenVehicle                   VehicleRegistrationIdentification
}
```

sessionOpenTime è l'ora in cui viene inserita la carta per l'uso corrente. Questo elemento viene azzerato all'atto dell'estrazione della carta.

sessionOpenVehicle è l'identificazione del veicolo in uso, impostata all'atto dell'inserimento della carta. Questo elemento viene azzerato all'atto dell'estrazione della carta.

2.17. **CardDriverActivity**

Informazioni, memorizzate in una carta del conducente o dell'officina, relative alle attività del conducente (requisiti 267, 268, 292, 293, 321 e 344 dell'allegato 1C).

```
CardDriverActivity ::= SEQUENCE {
   activityPointerOldestDayRecord       INTEGER(0.. CardActivityLengthRange-1),
   activityPointerNewestRecord          INTEGER(0.. CardActivityLengthRange-1),
   activityDailyRecords                 OCTET STRING
                                        (SIZE(CardActivityLengthRange))
}
```

activityPointerOldestDayRecord specifica il punto d'inizio della memorizzazione (numero di byte a partire dall'inizio della stringa) della registrazione completa meno recente del giorno nella stringa activityDailyRecords. Il valore massimo è dato dalla lunghezza della stringa.

▼B

activityPointerNewestRecord specifica il punto d'inizio della memorizzazione (numero di byte a partire dall'inizio della stringa) della registrazione più recente del giorno nella stringa activityDailyRecords. Il valore massimo è dato dalla lunghezza della stringa.

activityDailyRecords è lo spazio disponibile per memorizzare i dati relativi all'attività del conducente (struttura dei dati: CardActivityDailyRecord) per ogni giorno di calendario in cui è stata usata la carta.

Assegnazione valore: questa stringa di ottetti viene riempita ciclicamente con le registrazioni di CardActivityDailyRecord. Al primo impiego, la memorizzazione inizia a partire dal primo byte della stringa. Tutte le nuove registrazioni vengono aggiunte in coda alla precedente. Quando la stringa è piena, la memorizzazione prosegue a partire dal primo byte della stringa, indipendentemente dalla presenza di un'interruzione all'interno di un elemento di dati. Prima di inserire nella stringa nuovi dati relativi all'attività (ingrandendo l'activityDailyRecord corrente o inserendo un nuovo activityDailyRecord) per sostituire dati meno recenti, l'activityPointerOldestDayRecord deve essere aggiornato per tenere conto della nuova posizione della registrazione giornaliera completa meno recente, e l'activityPreviousRecordLength di questa (nuova) registrazione giornaliera completa meno recente deve essere riazzerato.

2.18. **CardDrivingLicenceInformation**

Informazioni, memorizzate in una carta del conducente, relative ai dati della patente di guida del titolare della carta (requisiti 259 e 284 dell'allegato 1C).

```
CardDrivingLicenceInformation ::= SEQUENCE {
   drivingLicenceIssuingAuthority       Name,
   drivingLicenceIssuingNation          NationNumeric,
   drivingLicenceNumber                 IA5String(SIZE(16))
}
```

drivingLicenceIssuingAuthority è l'autorità responsabile del rilascio della patente di guida.

drivingLicenceIssuingNation è la nazionalità dell'autorità che ha rilasciato la patente di guida.

drivingLicenceNumber è il numero della patente di guida.

2.19. **CardEventData**

Informazioni, memorizzate in una carta del conducente o dell'officina, relative alle anomalie associate al titolare della carta (requisiti 260, 285, 318 e 341 dell'allegato 1C).

```
CardEventData ::= SEQUENCE SIZE(6) OF {
   cardEventRecords                     SET SIZE(NoOfEventsPerType) OF
                                        CardEventRecord
}
```

CardEventData è una sequenza di cardEventRecords, ordinata in base al valore ascendente di EventFaultType (eccetto per le registrazioni relative ai tentativi di violazione della sicurezza, che sono raggruppate nell'ultima serie della sequenza).

cardEventRecords è una serie di registrazioni di anomalie di un determinato tipo (o categoria per le anomalie relative ai tentativi di violazione della sicurezza).

▼B

2.20. **CardEventRecord**

Informazioni, memorizzate in una carta del conducente o dell'officina, relative ad un'anomalia associata al titolare della carta (requisiti 261, 286, 318 e 341 dell'allegato 1C).

```
CardEventRecord ::= SEQUENCE {
   eventType                          EventFaultType,
   eventBeginTime                     TimeReal,
   eventEndTime                       TimeReal,
   eventVehicleRegistration           VehicleRegistrationIdentification
}
```

eventType è il tipo di anomalia.

eventBeginTime specifica la data e l'ora di inizio dell'anomalia.

eventEndTime specifica la data e l'ora di fine dell'anomalia.

eventVehicleRegistration contiene il VRN e lo Stato membro di immatricolazione del veicolo in cui si è verificata l'anomalia.

2.21. **CardFaultData**

Informazioni, memorizzate in una carta del conducente o dell'officina, relative ai guasti associati al titolare della carta (requisiti 263, 288, 318 e 341 dell'allegato 1C).

```
CardFaultData ::= SEQUENCE SIZE(2) OF {
   cardFaultRecords                   SET SIZE(NoOfFaultsPerType) OF
                                      CardFaultRecord
}
```

CardFaultData è una sequenza di una serie di registrazioni di guasti dell'apparecchio di controllo seguita dalla serie di registrazioni dei guasti della carta.

cardFaultRecords è una serie di registrazioni di guasti di una determinata categoria (apparecchio di controllo o carta).

2.22. **CardFaultRecord**

Informazioni, memorizzate in una carta del conducente o dell'officina, relative ad un guasto associato al titolare della carta (requisiti 264, 289, 318 e 341 dell'allegato 1C).

```
CardFaultRecord ::= SEQUENCE {
   faultType                          EventFaultType,
   faultBeginTime                     TimeReal,
   faultEndTime                       TimeReal,
   faultVehicleRegistration           VehicleRegistrationIdentification
}
```

faultType è il tipo di guasto.

faultBeginTime specifica la data e l'ora di inizio del guasto.

faultEndTime specifica la data e l'ora di fine del guasto.

faultVehicleRegistration contiene il VRN e lo Stato membro di immatricolazione del veicolo in cui si è verificato il guasto.

▼B

2.23. **CardIccIdentification**

Informazioni, memorizzate in una carta, relative all'identificazione della carta a circuito integrato (IC) (requisito 248 dell'allegato 1C).

```
CardIccIdentification ::= SEQUENCE {
   clockStop                          OCTET STRING (SIZE(1)),
   cardExtendedSerialNumber           ExtendedSerialNumber,
   cardApprovalNumber                 CardApprovalNumber,
   cardPersonaliserID                 ManufacturerCode,
   embedderIcAssemblerId              EmbedderIcAssemblerId,
   icIdentifier                       OCTET STRING (SIZE(2))
}
```

clockStop è la modalità «Clockstop», come definita nell'appendice 2.

cardExtendedSerialNumber contiene il numero di serie unico della carta IC, come ulteriormente specificato dal tipo di dati ExtendedSerial-Number.

cardApprovalNumber è il numero di omologazione della carta.

cardPersonaliserID è l'identificazione personalizzata della carta (ID) codificata come ManufacturerCode.

embedderIcAssemblerId fornisce informazioni circa l'assemblatore della carta IC.

icIdentifier è l'identificativo dell'IC sulla carta e del fabbricante dell'IC, come definita nella norma ISO/IEC 7816-6.

2.24. **CardIdentification**

Informazioni, memorizzate in una carta, relative all'identificazione della carta (requisiti 255, 280, 310, 333, 359, 365, 371 e 377 dell'allegato 1C).

```
CardIdentification ::= SEQUENCE {
   cardIssuingMemberState             NationNumeric,
   cardNumber                         CardNumber,
   cardIssuingAuthorityName           Name,
   cardIssueDate                      TimeReal,
   cardValidityBegin                  TimeReal,
   cardExpiryDate                     TimeReal
}
```

cardIssuingMemberState è il codice dello Stato membro che ha rilasciato la carta.

cardNumber è il numero della carta.

cardIssuingAuthorityName è il nome dell'autorità che ha rilasciato la carta.

cardIssueDate è la data di rilascio della carta all'attuale titolare.

cardValidityBegin è la data di inizio validità della carta.

cardExpiryDate è la data in cui termina la validità della carta.

▼B

2.25. **CardMACertificate**

Seconda generazione:

Certificato della chiave pubblica della carta per l'autenticazione reciproca con una VU. La struttura di tale certificato è specificata nell'appendice 11.

```
CardMACertificate ::= Certificate
```

2.26. **CardNumber**

Numero della carta, secondo la definizione g).

```
CardNumber ::= CHOICE {
   SEQUENCE {
      driverIdentification              IA5String(SIZE(14)),
      cardReplacementIndex              CardReplacementIndex,
      cardRenewalIndex                  CardRenewalIndex
   },
   SEQUENCE {
      ownerIdentification               IA5String(SIZE(13)),
      cardConsecutiveIndex              CardConsecutiveIndex,
      cardReplacementIndex              CardReplacementIndex,
      cardRenewalIndex                  CardRenewalIndex
   }
}
```

driverIdentification è l'identificazione univoca di un conducente in uno Stato membro.

ownerIdentification è l'identificazione univoca di un'impresa o di un'officina o di un organismo di controllo all'interno di uno Stato membro.

cardConsecutiveIndex è il codice di serie della carta.

cardReplacementIndex è il codice di sostituzione della carta.

cardRenewalIndex è il codice di rinnovo della carta.

La prima sequenza della scelta (CHOICE) è adatta a codificare il numero della carta del conducente, la seconda sequenza a codificare i numeri delle carte dell'officina, di controllo e dell'azienda.

2.27. **CardPlaceDailyWorkPeriod**

Informazioni, memorizzate in una carta del conducente o dell'officina, relative al luogo in cui inizia e/o termina il periodo di lavoro giornaliero (requisiti 272, 297, 325 e 348 dell'allegato 1C).

```
CardPlaceDailyWorkPeriod ::= SEQUENCE {
   placePointerNewestRecord    INTEGER(0 .. NoOfCardPlaceRecords-1),
   placeRecords                SET SIZE(NoOfCardPlaceRecords) OF PlaceRecord
}
```

placePointerNewestRecord è l'indice della registrazione più aggiornata del luogo.

Assegnazione valore: numero corrispondente al numeratore della registrazione del luogo, a partire da ′0′ per la prima volta in cui tale registrazione compare nella struttura.

placeRecords è la serie di registrazioni contenenti le informazioni relative ai luoghi inseriti.

▼B

2.28. **CardPrivateKey**

Prima generazione:

La chiave privata di una carta.

```
CardPrivateKey ::= RSAKeyPrivateExponent
```

2.29. **CardPublicKey**

La chiave pubblica di una carta.

```
CardPublicKey ::= PublicKey
```

2.30. **CardRenewalIndex**

Il codice di rinnovo di una carta [definizione i)].

```
CardRenewalIndex ::= IA5String(SIZE(1))
```

Assegnazione valore: (cfr. capitolo VII del presente allegato).

‘0’ Primo rilascio.

Ordine di incremento: ‘0, …, 9, A, …, Z’

2.31. **CardReplacementIndex**

Il codice di sostituzione di una carta [definizione j)].

```
CardReplacementIndex ::= IA5String(SIZE(1))
```

Assegnazione valore: (cfr. capitolo VII del presente allegato).

‘0’ Carta originale.

Ordine di incremento: ‘0, …, 9, A, …, Z’

2.32. **CardSignCertificate**

Seconda generazione:

Certificato della chiave pubblica della carta per la firma. La struttura di tale certificato è specificata nell'appendice 11.

```
CardSignCertificate ::= Certificate
```

2.33. **CardSlotNumber**

Codice usato per distinguere le due sedi (slot) di un'unità elettronica di bordo.

```
CardSlotNumber ::= INTEGER {
   driverSlot                          (0),
   co-driverSlot                       (1)
}
```

Assegnazione valore: nessun'altra specificazione.

2.34. **CardSlotsStatus**

Codice che indica il tipo di carta inserita nelle due sedi (slot) dell'unità elettronica di bordo.

```
CardSlotsStatus ::= OCTET STRING (SIZE(1))
```

▼B

Assegnazione valore — Allineato all'ottetto: ‘ccccdddd’B

‘cccc’B Identificazione del tipo di carta inserita nella sede (slot) «secondo conducente»,

‘dddd’B Identificazione del tipo di carta inserita nella sede (slot) “conducente”,

con i seguenti codici di identificazione:

‘0000’B carta non inserita,

‘0001’B carta del conducente inserita,

‘0010’B carta dell'officina inserita,

‘0011’B carta di controllo inserita,

‘0100’B carta dell'azienda inserita.

2.35. **CardSlotsStatusRecordArray**

Seconda generazione:

Il CardSlotsStatus più i metadati usati nel protocollo di trasferimento.

```
CardSlotsStatusRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF CardSlotsStatus
}
```

recordType rappresenta il tipo di registrazione (CardSlotsStatus). **Assegnazione valore**: Cfr. RecordType

recordSize sono le dimensioni di CardSlotsStatus in byte.

noOfRecords è il numero di registrazioni nella serie di registrazioni.

records è la serie di registrazioni del CardSlotsStatus.

2.36. **CardStructureVersion**

Codice che indica la versione della struttura utilizzata in una carta tachigrafica.

```
CardStructureVersion ::= OCTET STRING (SIZE(2))
```

Assegnazione valore: ‘aabb’H:

‘aa’H Indice per le modifiche della struttura.

‘00’H per le applicazioni di prima generazione

‘01’H per le applicazioni di seconda generazione

‘bb’H Indice per le modifiche riguardanti l'impiego degli elementi di dati definiti per la struttura data dal byte più significativo.

‘00’H per questa versione delle applicazioni di prima generazione

‘00’H per questa versione delle applicazioni di seconda generazione

▼B

2.37. **CardVehicleRecord**

Informazioni, memorizzate in una carta del conducente o dell'officina, relative al periodo d'impiego di un veicolo durante un giorno di calendario (requisiti 269, 294, 322 e 345 dell'allegato 1C).

Prima generazione:

```
CardVehicleRecord ::= SEQUENCE {
   vehicleOdometerBegin                    OdometerShort,
   vehicleOdometerEnd                      OdometerShort,
   vehicleFirstUse                         TimeReal,
   vehicleLastUse                          TimeReal,
   vehicleRegistration                     VehicleRegistrationIdentification,
   vuDataBlockCounter                      VuDataBlockCounter
}
```

vehicleOdometerBegin è il valore dell'odometro del veicolo all'inizio del periodo d'impiego del veicolo.

vehicleOdometerEnd è il valore dell'odometro del veicolo al termine del periodo d'impiego del veicolo.

vehicleFirstUse specifica la data e l'ora d'inizio del periodo d'impiego del veicolo.

vehicleLastUse specifica la data e l'ora di termine del periodo d'impiego del veicolo.

vehicleRegistration contiene il VRN e lo Stato membro di immatricolazione del veicolo.

vuDataBlockCounter è il valore del VuDataBlockCounter all'atto dell'ultima estrazione nel periodo d'impiego del veicolo.

Seconda generazione:

```
CardVehicleRecord ::= SEQUENCE {
   vehicleOdometerBegin                    OdometerShort,
   vehicleOdometerEnd                      OdometerShort,
   vehicleFirstUse                         TimeReal,
   vehicleLastUse                          TimeReal,
   vehicleRegistration                     VehicleRegistrationIdentification,
   vuDataBlockCounter                      VuDataBlockCounter,
   vehicleIdentificationNumber             VehicleIdentificationNumber
}
```

Oltre alla prima generazione, è utilizzato il seguente elemento di dati:

VehicleIdentificationNumber è il numero di identificazione del veicolo che si riferisce al veicolo nel suo complesso.

2.38. **CardVehiclesUsed**

Informazioni, memorizzate in una carta del conducente o dell'officina, relative ai veicoli usati dal titolare della carta (requisiti 270, 295, 323 e 346 dell'allegato 1C).

```
CardVehiclesUsed := SEQUENCE {
   vehiclePointerNewestRecord          INTEGER(0..NoOfCardVehicleRecords-1),
   cardVehicleRecords                  SET SIZE(NoOfCardVehicleRecords) OF
                                       CardVehicleRecord
}
```

vehiclePointerNewestRecord è l'indice della registrazione più aggiornata del veicolo.

▼B

Assegnazione valore: numero corrispondente al numeratore della registrazione del veicolo, a partire da ′0′ per la prima volta in cui tale registrazione compare nella struttura.

cardVehicleRecords è la serie di registrazioni contenenti le informazioni relative ai veicoli utilizzati.

2.39. **CardVehicleUnitRecord**

Seconda generazione:

Informazioni, memorizzate in una carta del conducente o dell'officina, relative ad un'unità elettronica di bordo utilizzata (requisiti 303 e 351 dell'allegato 1C).

```
CardVehicleUnitRecord ::= SEQUENCE {
   timeStamp                              TimeReal,
   manufacturerCode                       ManufacturerCode,
   deviceID                               INTEGER(0..255),
   vuSoftwareVersion                      VuSoftwareVersion
}
```

timeStampindica l'inizio del periodo d'impiego dell'unità elettronica di bordo (cioè il primo inserimento della carta nell'unità elettronica di bordo per il periodo).

manufacturerCode identifica il fabbricante dell'unità elettronica di bordo.

deviceID identifica il tipo di unità elettronica di bordo di un fabbricante. Il valore è specifico del fabbricante.

vuSoftwareVersion è il numero della versione del software dell'unità elettronica di bordo.

2.40. **CardVehicleUnitsUsed**

Seconda generazione:

Informazioni, memorizzate in una carta del conducente o dell'officina, relative alle unità elettroniche di bordo usate dal titolare della carta (requisiti 306 e 352 dell'allegato 1C).

```
CardVehicleUnitsUsed := SEQUENCE {
   vehicleUnitPointerNewestRecord       INTEGER(0..NoOfCardVehicleUnitRecords-1),
   cardVehicleUnitRecords               SET SIZE(NoOfCardVehicleUnitRecords) OF
                                        CardVehicleUnitRecord
}
```

vehicleUnitPointerNewestRecord è l'indice della registrazione più aggiornata dell'unità elettronica di bordo.

Assegnazione valore: numero corrispondente al numeratore della registrazione dell'unità elettronica di bordo, a partire da ‘0’ per la prima volta in cui tale registrazione compare nella struttura.

cardVehicleUnitRecords è la serie di registrazioni contenenti le informazioni relative alle unità elettroniche di bordo utilizzate.

2.41. **Certificate**

Il certificato di una chiave pubblica rilasciato da un'autorità di certificazione.

Prima generazione:

```
Certificate ::= OCTET STRING (SIZE(194))
```

▼B

Assegnazione valore: firma digitale con recupero parziale di un CertificateContent, secondo i meccanismi comuni di sicurezza di cui all'appendice 11: firma (128 byte) resto chiave pubblica (58 byte) riferimento dell'autorità di certificazione (8 byte).

Seconda generazione:

```
Certificate ::= OCTET STRING (SIZE(204..341))
```

Assegnazione valore: v. appendice 11

2.42. **CertificateContent**

Prima generazione:

Il contenuto (in chiaro) del certificato di una chiave pubblica, secondo i meccanismi comuni di sicurezza di cui all'appendice 11.

```
CertificateContent ::= SEQUENCE {
   certificateProfileIdentifier          INTEGER(0..255),
   certificationAuthorityReference       KeyIdentifier,
   certificateHolderAuthorisation        CertificateHolderAuthorisation,
   certificateEndOfValidity              TimeReal,
   certificateHolderReference            KeyIdentifier,
   publicKey                             PublicKey
}
```

certificateProfileIdentifier è la versione del certificato corrispondente.

Assegnazione valore: '01h' per questa versione.

certificationAuthorityReference identifica l'autorità di certificazione che ha rilasciato il certificato. Fornisce inoltre il riferimento della chiave pubblica di tale autorità.

certificateHolderAuthorisation identifica i diritti del titolare del certificato.

certificateEndOfValidity è la data di scadenza amministrativa del certificato.

certificateHolderReference identifica il titolare del certificato. Fornisce inoltre il riferimento della chiave pubblica del titolare.

publicKey è la chiave pubblica per la quale è stato rilasciato il certificato in questione.

2.43. **CertificateHolderAuthorisation**

Identificazione dei diritti del titolare di un certificato.

```
CertificateHolderAuthorisation ::= SEQUENCE {
   tachographApplicationID              OCTET STRING(SIZE(6))
   equipmentType                        EquipmentType
}
```

Prima generazione:

tachographApplicationID è l'identificativo di applicazione dell'applicazione del tachigrafo.

Assegnazione valore: 'FFh' '54h' '41h' '43h' '48h' '4Fh'. Si tratta di un identificativo di applicazione di proprietà riservata, non registrata, secondo ISO/IEC 7816-5.

equipmentType è l'identificazione del tipo di apparecchio cui è destinato il certificato.

Assegnazione valore: in conformità al tipo di dati EquipmentType. **0** se si tratta del certificato di uno Stato membro.

▼B

Seconda generazione:

tachographApplicationID rappresenta i 6 byte più significativi dell'identificativo di applicazione (AID) della carta tachigrafica di seconda generazione. L'AID dell'applicazione della carta tachigrafica è specificato al capitolo 6.2.

Assegnazione valore: 'FF 53 4D 52 44 54'.

equipmentType è l'identificazione del tipo di apparecchio, specificato per la seconda generazione, cui è destinato il certificato.

Assegnazione valore: in conformità al tipo di dati EquipmentType.

2.44. **CertificateRequestID**

Identificazione univoca di una richiesta di certificato. Si può anche usare come identificativo della chiave pubblica di un'unità elettronica di bordo, nel caso in cui il numero di serie dell'unità elettronica di bordo cui è destinata la chiave non sia noto al momento della generazione del certificato.

```
CertificateRequestID ::= SEQUENCE{
   requestSerialNumber                  INTEGER(0..2^32-1),
   requestMonthYear                     BCDString(SIZE(2)),
   crIdentifier                         OCTET STRING(SIZE(1)),
   manufacturerCode                     ManufacturerCode
}
```

requestSerialNumber è un numero di serie per la richiesta di certificato, associato univocamente al fabbricante e al mese di cui sotto.

requestMonthYear è l'identificazione del mese e dell'anno di richiesta del certificato.

Assegnazione valore: codifica BCD del mese (due cifre) e dell'anno (ultime due cifre).

crIdentifier: è un identificativo usato per distinguere una richiesta di certificato da un numero di serie completo.

Assegnazione valore: 'FFh'.

manufacturerCode: è il codice numerico del fabbricante che ha richiesto il certificato.

2.45. **CertificationAuthorityKID**

Identificativo della chiave pubblica di un'autorità di certificazione (di uno Stato membro o dell'autorità europea di certificazione).

```
CertificationAuthorityKID ::= SEQUENCE{
   nationNumeric                        NationNumeric,
   nationAlpha                          NationAlpha,
   keySerialNumber                      INTEGER(0..255),
   additionalInfo                       OCTET STRING(SIZE(2)),
   caIdentifier                         OCTET STRING(SIZE(1))
}
```

nationNumeric è il codice numerico del paese dell'autorità di certificazione.

nationAlpha è il codice alfanumerico del paese dell'autorità di certificazione.

▼B

keySerialNumber è un numero di serie usato per distinguere le diverse chiavi dell'autorità di certificazione in caso di cambio di chiavi.

additionalInfo è un campo a due byte per codifiche supplementari (a cura dell'autorità di certificazione).

caIdentifier è un identificativo usato per distinguere l'identificativo della chiave di un'autorità di certificazione dagli identificativi di altre chiavi.

Assegnazione valore: '01h'.

2.46. **CompanyActivityData**

Informazioni, memorizzate in una carta dell'azienda, relative alle attività eseguite con la carta (requisiti 373 e 379 dell'allegato 1C).

```
CompanyActivityData ::= SEQUENCE {
   companyPointerNewestRecord        INTEGER(0..NoOfCompanyActivityRecords-1),
   companyActivityRecords            SET SIZE(NoOfCompanyActivityRecords) OF
    companyActivityRecord             SEQUENCE {
     companyActivityType               CompanyActivityType,
     companyActivityTime               TimeReal,
     cardNumberInformation             FullCardNumber,
     vehicleRegistrationInformation    VehicleRegistrationIdentification,
     downloadPeriodBegin               TimeReal,
     downloadPeriodEnd                 TimeReal
    }
}
```

companyPointerNewestRecord è l'indice del companyActivityRecord più aggiornato.

Assegnazione valore: numero corrispondente al numeratore della registrazione delle attività dell'impresa, a partire da '0' per la prima volta in cui tale registrazione compare nella struttura.

companyActivityRecords è la serie di tutte le registrazioni delle attività dell'impresa.

companyActivityRecord è la sequenza di informazioni relative ad un'attività dell'impresa.

companyActivityType è il tipo di attività dell'impresa.

companyActivityTime specifica la data e l'ora dell'attività dell'impresa.

cardNumberInformation contiene il numero della carta e lo Stato membro che ha rilasciato la carta da cui sono stati trasferiti i dati, se pertinente.

vehicleRegistrationInformation contiene il VRN e lo Stato membro di immatricolazione del veicolo da cui sono stati trasferiti i dati o in cui è stato attivato o disattivato un blocco.

downloadPeriodBegin e **downloadPeriodEnd** specificano il periodo cui si riferisce il trasferimento dei dati della VU, se pertinente.

2.47. **CompanyActivityType**

Codice che indica un'attività eseguita da un'impresa utilizzando la propria carta dell'azienda.

```
CompanyActivityType ::= INTEGER {
   card downloading                  (1),
   VU downloading                    (2),
   VU lock-in                        (3),
   VU lock-out                       (4)
}
```

▼B

2.48. **CompanyCardApplicationIdentification**

Informazioni, memorizzate in una carta dell'azienda, relative all'identificazione dell'applicazione della carta (requisiti 369 e 375 dell'allegato 1C).

```
CompanyCardApplicationIdentification ::= SEQUENCE {
   typeOfTachographCardId               EquipmentType,
   cardStructureVersion                 CardStructureVersion,
   noOfCompanyActivityRecords           NoOfCompanyActivityRecords
}
```

typeOfTachographCardId specifica il tipo di carta.

cardStructureVersion specifica la versione della struttura utilizzata nella carta.

noOfCompanyActivityRecords è il numero di registrazioni delle attività dell'impresa che la carta è in grado di memorizzare.

2.49. **CompanyCardHolderIdentification**

Informazioni, memorizzate in una carta dell'azienda, relative all'identificazione del titolare della carta (requisiti 372 e 378 dell'allegato 1C).

```
CompanyCardHolderIdentification ::= SEQUENCE {
   companyName                          Name,
   companyAddress                       Address,
   cardHolderPreferredLanguage          Language
}
```

companyName è il nome dell'impresa titolare.

companyAddress è l'indirizzo dell'impresa titolare.

cardHolderPreferredLanguage è la lingua abituale del titolare della carta.

2.50. **ControlCardApplicationIdentification**

Informazioni, memorizzate in una carta di controllo, relative all'identificazione dell'applicazione della carta (requisiti 357 e 363 dell'allegato 1C).

```
ControlCardApplicationIdentification ::= SEQUENCE {
   typeOfTachographCardId               EquipmentType,
   cardStructureVersion                 CardStructureVersion,
   noOfControlActivityRecords           NoOfControlActivityRecords
}
```

typeOfTachographCardId specifica il tipo di carta.

cardStructureVersion specifica la versione della struttura utilizzata nella carta.

noOfControlActivityRecords è il numero di registrazioni di attività di controllo che la carta è in grado di memorizzare.

▼B

2.51. **ControlCardControlActivityData**

Informazioni, memorizzate in una carta di controllo, relative all'attività di controllo eseguita con la carta (requisiti 361 e 367 dell'allegato 1C).

```
ControlCardControlActivityData ::= SEQUENCE {
   controlPointerNewestRecord        INTEGER(0.. NoOfControlActivityRecords-1),
   controlActivityRecords            SET SIZE(NoOfControlActivityRecords) OF
    controlActivityRecord             SEQUENCE {
      controlType                      ControlType,
      controlTime                      TimeReal,
      controlledCardNumber             FullCardNumber,
      controlledVehicleRegistration    VehicleRegistrationIdentification,
      controlDownloadPeriodBegin       TimeReal,
      controlDownloadPeriodEnd         TimeReal
    }
}
```

controlPointerNewestRecord è l'indice della registrazione più aggiornata dell'attività di controllo.

Assegnazione valore: numero corrispondente al numeratore della registrazione dell'attività di controllo, a partire da '0' per la prima volta in cui tale registrazione compare nella struttura.

controlActivityRecords è la serie di tutte le registrazioni delle attività di controllo.

controlActivityRecord è la sequenza di informazioni relative ad un controllo.

controlType è il tipo di controllo.

controlTime è la data e l'ora del controllo.

controlledCardNumber contiene il numero della carta e lo Stato membro che ha rilasciato la carta sottoposta al controllo.

controlledVehicleRegistration contiene il VRN e lo Stato membro di immatricolazione del veicolo in cui è stato effettuato il controllo.

controlDownloadPeriodBegin e **controlDownloadPeriodEnd** specificano il periodo trasferito, in caso di trasferimento.

2.52. **ControlCardHolderIdentification**

Informazioni, memorizzate in una carta di controllo, relative all'identificazione del titolare della carta (requisiti 360 e 366 dell'allegato 1C).

```
ControlCardHolderIdentification ::= SEQUENCE {
   controlBodyName                    Name,
   controlBodyAddress                 Address,
   cardHolderName                     HolderName,
   cardHolderPreferredLanguage        Language
}
```

controlBodyName è il nome dell'organismo di controllo del titolare della carta.

controlBodyAddress è l'indirizzo dell'organismo di controllo del titolare della carta.

cardHolderName contiene cognome e nome/i del titolare della carta di controllo.

▼B

cardHolderPreferredLanguage è la lingua abituale del titolare della carta.

2.53. **ControlType**

Codice che indica le attività eseguite durante un controllo. Questo tipo di dati si riferisce ai requisiti 126, 274, 299, 327 e 350 dell'allegato 1C.

```
ControlType ::= OCTET STRING (SIZE(1))
```

Prima generazione:

Assegnazione valore — **Allineato all'ottetto**: ‘cvpdxxxx’B (8 bit)

‘c’B trasferimento dati carta:

‘0’B: dati carta non trasferiti durante l'attività di controllo,

‘1’B: ‘1’B: dati carta trasferiti durante l'attività di controllo

‘v’B trasferimento dati VU:

‘0’B: dati VU non trasferiti durante l'attività di controllo,

‘1’B: dati VU trasferiti durante l'attività di controllo

‘p’B stampa:

‘0’B: stampa non eseguita durante l'attività di controllo,

‘1’B: stampa eseguita durante l'attività di controllo

‘d’B visualizzazione:

‘0’B: visualizzazione non utilizzata durante l'attività di controllo,

‘1’B: visualizzazione utilizzata durante l'attività di controllo

‘xxxx’B Non usato.

Seconda generazione:

Assegnazione valore — **Allineato all'ottetto**: ‘cvpdexxx’B (8 bit)

‘c’B trasferimento dati carta:

‘0’B: dati carta non trasferiti durante l'attività di controllo,

‘1’B: ‘1’B: dati carta trasferiti durante l'attività di controllo

‘v’B trasferimento dati VU:

‘0’B: dati VU non trasferiti durante l'attività di controllo,

‘1’B: dati VU trasferiti durante l'attività di controllo

‘p’B stampa:

‘0’B: stampa non eseguita durante l'attività di controllo,

‘1’B: stampa eseguita durante l'attività di controllo

▼B

‘d’B	visualizzazione:
	‘0’B: visualizzazione non utilizzata durante l'attività di controllo,
	‘1’B: visualizzazione utilizzata durante l'attività di controllo
‘e’B	verifica della taratura su strada,
	‘0’B: parametri di taratura non controllati durante l'attività di controllo,
	‘1’B: parametri di taratura controllati durante l'attività di controllo
‘xxx’B	RFU.

2.54. **CurrentDateTime**

La data e l'ora correnti dell'apparecchio di controllo.

```
CurrentDateTime ::= TimeReal
```

Assegnazione valore: nessun'altra specificazione.

2.55. **CurrentDateTimeRecordArray**

Seconda generazione:

La data e l'ora correnti più i metadati usati nel protocollo di trasferimento.

```
CurrentDateTimeRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF CurrentDateTime
}
```

recordType rappresenta il tipo di registrazione (CurrentDateTime). **Assegnazione valore**: Cfr. RecordType

recordSize sono le dimensioni di CurrentDateTime in byte.

noOfRecords è il numero di registrazioni nella serie di registrazioni.

records è una serie di registrazioni di data e ora correnti.

2.56. **DailyPresenceCounter**

Un contatore, memorizzato in una carta del conducente o dell'officina, incrementato di un'unità per ogni giorno di calendario in cui la carta viene inserita in una VU. Questo tipo di dati si riferisce ai requisiti 266, 299, 320 e 343 dell'allegato 1C.

```
DailyPresenceCounter ::= BCDString(SIZE(2))
```

Assegnazione valore: numero consecutivo con valore massimo = 9 999, anche in questo caso a partire da 0. All'atto del primo rilascio della carta il numero è impostato su 0.

▼B

2.57. **Datef**

Data espressa in un formato numerico idoneo alla stampa.

```
Datef ::= SEQUENCE {
   year        BCDString(SIZE(2)),
   month       BCDString(SIZE(1)),
   day         BCDString(SIZE(1))
}
```

Assegnazione valore:

yyyy	Anno
mm	Mese
dd	Giorno
‘00000000’H	denota esplicitamente l'assenza di data.

2.58. **DateOfDayDownloaded**

Seconda generazione:

la data e l'ora del trasferimento.

```
DateOfDayDownloaded ::= TimeReal
```

Assegnazione valore: nessun'altra specificazione.

2.59. **DateOfDayDownloadedRecordArray**

Seconda generazione:

La data e l'ora del trasferimento più i metadati usati nel protocollo di trasferimento.

```
DateofDayDownloadedRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF
                                       DateOfDayDownloaded
}
```

recordType rappresenta il tipo di registrazione (DateOfDayDownloaded). **Assegnazione valore**: Cfr. RecordType

recordSize sono le dimensioni di CurrentDateTime in byte.

noOfRecords è il numero di registrazioni nella serie di registrazioni.

records è la serie di data e ora delle registrazioni dei trasferimenti.

2.60. **Distance**

Una distanza percorsa (risultante dal calcolo della differenza tra due valori dell'odometro del veicolo espressi in chilometri).

```
Distance ::= INTEGER(0..2^16-1)
```

Assegnazione valore: binario senza segno. Valore in km nell'intervallo operativo 0-9 999 km.

2.61. **DriverCardApplicationIdentification**

Informazioni, memorizzate in una carta del conducente, relative all'identificazione dell'applicazione della carta (requisiti 253 e 278 dell'allegato 1C).

▼B

Prima generazione:

```
DriverCardApplicationIdentification ::= SEQUENCE {
   typeOfTachographCardId              EquipmentType,
   cardStructureVersion                CardStructureVersion,
   noOfEventsPerType                   NoOfEventsPerType,
   noOfFaultsPerType                   NoOfFaultsPerType,
   activityStructureLength             CardActivityLengthRange,
   noOfCardVehicleRecords              NoOfCardVehicleRecords,
   noOfCardPlaceRecords                NoOfCardPlaceRecords
}
```

typeOfTachographCardId specifica il tipo di carta.

cardStructureVersion specifica la versione della struttura utilizzata nella carta.

noOfEventsPerType è il numero di anomalie per tipo di anomalia che la carta è in grado di registrare.

noOfFaultsPerType è il numero di guasti per tipo di guasto che la carta è in grado di registrare.

activityStructureLength indica il numero di byte disponibili per memorizzare le registrazioni delle attività.

noOfCardVehicleRecords è il numero di registrazioni del veicolo che la carta è in grado di contenere.

noOfCardPlaceRecords è il numero di luoghi che la carta è in grado di registrare.

Seconda generazione:

```
DriverCardApplicationIdentification ::= SEQUENCE {
   typeOfTachographCardId              EquipmentType,
   cardStructureVersion                CardStructureVersion,
   noOfEventsPerType                   NoOfEventsPerType,
   noOfFaultsPerType                   NoOfFaultsPerType,
   activityStructureLength             CardActivityLengthRange,
   noOfCardVehicleRecords              NoOfCardVehicleRecords,
   noOfCardPlaceRecords                NoOfCardPlaceRecords,
   noOfGNSSCDRecords                   NoOfGNSSCDRecords,
   noOfSpecificConditionRecords        NoOfSpecificConditionRecords
}
```

Oltre alla prima generazione, sono utilizzati i seguenti elementi di dati:

noOfGNSSCDRecords è il numero di registrazioni di guida continua del GNSS che la carta è in grado di memorizzare.

noOfSpecificConditionRecords è il numero di registrazioni di condizioni particolari che la carta è in grado di memorizzare.

2.62. **DriverCardHolderIdentification**

Informazioni, memorizzate in una carta del conducente, relative all'identificazione del titolare della carta (requisiti 256 e 281 dell'allegato 1C).

```
DriverCardHolderIdentification ::= SEQUENCE {
   cardHolderName                      HolderName,
   cardHolderBirthDate                 Datef,
   cardHolderPreferredLanguage         Language
}
```

▼B

cardHolderName contiene cognome e nome/i del titolare della carta del conducente.

cardHolderBirthDate è la data di nascita del titolare della carta del conducente.

cardHolderPreferredLanguage è la lingua abituale del titolare della carta.

2.63. **DSRCSecurityData**

Seconda generazione:

Le informazioni in testo normale e il MAC da trasmettere tramite DSRC dal tachigrafo all'interrogatore a distanza (RI). Per maggiori dettagli, cfr. appendice 11, parte B, capitolo 13.

```
DSRCSecurityData ::= SEQUENCE {
   tagLenthPlainText                    OCTET STRING(SIZE(2)),
   currentDateTime                      CurrentDateTime,
   counter                              INTEGER(0..2^24-1),
   vuSerialNumber                       VuSerialNumber,
   dSRCMKVersionNumber                  INTEGER(SIZE(1)),
   tagLengthMac                         OCTET STRING(SIZE(2)),
   mac                                  MAC
}
```

tagLength fa parte della codifica DER-TLV e va fissata a '81 10' (cfr. appendice 11, parte B, capitolo 13).

currentDateTime specifica la data e l'ora correnti dell'unità elettronica di bordo.

counter elenca i messaggi RTM.

vuSerialNumber è il numero di serie dell'unità elettronica di bordo.

dSRCMKVersionNumber è il numero della versione della Master Key del DSRC da cui derivano le chiavi DSRC specifiche della VU.

tagLengthMa definisce il codice e la lunghezza dell'oggetto di dati del MAC come parte della codifica DER-TLV. Il codice va impostato su '8E' e la lunghezza deve codificare la lunghezza del MAC in ottetti (cfr. appendice 11, parte B, capitolo 13).

mac è il MAC calcolato sul messaggio RTM (cfr. appendice 11, parte B, capitolo 13).

2.64. **EGFCertificate**

Seconda generazione:

Certificato della chiave pubblica del dispositivo GNSS esterno per l'autenticazione reciproca con una VU. La struttura di tale certificato è specificata nell'appendice 11.

```
EGFCertificate ::= Certificate
```

▼B

2.65. **EmbedderIcAssemblerId**

Fornisce informazioni sull'assemblatore della carta IC.

```
EmbedderIcAssemblerId ::= SEQUENCE{
   countryCode                          IA5String(SIZE(2)),
   moduleEmbedder                       BCDString(SIZE(2)),
   manufacturerInformation              OCTET STRING(SIZE(1))
}
```

countryCode è il codice paese di 2 lettere dell'assemblatore del modulo in conformità alla norma ISO 3166.

moduleEmbedder identifica l'assemblatore del modulo.

manufacturerInformation ad uso interno del fabbricante.

2.66. **EntryTypeDailyWorkPeriod**

Codice usato per distinguere inizio e termine dell'immissione del luogo di un periodo di lavoro giornaliero e la condizione dell'immissione.

Prima generazione

```
EntryTypeDailyWorkPeriod ::= INTEGER {
   Begin,  related time = card insertion time or time of entry          (0),
   End,    related time = card withdrawal time or time of entry        (1),
   Begin,  related time manually entered (start time)                  (2),
   End,    related time manually entered (end of work period)          (3),
   Begin,  related time assumed by VU                                  (4),
   End,    related time assumed by VU                                  (5)
}
```

Assegnazione valore: secondo ISO/IEC8824-1.

Seconda generazione

```
EntryTypeDailyWorkPeriod ::= INTEGER {
   Begin,  related time = card insertion time or time of entry          (0),
   End,    related time = card withdrawal time or time of entry        (1),
   Begin,  related time manually entered (start time)                  (2),
   End,    related time manually entered (end of work period)          (3),
   Begin,  related time assumed by VU                                  (4),
   End,    related time assumed by VU                                  (5),
   Begin,  related time based on GNSS data                             (6),
   End     related time based on GNSS data                             (7)
}
```

Assegnazione valore: secondo ISO/IEC8824-1.

2.67. **EquipmentType**

Codice usato per distinguere i diversi tipi di apparecchio per l'applicazione tachigrafica.

```
EquipmentType ::= INTEGER(0..255)
```

▼B

Prima generazione:

```
 --Reserved                              (0),
 --Driver Card                           (1),
 --Workshop Card                         (2),
 --Control Card                          (3),
 --Company Card                          (4),
 --Manufacturing Card                    (5),
 --Vehicle Unit                          (6),
 --Motion Sensor                         (7),
 --RFU                                   (8..255)
```

Assegnazione valore: secondo ISO/IEC8824-1.

Il valore 0 è riservato; serve ad indicare uno Stato membro o l'Europa nel campo CHA dei certificati.

Seconda generazione:

Si usano gli stessi valori della prima generazione con le seguenti aggiunte:

```
--GNSS Facility                         (8),
--Remote Communication Module           (9),
--ITS interface module                  (10),
--Plaque                                (11), -- may be used in SealRecord
--M1/N1 Adapter                         (12), -- may be used in SealRecord
--European Root CA (ERCA)               (13),
--Member State CA (MSCA)                (14),
--External GNSS connection              (15), -- may be used in SealRecord
--Unused                                (16), -- used in SealDataVu
--RFU                                   (17..255)
```

Nota: I valori della seconda generazione per la targa, l'adattatore e la connessione del dispositivo GNSS esterno e i valori della prima generazione per l'unità elettronica di bordo e il sensore di movimento possono essere utilizzati in SealRecord, se del caso.

2.68. **EuropeanPublicKey**

Prima generazione:

La chiave pubblica europea.

```
EuropeanPublicKey ::= PublicKey
```

2.69. **EventFaultRecordPurpose**

Codice che spiega il motivo per cui sono stati registrati un'anomalia o un guasto.

```
EventFaultRecordPurpose ::= OCTET STRING (SIZE(1))
```

Assegnazione valore:

'00'H	una delle 10 anomalie o dei 10 guasti più recenti (o ultimi)
'01'H	l'anomalia più lunga per uno degli ultimi 10 giorni in cui si è verificata
'02'H	una delle 5 anomalie più lunghe nel corso degli ultimi 365 giorni
'03'H	l'ultima anomalia per uno degli ultimi 10 giorni in cui si è verificata
'04'H	l'anomalia più grave per uno degli ultimi 10 giorni in cui si è verificata
'05'H	una delle 5 anomalie più gravi nel corso degli ultimi 365 giorni
'06'H	la prima anomalia o il primo guasto che si è verificato dopo l'ultima taratura
'07'H	un'anomalia o un guasto attivo/in atto
'08'H to '7F'H	RFU
'80'H to 'FF'H	specifico del fabbricante

▼B

2.70. **EventFaultType**

Codice che identifica un'anomalia o un guasto.

```
EventFaultType ::= OCTET STRING (SIZE(1))
```

Assegnazione valore:

Prima generazione:

'0x'H	Anomalie generali,
'00'H	Nessun'altra informazione,
'01'H	Inserimento di una carta non valida,
'02'H	Conflitto di carte,
'03'H	Sovrapposizione di orari,
'04'H	Guida in assenza di una carta adeguata;
'05'H	Inserimento carta durante la guida,
'06'H	Chiusura errata ultima sessione carta,
'07'H	Superamento di velocità,
'08'H	Interruzione dell'alimentazione di energia,
'09'H	Errore dei dati di movimento,
'0A'H	Dati contrastanti sul movimento del veicolo,
'0B' to '0F'H	RFU,

'1x'H	Anomalie relative a tentativi di violazione della sicurezza riguardanti l'unità elettronica di bordo,
'10'H	Nessun'altra informazione,
'11'H	Mancata autenticazione del sensore di movimento,
'12'H	Mancata autenticazione della carta tachigrafica,
'13'H	Cambiamento non autorizzato di sensore di movimento,
'14'H	Errore di integrità nell'immissione dei dati della carta,
'15'H	Errore di integrità dei dati dell'utente memorizzati,
'16'H	Errore nel trasferimento interno di dati,
'17'H	Apertura non autorizzata dell'involucro,
'18'H	Sabotaggio di elementi hardware,
'19'H to '1F'H	RFU,

'2x'H	Anomalie relative a tentativi di violazione della sicurezza riguardanti il sensore,
'20'H	Nessun'altra informazione,
'21'H	Autenticazione fallita,
'22'H	Errore di integrità dei dati memorizzati,
'23'H	Errore nel trasferimento interno di dati,
'24'H	Apertura non autorizzata dell'involucro,
'25'H	Sabotaggio di elementi hardware,
'26'H to '2F'H	RFU,

'3x'H	Guasti dell'apparecchio di controllo,
'30'H	Nessun'altra informazione,
'31'H	Guasto all'interno della VU,
'32'H	Guasto della stampante,
'33'H	Guasto del dispositivo di visualizzazione,
'34'H	Guasto nel trasferimento di dati,
'35'H	Guasto del sensore,
'36'H to '3F'H	RFU,

'4x'H	Guasti della carta,
'40'H	Nessun'altra informazione,
'41'H to '4F'H	RFU,

'50'H to '7F'H	RFU,

'80'H to 'FF'H	Specifico del fabbricante.

▼B

Seconda generazione:

Si usano gli stessi valori della prima generazione con le seguenti aggiunte:

'0B'H	Conflitto di orari (orologio interno del GNSS e orologio interno della VU),
'0C' to '0F'H	RFU,
'5x'H	guasti associati al GNSS,
'50'H	Nessun'altra informazione,
'51'H	Guasto al ricevitore del GNSS interno,
'52'H	Guasto al ricevitore del GNSS esterno,
'53'H	Guasto alla comunicazione del GNSS esterno,
'54'H	Nessun dato sulla posizione dal GNSS,
'55'H	Individuazione di manomissione del GNSS,
'56'H	Certificato del dispositivo GNSS esterno scaduto,
'57'H to '5F'H	RFU,
'6x'H	Guasti connessi al modulo di comunicazione remota,
'60'H	Nessun'altra informazione,
'61'H	Guasto al modulo di comunicazione remota,
'62'H	Guasto alla comunicazione del modulo di comunicazione remota,
'63'H to '6F'H	RFU,
'7x'H	Guasti all'interfaccia ITS,
'70'H	Nessun'altra informazione,
'71'H to '7F'H	RFU.

2.71. **ExtendedSealIdentifier**

Seconda generazione:

L'identificativo completo del sigillo identifica in modo univoco un sigillo (requisito 401 dell'allegato 1C).

```
ExtendedSealIdentifier ::= SEQUENCE{
   manufacturerCode                    OCTET STRING (SIZE(2)),
   sealIdentifier                      OCTET STRING (SIZE(6))
}
```

manufacturerCode è un codice del fabbricante del sigillo.

sealIdentifier è un identificativo del sigillo che è unico per il fabbricante.

2.72. **ExtendedSerialNumber**

Identificazione univoca di un apparecchio. Si può anche usare come identificativo della chiave pubblica di un apparecchio.

Prima generazione:

```
ExtendedSerialNumber ::= SEQUENCE{
   serialNumber                        INTEGER(0..2^32-1),
   monthYear                           BCDString(SIZE(2)),
   type                                OCTET STRING(SIZE(1)),
   manufacturerCode                    ManufacturerCode
}
```

serialNumber è un numero di serie dell'apparecchio, univocamente associato al fabbricante, al tipo di apparecchio e al mese e all'anno di cui sotto.

monthYear è l'identificazione del mese e dell'anno di fabbricazione (o di assegnazione del numero di serie).

▼B

Assegnazione valore: codifica BCD del mese (due cifre) e dell'anno (ultime due cifre).

type è un identificativo del tipo di apparecchio.

Assegnazione valore: specifico del fabbricante, con valore riservato 'FFh'.

manufacturerCode: è il codice numerico che identifica un fabbricante di un apparecchio omologato.

Seconda generazione:

```
ExtendedSerialNumber ::= SEQUENCE{
   serialNumber                          INTEGER(0..2^32-1),
   monthYear                             BCDString(SIZE(2)),
   type                                  EquipmentType,
   manufacturerCode                      ManufacturerCode
}
```

serialNumber cfr. prima generazione

monthYear cfr. prima generazione

type indica il tipo di apparecchio

manufacturerCode: cfr. prima generazione.

2.73. **FullCardNumber**

Codice per l'identificazione completa di una carta tachigrafica.

```
FullCardNumber ::= SEQUENCE {
   cardType                              EquipmentType,
   cardIssuingMemberState                NationNumeric,
   cardNumber                            CardNumber
}
```

cardType è il tipo di carta tachigrafica.

cardIssuingMemberState è il codice dello Stato membro che ha rilasciato la carta.

cardNumber è il numero della carta.

2.74. **FullCardNumberAndGeneration**

Seconda generazione:

Codice per l'identificazione completa di una carta tachigrafica e della sua generazione.

```
FullCardNumberAndGeneration ::= SEQUENCE {
   fullCardNumber                        FullCardNumber,
   generation                            Generation
}
```

fullcardNumber identifica la carta tachigrafica.

generation indica la generazione della carta tachigrafica utilizzata.

▼B

2.75. **Generation**

Seconda generazione:

Indica la generazione del tachigrafo utilizzato.

```
Generation ::= INTEGER(0..255)
```

Assegnazione valore:

'00'H	RFU
'01'H	Prima generazione
'02'H	Seconda generazione
'03'H .. 'FF'H	RFU

2.76. **GeoCoordinates**

Seconda generazione:

Le coordinate geografiche sono codificate come numeri interi. Tali numeri interi sono multipli della codifica ± DDMM.M per la latitudine e ± DDDMM.M per la longitudine. Qui ± DD e ± DDD rispettivamente indicano i gradi e MM.M indica i minuti.

```
GeoCoordinates ::= SEQUENCE {
   latitude                                INTEGER(-90000..90001),
   longitude                               INTEGER(-180000..180001)
}
```

latitude è codificato come multiplo (fattore 10) della rappresentazione di ±DDMM.M.

longitude è codificato come multiplo (fattore 10) della rappresentazione di ±DDDMM.M.

2.77. **GNSSAccuracy**

Seconda generazione:

L'accuratezza dei dati del GNSS sulla posizione [definizione eee)]. Tale accuratezza è codificata come numero intero ed è un multiplo (fattore 10) del valore X.Y fornito dalla frase GSA NMEA.

```
GNSSAccuracy ::= INTEGER(1..100)
```

2.78. **GNSSContinuousDriving**

Seconda generazione:

Informazioni, memorizzate in una carta del conducente o dell'officina, relative alla posizione del veicolo rilevata dal GNSS, se il periodo di guida continuo del conducente raggiunge un multiplo di tre ore (requisiti 306 e 354 dell'allegato 1C).

```
GNSSContinuousDriving := SEQUENCE {
   gnssCDPointerNewestRecord               INTEGER(0..NoOfGNSSCDRecords -1),
   gnssContinuousDrivingRecords            SET SIZE(NoOfGNSSCDRecords) OF
                                           GNSSContinuousDrivingRecord
}
```

gnssCDPointerNewestRecord è l'indice della registrazione più aggiornata di guida continua effettuata dal GNSS.

▼B

Assegnazione valore: numero corrispondente al numeratore della registrazione di guida continua effettuata dal GNSS, a partire da '0' per la prima volta in cui tale registrazione compare nella struttura.

gnssContinuousDrivingRecords è la serie di registrazioni contenenti la data e l'ora in cui la guida continua raggiunge un multiplo di tre ore e informazioni sulla posizione del veicolo.

2.79. **GNSSContinuousDrivingRecord**

Seconda generazione:

Informazioni, memorizzate in una carta del conducente o dell'officina, relative alla posizione del veicolo rilevata dal GNSS, se il periodo di guida continuo del conducente raggiunge un multiplo di tre ore (requisiti 305 e 353 dell'allegato 1C).

```
GNSSContinuousDrivingRecord ::= SEQUENCE {
   timeStamp                              TimeReal,
   gnssPlaceRecord                        GNSSPlaceRecord
}
```

timeStamp indica la data e l'ora in cui il periodo di guida continuo del titolare della carta raggiunge un multiplo di tre ore.

gnssPlaceRecord contiene informazioni relative alla posizione del veicolo.

2.80. **GNSSPlaceRecord**

Seconda generazione:

Informazioni relative alla posizione del veicolo rilevata dal GNSS (requisiti 108, 109, 110, 296, 305, 347 e 353 dell'allegato 1C).

```
GNSSPlaceRecord ::= SEQUENCE {
   timeStamp                              TimeReal,
   gnssAccuracy                           GNSSAccuracy,
   geoCoordinates                         GeoCoordinates
}
```

timeStamp indica la data e l'ora di determinazione della posizione del veicolo da parte del GNSS.

gnssAccuracy è l'accuratezza dei dati sulla posizione del GNSS.

geoCoordinates è la posizione registrata tramite GNSS.

2.81. **HighResOdometer**

Valore dell'odometro del veicolo: distanza cumulata percorsa dal veicolo durante il funzionamento.

```
HighResOdometer ::= INTEGER(0..2^32-1)
```

▼B

Assegnazione valore: binario senza segno. Valore espresso in 1/200 km nell'intervallo operativo 0-21 055 406 km.

2.82. **HighResTripDistance**

Una distanza percorsa durante un intero viaggio o parte di esso.

```
HighResTripDistance ::= INTEGER(0..2^32-1)
```

Assegnazione valore: binario senza segno. Valore espresso in 1/200 km nell'intervallo operativo 0-21 055 406 km.

2.83. **HolderName**

Cognome e nome/i del titolare di una carta.

```
HolderName ::= SEQUENCE {
   holderSurname                    Name,
   holderFirstNames                 Name
}
```

holderSurname è il cognome del titolare. Il cognome non comprende titoli.

Assegnazione valore: nel caso di una carta non personale, holderSurname contiene le stesse informazioni di companyName o workshopName o controlBodyName.

holderFirstNames contiene il nome (o i nomi) e le iniziali del titolare.

2.84. **InternalGNSSReceiver**

Seconda generazione:

Indicazione se il ricevitore GNSS è interno o esterno all'unità elettronica di bordo. «Vero» significa che il ricevitore GNSS è interno alla VU. «Falso» significa che il ricevitore GNSS è esterno.

```
InternalGNSSReceiver ::= BOOLEAN
```

2.85. **K-ConstantOfRecordingEquipment**

Costante dell'apparecchio di controllo [definizione m)].

```
K-ConstantOfRecordingEquipment ::= INTEGER(0..2^16-1)
```

Assegnazione valore: impulsi per chilometro nell'intervallo operativo 0-64 255 impulsi/km.

2.86. **KeyIdentifier**

Identificativo univoco di una chiave pubblica utilizzato per codificare e selezionare la chiave. Identifica anche il titolare della chiave.

```
KeyIdentifier ::= CHOICE {
   extendedSerialNumber             ExtendedSerialNumber,
   certificateRequestID             CertificateRequestID,
   certificationAuthorityKID        CertificationAuthorityKID
}
```

▼B

La prima scelta (CHOICE) è adatta a codificare la chiave pubblica di un'unità elettronica di bordo o di una carta tachigrafica.

La seconda scelta è adatta a codificare la chiave pubblica di un'unità elettronica di bordo (nel caso in cui il numero di serie dell'unità elettronica di bordo non sia noto al momento della generazione del certificato).

La terza scelta è adatta a codificare la chiave pubblica di uno Stato membro.

2.87. **KMWCKey**

Seconda generazione:

Chiave AES e versione della chiave ivi associata usata per l'abbinamento del sensore di movimento alla VU. Per i dettagli cfr. l'appendice 11.

```
KMWCKey ::= SEQUENCE {
   kMWCKey                                 AESKey,
   keyVersion                              INTEGER (SIZE(1))
}
```

kMWCKey è la lunghezza della chiave AES concatenata con la chiave usata per l'abbinamento del sensore di movimento alla VU.

keyVersion rappresenta la versione della chiave AES.

2.88. **Language**

Codice che identifica una lingua.

```
Language ::= IA5String(SIZE(2))
```

Assegnazione valore: codifica a due lettere minuscole, secondo ISO 639.

2.89. **LastCardDownload**

Data e ora, registrati sulla carta del conducente, dell'ultimo trasferimento di dati dalla carta (a fini diversi da quelli di controllo), requisiti 257 e 282 dell'allegato 1C. La data può essere aggiornata dalla VU o da qualsiasi lettore di carte.

```
LastCardDownload ::= TimeReal
```

Assegnazione valore: nessun'altra specificazione.

2.90. **LinkCertificate**

Seconda generazione:

Il certificato di collegamento tra coppie di chiavi dell'autorità europea di certificazione primaria.

```
LinkCertificate ::= Certificate
```

2.91. **L-TyreCircumference**

Circonferenza effettiva degli pneumatici delle ruote [definizione u)].

```
L-TyreCircumference ::= INTEGER(0.. 2^16-1)
```

▼B

Assegnazione valore: binario senza segno, valore espresso in 1/8 mm nell'intervallo operativo 0-8 031 mm.

2.92. **MAC**

Seconda generazione:

Un totale di controllo crittografico di 8, 12 o 16 byte di lunghezza corrispondente alle cipher suites (sequenze crittografiche) di cui all'appendice 11.

```
MAC ::= CHOICE {
   mac8                                    OCTET STRING (SIZE(8)),
   mac12                                   OCTET STRING (SIZE(12)),
   mac16                                   OCTET STRING (SIZE(12))
}
```

2.93. **ManualInputFlag**

Codice che indica se, all'atto dell'inserimento della carta, il titolare di una carta abbia o meno inserito manualmente le attività del conducente (requisito 081 dell'allegato 1B e requisito 102 dell'allegato 1C).

```
ManualInputFlag ::= INTEGER {
   noEntry                                 (0)
   manualEntries                           (1)
}
```

Assegnazione valore: nessun'altra specificazione.

2.94. **ManufacturerCode**

Codice che identifica il fabbricante di un apparecchio omologato.

```
ManufacturerCode ::= INTEGER(0..255)
```

Il laboratorio competente per le prove di interoperabilità aggiorna e pubblica sul proprio sito Internet l'elenco dei codici dei fabbricanti (requisito 454 dell'allegato 1C).

I ManufacturerCodes sono assegnati in via provvisoria ai progettisti di tachigrafi su richiesta del laboratorio responsabile delle prove di interoperabilità.

2.95. **ManufacturerSpecificEventFaultData**

Seconda generazione:

I codici di errore specifici del fabbricante semplificano l'analisi degli errori e la manutenzione delle unità elettroniche di bordo.

```
ManufacturerSpecificEventFaultData ::= SEQUENCE {
   manufacturerCode                        ManufacturerCode,
   manufacturerSpecificErrorCode           OCTET STRING(SIZE(3))
}
```

manufacturerCode identifica il fabbricante dell'unità elettronica di bordo.

manufacturerSpecificErrorCode è un codice di errore specifico del fabbricante.

▼B

2.96. **MemberStateCertificate**

Il certificato della chiave pubblica di uno Stato membro rilasciato dall'autorità europea di certificazione.

```
MemberStateCertificate ::= Certificate
```

2.97. **MemberStateCertificateRecordArray**

Seconda generazione:

Il certificato dello Stato membro più i metadati usati nel protocollo di trasferimento.

```
MemberStateCertificateRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF
                                       MemberStateCertificate
}
```

recordType rappresenta il tipo di registrazione (MemberStateCertificate). **Assegnazione valore**: Cfr. RecordType

recordSize sono le dimensioni di MemberStateCertificate in byte.

noOfRecords è il numero di registrazioni nella serie di registrazioni. Il valore deve essere fissato a 1 perché i certificati possono avere lunghezze diverse.

records è la serie di certificati dello Stato membro.

2.98. **MemberStatePublicKey**

Prima generazione:

La chiave pubblica di uno Stato membro.

```
MemberStatePublicKey ::= PublicKey
```

2.99. **Name**

Un nome.

```
Name ::= SEQUENCE {
   codePage                            INTEGER (0..255),
   name                                OCTET STRING (SIZE(35))
}
```

codePage specifica una serie di caratteri quali definiti nel capitolo 4,

name è un nome codificato usando la serie specifica di caratteri.

2.100. **NationAlpha**

Codice alfabetico del paese conforme ai segni distintivi usati sui veicoli nel traffico internazionale (Convenzione delle Nazioni Unite sulla circolazione stradale — Vienna 1968).

```
NationAlpha ::= IA5String(SIZE(3))
```

I codici NationAlpha e i codici numerici devono figurare in un elenco pubblicato nel sito Internet del laboratorio incaricato di effettuare le prove di interoperabilità, come previsto dal requisito 440 dell'allegato 1C.

▼B

2.101. **NationNumeric**

Codice numerico di un paese.

```
NationNumeric ::= INTEGER(0 .. 255)
```

Assegnazione valore: cfr. tipo di dati 2.100 (NationAlpha).

Qualsiasi modifica delle specifiche NationAlpha o numeriche descritte nel precedente paragrafo può essere apportata soltanto dopo che il laboratorio incaricato abbia ottenuto il parere dei fabbricanti dell'unità elettronica di bordo del tachigrafo intelligente e digitale omologato.

2.102. **NoOfCalibrationRecords**

Numero di registrazioni di tarature che una carta dell'officina è in grado di memorizzare.

Prima generazione:

```
NoOfCalibrationRecords ::= INTEGER(0..255)
```

Assegnazione valore: cfr. appendice 2.

Seconda generazione:

```
NoOfCalibrationRecords ::= INTEGER(0..2^16-1)
```

Assegnazione valore: cfr. appendice 2.

2.103. **NoOfCalibrationsSinceDownload**

Contatore che indica il numero di tarature effettuate con una carta dell'officina dall'ultimo trasferimento dei suoi dati (requisiti 317 e 340 dell'allegato 1C).

```
NoOfCalibrationsSinceDownload ::= INTEGER(0..2^16-1)
```

Assegnazione valore: nessun'altra specificazione.

2.104. **NoOfCardPlaceRecords**

Numero di registrazioni di luoghi che una carta del conducente o dell'officina è in grado di memorizzare.

Prima generazione:

```
NoOfCardPlaceRecords ::= INTEGER(0..255)
```

Assegnazione valore: cfr. appendice 2.

Seconda generazione:

```
NoOfCardPlaceRecords ::= INTEGER(0..2^16-1)
```

Assegnazione valore: cfr. appendice 2.

▼B

2.105. **NoOfCardVehicleRecords**

Numero di registrazioni relative ai veicoli utilizzati che una carta del conducente o dell'officina è in grado di memorizzare.

```
NoOfCardVehicleRecords ::= INTEGER(0.. 2^16-1)
```

Assegnazione valore: cfr. appendice 2.

2.106. **NoOfCardVehicleUnitRecords**

Seconda generazione:

Numero di registrazioni relative alle unità elettroniche di bordo utilizzate che una carta del conducente o dell'officina è in grado di memorizzare.

```
NoOfCardVehicleUnitRecords ::= INTEGER(0.. 2^16-1)
```

Assegnazione valore: cfr. appendice 2.

2.107. **NoOfCompanyActivityRecords**

Numero di registrazioni delle attività dell'impresa che una carta dell'azienda è in grado di memorizzare.

```
NoOfCompanyActivityRecords ::= INTEGER(0.. 2^16-1)
```

Assegnazione valore: cfr. appendice 2.

2.108. **NoOfControlActivityRecords**

Numero di registrazioni delle attività di controllo che una carta di controllo è in grado di memorizzare.

```
NoOfControlActivityRecords ::= INTEGER(0.. 2^16-1)
```

Assegnazione valore: cfr. appendice 2.

2.109. **NoOfEventsPerType**

Numero di anomalie per tipo di anomalia che una carta è in grado di memorizzare.

```
NoOfEventsPerType ::= INTEGER(0..255)
```

Assegnazione valore: cfr. appendice 2.

2.110. **NoOfFaultsPerType**

Numero di guasti per tipo di guasto che una carta è in grado di memorizzare.

```
NoOfFaultsPerType ::= INTEGER(0..255)
```

Assegnazione valore: cfr. appendice 2.

▼B

2.111. **NoOfGNSSCDRecords**

Seconda generazione:

Numero di registrazioni di guida continua del GNSS che una carta è in grado di memorizzare.

```
NoOfGNSSCDRecords ::= INTEGER(0..2^16-1)
```

Assegnazione valore: cfr. appendice 2.

2.112. **NoOfSpecificConditionRecords**

Seconda generazione:

Numero di registrazioni di condizioni particolari che una carta è in grado di memorizzare.

```
NoOfSpecificConditionRecords ::= INTEGER(0..2^16-1)
```

Assegnazione valore: cfr. appendice 2.

2.113. **OdometerShort**

Valore dell'odometro del veicolo in forma abbreviata.

```
OdometerShort ::= INTEGER(0..2^24-1)
```

Assegnazione valore: binario senza segno. Valore espresso in km nell'intervallo operativo 0-9 999 999 km.

2.114. **OdometerValueMidnight**

Il valore dell'odometro del veicolo alla mezzanotte di un determinato giorno (requisito 090 dell'allegato 1B e requisito 113 dell'allegato 1C).

```
OdometerValueMidnight ::= OdometerShort
```

Assegnazione valore: nessun'altra specificazione.

2.115. **OdometerValueMidnightRecordArray**

Seconda generazione:

L'OdometerValueMidnight più i metadati usati nel protocollo di trasferimento.

```
OdometerValueMidnightRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF
                                       OdometerValueMidnight
}
```

recordType rappresenta il tipo di registrazione (OdometerValueMidnight). **Assegnazione valore**: Cfr. RecordType

recordSize sono le dimensioni di OdometerValueMidnight in byte.

noOfRecords è il numero di registrazioni nella serie di registrazioni.

records è la serie di registrazioni dell'OdometerValueMidnight.

▼B

2.116. **OverspeedNumber**

Numero di anomalie per superamento di velocità dopo l'ultimo controllo di superamento di velocità.

```
OverspeedNumber ::= INTEGER(0..255)
```

Assegnazione valore: 0 significa che non si è verificata alcuna anomalia per superamento di velocità dopo l'ultimo controllo di superamento di velocità, 1 significa che si è verificata un'anomalia per superamento velocità dopo l'ultimo controllo … 255 significa che si sono verificate 255 o più anomalie per superamento di velocità dopo l'ultimo controllo di superamento di velocità.

2.117. **PlaceRecord**

Informazioni relative al luogo in cui inizia o termina un periodo di lavoro giornaliero (requisiti 108, 271, 296, 324 e 347 dell'allegato 1C).

Prima generazione:

```
PlaceRecord ::= SEQUENCE {
   entryTime                           TimeReal,
   entryTypeDailyWorkPeriod            EntryTypeDailyWorkPeriod,
   dailyWorkPeriodCountry              NationNumeric,
   dailyWorkPeriodRegion               RegionNumeric,
   vehicleOdometerValue                OdometerShort
}
```

entryTime specifica la data e l'ora relative all'immissione.

entryTypeDailyWorkPeriod è il tipo di immissione.

dailyWorkPeriodCountry è il paese inserito.

dailyWorkPeriodRegion è la regione inserita.

vehicleOdometerValue è il valore dell'odometro all'atto dell'immissione del luogo.

Seconda generazione:

```
PlaceRecord ::= SEQUENCE {
   entryTime                           TimeReal,
   entryTypeDailyWorkPeriod            EntryTypeDailyWorkPeriod,
   dailyWorkPeriodCountry              NationNumeric,
   dailyWorkPeriodRegion               RegionNumeric,
   vehicleOdometerValue                OdometerShort,
   entryGNSSPlaceRecord                GNSSPlaceRecord
}
```

Oltre alla prima generazione, si usa il seguente componente:

entryGNSSPlaceRecord indica il luogo e l'ora registrati.

▼B

2.118. **PreviousVehicleInfo**

Informazioni relative al veicolo precedentemente usato da un conducente all'atto dell'inserimento della carta in un'unità elettronica di bordo (requisito 081 dell'allegato 1B e requisito 102 dell'allegato 1C).

Prima generazione:

```
PreviousVehicleInfo ::= SEQUENCE {
   vehicleRegistrationIdentification      VehicleRegistrationIdentification,
   cardWithdrawalTime                     TimeReal
}
```

vehicleRegistrationIdentification contiene il VRN e lo Stato membro di immatricolazione del veicolo.

cardWithdrawalTime specifica la data e l'ora di estrazione della carta.

Seconda generazione:

```
PreviousVehicleInfo ::= SEQUENCE {
   vehicleRegistrationIdentification      VehicleRegistrationIdentification,
   cardWithdrawalTime                     TimeReal,
   vuGeneration                           Generation
}
```

Oltre alla prima generazione, è utilizzato il seguente elemento di dati:

vuGeneration identifica la generazione dell'unità elettronica di bordo.

2.119. **PublicKey**

Prima generazione:

Una chiave pubblica RSA.

```
PublicKey ::= SEQUENCE {
   rsaKeyModulus                          RSAKeyModulus,
   rsaKeyPublicExponent                   RSAKeyPublicExponent
}
```

rsaKeyModulus è il modulo della coppia di chiavi.

rsaKeyPublicExponent è l'esponente pubblico della coppia di chiavi.

2.120. **RecordType**

Seconda generazione:

Riferimento ad un tipo di registrazione. Questo tipo di dati è usato in RecordArrays.

```
RecordType ::= OCTET STRING(SIZE(1))
```

▼B

Assegnazione valore:

'01'H	ActivityChangeInfo,
'02'H	CardSlotsStatus,
'03'H	CurrentDateTime,
'04'H	MemberStateCertificate,
'05'H	OdometerValueMidnight,
'06'H	DateOfDayDownloaded,
'07'H	SensorPaired,
'08'H	Signature,
'09'H	SpecificConditionRecord,
'0A'H	VehicleIdentificationNumber,
'0B'H	VehicleRegistrationNumber,
'0C'H	VuCalibrationRecord,
'0D'H	VuCardIWRecord,
'0E'H	VuCardRecord,
'0F'H	VuCertificate,
'10'H	VuCompanyLocksRecord,
'11'H	VuControlActivityRecord,
'12'H	VuDetailedSpeedBlock,
'13'H	VuDownloadablePeriod,
'14'H	VuDownloadActivityData,
'15'H	VuEventRecord,
'16'H	VuGNSSCDRecord,
'17'H	VuITSConsentRecord,
'18'H	VuFaultRecord,
'19'H	VuIdentification,
'1A'H	VuOverSpeedingControlData,
'1B'H	VuOverSpeedingEventRecord,
'1C'H	VuPlaceDailyWorkPeriodRecord,
'1D'H	VuTimeAdjustmentGNSSRecord,
'1E'H	VuTimeAdjustmentRecord,
'1F'H	VuPowerSupplyInterruptionRecord,
'20'H	SensorPairedRecord,
'21'H	SensorExternalGNSSCoupledRecord,
'22'H to '7F'H	RFU,
'80'H to 'FF'H	Specifico del fabbricante.

2.121. **RegionAlpha**

Codice numerico delle diverse regioni di un determinato paese.

```
RegionAlpha ::= IA5STRING(SIZE(3))
```

Prima generazione:

Assegnazione valore:

' '	No information available,
Spain:	
'AN '	Andalucía,
'AR '	Aragón,
'AST'	Asturias,
'C '	Cantabria,
'CAT'	Cataluña,
'CL '	Castilla-León,
'CM '	Castilla-La-Mancha,
'CV'	Valencia,
'EXT'	Extremadura,
'G '	Galicia,
'IB '	Baleares,
'IC '	Canarias,
'LR '	La Rioja,
'M '	Madrid,
'MU '	Murcia,
'NA '	Navarra,
'PV '	País Vasco

▼B

Seconda generazione:

I codici RegionAlpha devono figurare in un elenco pubblicato nel sito Internet del laboratorio incaricato di effettuare le prove di interoperabilità.

2.122. **RegionNumeric**

Codice numerico delle diverse regioni di un determinato paese.

```
RegionNumeric ::= OCTET STRING (SIZE(1))
```

Prima generazione:

Assegnazione valore:

```
'00'H        No information available,
Spain:
'01'H        Andalucía,
'02'H        Aragón,
'03'H        Asturias,
'04'H        Cantabria,
'05'H        Cataluña,
'06'H        Castilla-León,
'07'H        Castilla-La-Mancha,
'08'H        Valencia,
'09'H        Extremadura,
'0A'H        Galicia,
'0B'H        Baleares,
'0C'H        Canarias,
'0D'H        La Rioja,
'0E'H        Madrid,
'0F'H        Murcia,
'10'H        Navarra,
'11'H        País Vasco
```

Seconda generazione:

I codici RegionNumeric devono figurare in un elenco pubblicato nel sito Internet del laboratorio incaricato di effettuare le prove di interoperabilità.

2.123. **RemoteCommunicationModuleSerialNumber**

Seconda generazione:

Numero di serie del modulo di comunicazione remota.

```
RemoteCommunicationModuleSerialNumber ::= ExtendedSerialNumber
```

2.124. **RSAKeyModulus**

Prima generazione:

Il modulo di una coppia di chiavi RSA.

```
RSAKeyModulus ::= OCTET STRING (SIZE(128))
```

Assegnazione valore: non specificato.

2.125. **RSAKeyPrivateExponent**

Prima generazione:

L'esponente privato di una coppia di chiavi RSA.

```
RSAKeyPrivateExponent ::= OCTET STRING (SIZE(128))
```

Assegnazione valore: non specificato.

▼B

2.126. **RSAKeyPublicExponent**

Prima generazione:

L'esponente pubblico di una coppia di chiavi RSA.

```
RSAKeyPublicExponent ::= OCTET STRING (SIZE(8))
```

Assegnazione valore: non specificato.

2.127. **RtmData**

Seconda generazione:

Per la definizione di questo tipo di dati, cfr. l'appendice 14.

2.128. **SealDataCard**

Seconda generazione:

Questo tipo di dati memorizza informazioni sui sigilli apposti ai diversi componenti di un veicolo ed è destinato alla memorizzazione su una carta. Questo tipo di dati si riferisce al requisito 337 dell'allegato 1C.

```
SealDataCard ::= SEQUENCE {
   noOfSealRecords                    INTEGER(1..5),
   sealRecords                        SET SIZE(noOfSealRecords) OF SealRecord
}
```

noOfSealRecords è il numero di registrazioni contenute in sealRecords.

sealRecords è una serie di registrazioni di sigilli.

2.129. **SealDataVu**

Seconda generazione:

Questo tipo di dati memorizza informazioni sui sigilli apposti ai diversi componenti di un veicolo ed è destinato alla memorizzazione in una VU.

```
SealDataVu ::= SEQUENCE SIZE(5) OF {
   sealRecords                        SealRecord
}
```

sealRecords è una serie di registrazioni di sigilli. Se sono presenti meno di 5 sigilli, il valore di EquipmentType in tutti i sealRecords inutilizzati deve essere impostato su 16, ossia «inutilizzato».

2.130. **SealRecord**

Seconda generazione:

Questo tipo di dati memorizza informazioni su un sigillo apposto ad un componente. Questo tipo di dati si riferisce al requisito 337 dell'allegato 1C.

```
SealRecord ::= SEQUENCE {
   equipmentType                      EquipmentType,
   extendedSealIdentifier             ExtendedSealIdentifier
}
```

equipmentType identifica il tipo di apparecchio su cui è apposto il sigillo.

extendedSealIdentifier è l'identificativo del sigillo apposto sull'apparecchio.

▼B

2.131. **SensorApprovalNumber**

Numero di omologazione del sensore.

Prima generazione:

```
SensorApprovalNumber ::= IA5String(SIZE(8))
```

Assegnazione valore: non specificato.

Seconda generazione:

```
SensorApprovalNumber ::= IA5String(SIZE(16))
```

Assegnazione valore:

Il numero di omologazione deve corrispondere a quanto pubblicato sul sito Internet della Commissione europea, vale a dire ad esempio compresi gli eventuali trattini. Il numero di omologazione deve essere allineato a sinistra.

2.132. **SensorExternalGNSSApprovalNumber**

Seconda generazione:

Numero di omologazione del dispositivo GNSS esterno.

```
SensorExternalGNSSApprovalNumber ::= IA5String(SIZE(16))
```

Assegnazione valore:

Il numero di omologazione deve corrispondere a quanto pubblicato sul sito Internet della Commissione europea, vale a dire ad esempio compresi gli eventuali trattini. Il numero di omologazione deve essere allineato a sinistra.

2.133. **SensorExternalGNSSCoupledRecord**

Seconda generazione:

Informazioni, memorizzate in un'unità elettronica di bordo, relative all'identificazione del dispositivo GNSS esterno accoppiato all'unità elettronica di bordo (requisito 100 dell'allegato 1C).

```
SensorExternalGNSSCoupledRecord ::= SEQUENCE {
   sensorSerialNumber                  SensorGNSSSerialNumber,
   sensorApprovalNumber                SensorExternalGNSSApprovalNumber,
   sensorCouplingDate                  SensorGNSSCouplingDate
}
```

sensorSerialNumber è il numero di serie del dispositivo GNSS esterno accoppiato all'unità elettronica di bordo.

sensorApprovalNumber è il numero di omologazione di questo dispositivo GNSS esterno.

sensorCouplingDate è una data di accoppiamento di questo dispositivo GNSS esterno con l'unità elettronica di bordo.

2.134. **SensorExternalGNSSIdentification**

Seconda generazione:

Informazioni relative all'identificazione del dispositivo GNSS esterno (requisito 98 dell'allegato 1C).

▼B

```
SensorExternalGNSSIdentification ::= SEQUENCE {
   sensorSerialNumber                    SensorGNSSSerialNumber,
   sensorApprovalNumber                  SensorExternalGNSSApprovalNumber,
   sensorSCIdentifier                    SensorExternalGNSSSCIdentifier,
   sensorOSIdentifier                    SensorExternalGNSSOSIdentifier
}
```

sensorSerialNumber è il numero di serie completo del dispositivo GNSS esterno.

sensorApprovalNumber è il numero di omologazione del dispositivo GNSS esterno.

sensorSCIdentifier è l'identificativo del componente di sicurezza del dispositivo GNSS esterno.

sensorOSIdentifier è l'identificativo del sistema operativo del dispositivo GNSS esterno.

2.135. **SensorExternalGNSSInstallation**

Seconda generazione:

Informazioni, memorizzate in un dispositivo GNSS esterno, relative all'installazione del sensore del dispositivo GNSS esterno (requisito 123 dell'allegato 1C).

```
SensorExternalGNSSInstallation ::= SEQUENCE {
   sensorCouplingDateFirst               SensorGNSSCouplingDate,
   firstVuApprovalNumber                 VuApprovalNumber,
   firstVuSerialNumber                   VuSerialNumber,
   sensorCouplingDateCurrent             SensorGNSSCouplingDate,
   currentVuApprovalNumber               VuApprovalNumber,
   currentVUSerialNumber                 VuSerialNumber
}
```

sensorCouplingDateFirst è la data del primo accoppiamento del dispositivo GNSS esterno con un'unità elettronica di bordo.

firstVuApprovalNumber è il numero di omologazione della prima unità elettronica di bordo accoppiata al dispositivo GNSS esterno.

firstVuSerialNumber è il numero di serie della prima unità elettronica di bordo abbinata al dispositivo GNSS esterno.

sensorCouplingDateCurrent è la data dell'accoppiamento corrente del dispositivo GNSS esterno con un'unità elettronica di bordo.

currentVuApprovalNumber è il numero di omologazione dell'unità elettronica di bordo attualmente accoppiata al dispositivo GNSS esterno.

currentVuSerialNumber è il numero di serie dell'unità elettronica di bordo attualmente accoppiata al dispositivo GNSS esterno.

▼B

2.136. **SensorExternalGNSSOSIdentifier**

Seconda generazione:

L'identificativo del sistema operativo del dispositivo GNSS esterno.

```
SensorOSIdentifier ::= IA5String(SIZE(2))
```

Assegnazione valore: a cura del fabbricante.

2.137. **SensorExternalGNSSSCIdentifier**

Seconda generazione:

Questo tipo è utilizzato, ad esempio, per individuare il modulo crittografico del dispositivo GNSS esterno.

Identificativo del componente di sicurezza del dispositivo GNSS esterno.

```
SensorExternalGNSSSCIdentifier ::= IA5String(SIZE(8))
```

Assegnazione valore: a cura del fabbricante del componente.

2.138. **SensorGNSSCouplingDate**

Seconda generazione:

Data di accoppiamento del dispositivo GNSS esterno con un'unità elettronica di bordo.

```
SensorGNSSCouplingDate ::= TimeReal
```

Assegnazione valore: non specificato.

2.139. **SensorGNSSSerialNumber**

Seconda generazione:

Questo tipo è utilizzato per memorizzare il numero di serie del ricevitore GNSS sia quando è all'interno della VU che quando è esterno alla VU.

Numero di serie del ricevitore GNSS.

```
SensorGNSSSerialNumber ::= ExtendedSerialNumber
```

2.140. **SensorIdentification**

Informazioni, memorizzate in un sensore di movimento, relative all'identificazione del sensore stesso (requisito 077 dell'allegato 1B e requisito 95 dell'allegato 1C).

```
SensorIdentification ::= SEQUENCE {
   sensorSerialNumber                  SensorSerialNumber,
   sensorApprovalNumber                SensorApprovalNumber,
   sensorSCIdentifier                  SensorSCIdentifier,
   sensorOSIdentifier                  SensorOSIdentifier
}
```

sensorSerialNumber è il numero di serie completo del sensore di movimento (comprende il codice componente e il codice del fabbricante).

sensorApprovalNumber è il numero di omologazione del sensore di movimento.

sensorSCIdentifier è l'identificativo del componente di sicurezza del sensore di movimento.

▼B

sensorOSIdentifier è l'identificativo del sistema operativo del sensore di movimento.

2.141. **SensorInstallation**

Informazioni, memorizzate in un sensore di movimento, relative all'installazione del sensore stesso (requisito 099 dell'allegato 1B e requisito 122 dell'allegato 1C).

```
SensorInstallation ::= SEQUENCE {
   sensorPairingDateFirst                SensorPairingDate,
   firstVuApprovalNumber                 VuApprovalNumber,
   firstVuSerialNumber                   VuSerialNumber,
   sensorPairingDateCurrent              SensorPairingDate,
   currentVuApprovalNumber               VuApprovalNumber,
   currentVUSerialNumber                 VuSerialNumber
}
```

sensorPairingDateFirst è la data del primo abbinamento del sensore di movimento con un'unità elettronica di bordo.

firstVuApprovalNumber è il numero di omologazione della prima unità elettronica di bordo abbinata al sensore di movimento.

firstVuSerialNumber è il numero di serie della prima unità elettronica di bordo abbinata al sensore di movimento.

sensorPairingDateCurrent è la data dell'attuale abbinamento del sensore di movimento con l'unità elettronica di bordo.

currentVuApprovalNumber è il numero di omologazione dell'unità elettronica di bordo attualmente abbinata al sensore di movimento.

currentVUSerialNumber è il numero di serie dell'unità elettronica di bordo attualmente abbinata al sensore di movimento.

2.142. **SensorInstallationSecData**

Informazioni, memorizzate in una carta dell'officina, relative ai dati di sicurezza necessari per l'abbinamento dei sensori di movimento con le unità elettroniche di bordo (requisiti 308 e 331 dell'allegato 1C).

Prima generazione:

```
SensorInstallationSecData ::= TdesSessionKey
```

Assegnazione valore: secondo ISO 16844-3.

Seconda generazione:

Come descritto nell'appendice 11, una carta dell'officina memorizza fino a tre chiavi per l'abbinamento del sensore di movimento alla VU. Tali chiavi hanno versioni diverse della chiave.

```
SensorInstallationSecData ::= SEQUENCE {
   kMWCKey1                              KMWCKey,
   kMWCKey2                              KMWCKey OPTIONAL,
   kMWCKey3                              KMWCKey OPTIONAL
}
```

▼B

2.143. **SensorOSIdentifier**

Identificativo del sistema operativo del sensore di movimento.

```
SensorOSIdentifier ::= IA5String(SIZE(2))
```

Assegnazione valore: a cura del fabbricante.

2.144. **SensorPaired**

Prima generazione:

Informazioni, memorizzate in un'unità elettronica di bordo, relative all'identificazione del sensore di movimento abbinato all'unità elettronica di bordo (requisito 079 dell'allegato 1B).

```
SensorPaired ::= SEQUENCE {
   sensorSerialNumber                    SensorSerialNumber,
   sensorApprovalNumber                  SensorApprovalNumber,
   sensorPairingDateFirst                SensorPairingDate
}
```

sensorSerialNumber è il numero di serie del sensore di movimento attualmente abbinato all'unità elettronica di bordo.

sensorApprovalNumber è il numero di omologazione del sensore di movimento attualmente abbinato all'unità elettronica di bordo.

sensorPairingDateFirst è la data del primo abbinamento con un'unità elettronica di bordo del sensore di movimento attualmente abbinato all'unità elettronica di bordo.

2.145. **SensorPairedRecord**

Seconda generazione:

Informazioni, memorizzate in un'unità elettronica di bordo, relative all'identificazione di un sensore di movimento abbinato all'unità elettronica di bordo (requisito 97 dell'allegato 1C).

```
SensorPairedRecord ::= SEQUENCE {
   sensorSerialNumber                    SensorSerialNumber,
   sensorApprovalNumber                  SensorApprovalNumber,
   sensorPairingDate                     SensorPairingDate
}
```

sensorSerialNumber è il numero di serie di un sensore di movimento abbinato all'unità elettronica di bordo.

sensorApprovalNumber è il numero di omologazione di questo sensore di movimento.

sensorPairingDate è una data di abbinamento di questo sensore di movimento con l'unità elettronica di bordo.

2.146. **SensorPairingDate**

Data di abbinamento del sensore di movimento con un'unità elettronica di bordo.

```
SensorPairingDate ::= TimeReal
```

Assegnazione valore: non specificato.

▼B

2.147. **SensorSCIdentifier**

Identificativo del componente di sicurezza del sensore di movimento.

```
SensorSCIdentifier ::= IA5String(SIZE(8))
```

Assegnazione valore: a cura del fabbricante del componente.

2.148. **SensorSerialNumber**

Numero di serie del sensore di movimento.

```
SensorSerialNumber ::= ExtendedSerialNumber
```

2.149. **Signature**

Una firma digitale.

Prima generazione:

```
Signature ::= OCTET STRING (SIZE(128))
```

Assegnazione valore: secondo l'appendice 11 (Meccanismi comuni di sicurezza).

Seconda generazione:

```
Signature ::= OCTET STRING (SIZE(64..132))
```

Assegnazione valore: secondo l'appendice 11 (Meccanismi comuni di sicurezza).

2.150. **SignatureRecordArray**

Seconda generazione:

una serie di firme più i metadati usati nel protocollo di trasferimento.

```
SignatureRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF Signature
}
```

recordType rappresenta il tipo di registrazione (Signature). **Assegnazione valore**: Cfr. RecordType

recordSize sono le dimensioni di Signature in byte.

noOfRecords è il numero di registrazioni nella serie di registrazioni. Il valore deve essere fissato a 1 perché le firme possono avere lunghezze diverse.

records è la serie di firme.

2.151. **SimilarEventsNumber**

Il numero di anomalie simili in un determinato giorno (requisito 094 dell'allegato 1B e requisito 117 dell'allegato 1C).

```
SimilarEventsNumber ::= INTEGER(0..255)
```

Assegnazione valore: 0 non è utilizzato, 1 significa che, nel giorno in questione, si è verificata ed è stata memorizzata una sola anomalia di un dato tipo, 2 significa che si sono verificate 2 anomalie dello stesso tipo (solo una è stata memorizzata), … 255 significa che si sono verificate 255 o più anomalie dello stesso tipo.

▼B

2.152. **SpecificConditionRecord**

Informazioni, memorizzate in una carta del conducente, una carta dell'officina o un'unità elettronica di bordo, relative ad una condizione particolare (requisiti 130, 276, 301, 328 e 355 dell'allegato 1C).

```
SpecificConditionRecord ::= SEQUENCE {
   entryTime                              TimeReal,
   specificConditionType                  SpecificConditionType
}
```

entryTime specifica la data e l'ora di immissione.

specificConditionType è il codice che identifica la condizione particolare.

2.153. **SpecificConditions**

Informazioni, memorizzate in una carta del conducente, una carta dell'officina o un'unità elettronica di bordo, relative ad una condizione particolare (requisiti 131, 277, 302, 329, e 356 dell'allegato 1C).

Seconda generazione:

```
SpecificConditions := SEQUENCE {
   conditionPointerNewestRecord          INTEGER(0..NoOfSpecificConditionRecords-1),
   specificConditionRecords              SET SIZE(NoOfSpecificConditionRecords) OF
                                         SpecificConditionRecord
}
```

conditionPointerNewestRecord è l'indice della registrazione più aggiornata della condizione particolare.

Assegnazione valore: numero corrispondente al numeratore della registrazione della condizione particolare, a partire da ′0′ per la prima volta in cui tale registrazione compare nella struttura.

specificConditionRecords è la serie di registrazioni contenenti le informazioni relative alle condizioni particolari registrate.

2.154. **SpecificConditionType**

Codice che identifica una condizione particolare (requisiti 050b, 105a, 212a e 230a dell'allegato 1B e requisito 62 dell'Allegato 1C).

```
SpecificConditionType ::= INTEGER(0..255)
```

Prima generazione:

Assegnazione valore:

‘00’H	RFU
‘01’H	Escluso dal campo di applicazione — Inizio
‘02’H	Escluso dal campo di applicazione — Fine
‘03’H	Attraversamento mediante traghetto/treno
‘04’H .. ‘FFH’	RFU

Seconda generazione:

Assegnazione valore:

‘00’H	RFU
‘01’H	Escluso dal campo di applicazione — Inizio
‘02’H	Escluso dal campo di applicazione — Fine
‘03’H	Attraversamento mediante traghetto/treno — Inizio
‘04’H	Attraversamento mediante traghetto/treno — Fine
‘05’H .. ‘FF’H	RFU

▼B

2.155. **Velocità**

Velocità del veicolo (km/h).

```
Speed ::= INTEGER(0..255)
```

Assegnazione valore: chilometri all'ora nell'intervallo operativo 0-220 km/h.

2.156. **SpeedAuthorised**

Velocità massima autorizzata del veicolo [definizione hh)].

```
SpeedAuthorised ::= Speed
```

2.157. **SpeedAverage**

Velocità media in un periodo precedentemente definito (km/h).

```
SpeedAverage ::= Speed
```

2.158. **SpeedMax**

Velocità massima misurata in un periodo precedentemente definito.

```
SpeedMax ::= Speed
```

2.159. **TachographPayload**

Seconda generazione:

Per la definizione di questo tipo di dati, cfr. l'appendice 14.

2.160. **TachographPayloadEncrypted**

Seconda generazione:

I dati utili trasmessi (payload) del tachigrafo criptati con la codifica DER-TLV, cioè i dati trasmessi criptati nel messaggio RTM. Per la cifratura, cfr. appendice 11, parte B, capitolo 13.

```
TachographPayloadEncrypted ::= SEQUENCE {
   tag                                  OCTET STRING(SIZE(1)),
   length                               OCTET STRING(SIZE(1..2)),
   paddingContentIndicatorByte          OCTET STRING(SIZE(1)),
   encryptedData                        OCTET STRING(SIZE(16..192))
}
```

tag fa parte della codifica DER-TLV e va fissato a '87' (cfr. appendice 11, parte B, capitolo 13).

length fa parte della codifica DER-TLV e codifica la lunghezza del paddingContentIndicatorByte e degli encryptedData a seguire.

paddingContentIndicatorByte va fissato a '00'.

encryptedData è tachographPayload criptato, come specificato nell'appendice 11, parte B, capitolo 13. La lunghezza di tali dati in ottetti deve sempre essere un multiplo di 16.

2.161. **TDesSessionKey**

Prima generazione:

Una chiave tripla di sessione DES.

```
TDesSessionKey ::= SEQUENCE {
   tDesKeyA                             OCTET STRING (SIZE(8)),
   tDesKeyB                             OCTET STRING (SIZE(8))
}
```

Assegnazione valore: nessun'altra specificazione.

▼B

2.162. **TimeReal**

Codice per un campo combinato di data e ora, in cui la data e l'ora sono espresse in termini di secondi trascorsi a partire dalle 00h00min00s. del 1º gennaio 1970 GMT.

```
TimeReal{INTEGER:TimeRealRange} ::= INTEGER(0..TimeRealRange)
```

Assegnazione valore — Allineato all'ottetto: numero di secondi a partire dalla mezzanotte del 1º gennaio 1970 GMT.

La data/ora massima possibile è nell'anno 2106.

2.163. **TyreSize**

Indicazione delle dimensioni degli pneumatici.

```
TyreSize ::= IA5String(SIZE(15))
```

Assegnazione valore: in conformità alla direttiva (CEE) 92/23 del 31.3.1992 (GU L 129, pag. 95).

2.164. **VehicleIdentificationNumber**

Numero di identificazione del veicolo (VIN) riferito al veicolo nel suo insieme, di norma corrispondente al numero di serie o al numero del telaio.

```
VehicleIdentificationNumber ::= IA5String(SIZE(17))
```

Assegnazione valore: secondo ISO 3779.

2.165. **VehicleIdentificationNumberRecordArray**

Seconda generazione:

Il numero di identificazione del veicolo più i metadati usati nel protocollo di trasferimento.

```
VehicleIdentificationNumberRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF
                                       VehicleIdentificationNumber
}
```

recordType rappresenta il tipo di registrazione (VehicleIdentification-Number). **Assegnazione valore**: Cfr. RecordType

recordSize sono le dimensioni di VehicleIdentificationNumber in byte.

noOfRecords è il numero di registrazioni nella serie di registrazioni.

records è la serie di numeri di identificazione del veicolo.

2.166. **VehicleRegistrationIdentification**

Identificazione di un veicolo, univoca per l'Europa (VRN e Stato membro).

```
VehicleRegistrationIdentification ::= SEQUENCE {
   vehicleRegistrationNation           NationNumeric,
   vehicleRegistrationNumber           VehicleRegistrationNumber
}
```

vehicleRegistrationNation è il paese in cui è stato immatricolato il veicolo.

▼B

vehicleRegistrationNumber è il numero di immatricolazione del veicolo (VRN).

2.167. **VehicleRegistrationNumber**

Numero di immatricolazione del veicolo (VRN). Il numero di immatricolazione è assegnato dall'autorità competente.

```
VehicleRegistrationNumber ::= SEQUENCE {
   codePage                          INTEGER (0..255),
   vehicleRegNumber                  OCTET STRING (SIZE(13))
}
```

codePage specifica una serie di caratteri quali definiti nel capitolo 4,

vehicleRegNumber è un VRN codificato usando la serie specifica di caratteri.

Assegnazione valore: a cura del paese.

2.168. **VehicleRegistrationNumberRecordArray**

Seconda generazione:

Il numero di immatricolazione del veicolo più i metadati usati nel protocollo di trasferimento.

```
VehicleRegistrationNumberRecordArray ::= SEQUENCE {
   recordType                        RecordType,
   recordSize                        INTEGER(1..65535),
   noOfRecords                       INTEGER(0..65535),
   records                           SET SIZE(noOfRecords) OF
                                     VehicleRegistrationNumber
}
```

recordType rappresenta il tipo di registrazione (VehicleRegistrationNumber). **Assegnazione valore**: Cfr. RecordType

recordSize sono le dimensioni di VehicleRegistrationNumber in byte.

noOfRecords è il numero di registrazioni nella serie di registrazioni.

records è la serie di numeri di immatricolazione del veicolo.

2.169. **VuAbility**

Seconda generazione:

Informazioni memorizzate in una VU sulla capacità della VU di utilizzare o meno carte tachigrafiche di prima generazione (requisito 121 dell'allegato 1C).

```
VuAbility ::= OCTET STRING (SIZE(1))
```

Assegnazione valore — Allineato all'ottetto: 'xxxxxxxa'B (8 bit)

Per la capacità di supportare la prima generazione:

'a'B	Capacità di supportare le carte tachigrafiche di prima generazione:
	'0' B la prima generazione è supportata,
	'1' B la prima generazione non è supportata,
'xxxxxxx'B	RFU

▼B

2.170. **VuActivityDailyData**

Prima generazione:

Informazioni, memorizzate in una VU, relative ai cambi di attività e/o alle variazioni della condizione di guida e/o alle variazioni della condizione della carta in un determinato giorno di calendario (requisito 084 dell'allegato 1B e requisiti 105, 106 e 107 dell'allegato 1C) e della condizione della sede (slot) alle 00h00 del giorno stesso.

```
VuActivityDailyData ::= SEQUENCE {
   noOfActivityChanges                  INTEGER SIZE(0..1440),
   activityChangeInfos                  SET SIZE(noOfActivityChanges) OF
                                        ActivityChangeInfo
}
```

noOfActivityChanges è il numero di parole (word) ActivityChangeInfo nella serie activityChangeInfos.

activityChangeInfos è la serie di parole (word) ActivityChangeInfo memorizzate nella VU il giorno in questione. Comprende sempre due parole ActivityChangeInfo che indicano la condizione delle due sedi (slot) alle 00h00 del giorno stesso.

2.171. **VuActivityDailyRecordArray**

Seconda generazione:

Informazioni, memorizzate in una VU, relative ai cambi di attività e/o alle variazioni della condizione di guida e/o alle variazioni della condizione della carta in un determinato giorno di calendario (requisiti 105, 106 e 107 dell'allegato 1C) e della condizione della sede (slot) alle 00h00 del giorno stesso.

```
VuActivityDailyRecordArray ::= SEQUENCE {
   recordType                           RecordType,
   recordSize                           INTEGER(1..65535),
   noOfRecords                          INTEGER(0..65535),
   records                              SET SIZE(noOfRecords) OF ActivityChangeInfo
}
```

recordType rappresenta il tipo di registrazione (ActivityChangeInfo).
Assegnazione valore: Cfr. RecordType

recordSize sono le dimensioni di ActivityChangeInfo in byte.

noOfRecords è il numero di registrazioni nella serie di registrazioni.

records è la serie di parole (word) ActivityChangeInfo memorizzate nella VU il giorno in questione. Comprende sempre due parole ActivityChangeInfo che indicano la condizione delle due sedi (slot) alle 00h00 del giorno stesso.

2.172. **VuApprovalNumber**

Numero di omologazione dell'unità elettronica di bordo.

Prima generazione:

```
VuApprovalNumber ::= IA5String(SIZE(8))
```

Assegnazione valore: non specificato.

Seconda generazione:

```
VuApprovalNumber ::= IA5String(SIZE(16))
```

▼B

Assegnazione valore:

Il numero di omologazione deve corrispondere a quanto pubblicato sul sito Internet della Commissione europea, vale a dire ad esempio compresi gli eventuali trattini. Il numero di omologazione deve essere allineato a sinistra.

2.173. **VuCalibrationData**

Prima generazione:

Informazioni, memorizzate in un'unità elettronica di bordo, relative alle tarature dell'apparecchio di controllo (requisito 098 dell'allegato 1B).

```
VuCalibrationData ::= SEQUENCE {
   noOfVuCalibrationRecords              INTEGER(0..255),
   vuCalibrationRecords                  SET SIZE(noOfVuCalibrationRecords) OF
                                         VuCalibrationRecord
}
```

noOfVuCalibrationRecords è il numero di registrazioni contenute nella serie vuCalibrationRecords.

vuCalibrationRecords è la serie di registrazioni di tarature.

2.174. **VuCalibrationRecord**

Informazioni, memorizzate in un'unità elettronica di bordo, relative ad una taratura dell'apparecchio di controllo (requisito 098 dell'allegato 1B e requisiti 119 e 120 dell'allegato 1C).

Prima generazione:

```
VuCalibrationRecord ::= SEQUENCE {
   calibrationPurpose                    CalibrationPurpose,
   workshopName                          Name,
   workshopAddress                       Address,
   workshopCardNumber                    FullCardNumber,
   workshopCardExpiryDate                TimeReal,
   vehicleIdentificationNumber           VehicleIdentificationNumber,
   vehicleRegistrationIdentification     VehicleRegistrationIdentification,
   wVehicleCharacteristicConstant        W-VehicleCharacteristicConstant,
   kConstantOfRecordingEquipment         K-ConstantOfRecordingEquipment,
   lTyreCircumference                    L-TyreCircumference,
   tyreSize                              TyreSize,
   authorisedSpeed                       SpeedAuthorised,
   oldOdometerValue                      OdometerShort,
   newOdometerValue                      OdometerShort,
   oldTimeValue                          TimeReal,
   newTimeValue                          TimeReal,
   nextCalibrationDate                   TimeReal
}
```

calibrationPurpose è lo scopo della taratura.

workshopName, workshopAddress sono il nome e l'indirizzo dell'officina.

workshopCardNumber identifica la carta dell'officina usata durante la taratura.

workshopCardExpiryDate è la data di termine validità della carta.

vehicleIdentificationNumber è il VIN.

▼B

vehicleRegistrationIdentification contiene il VRN e lo Stato membro di immatricolazione.

wVehicleCharacteristicConstant è il coefficiente caratteristico del veicolo.

kConstantOfRecordingEquipment è la costante dell'apparecchio di controllo.

lTyreCircumference è la circonferenza effettiva degli pneumatici delle ruote.

tyreSize è l'indicazione delle dimensioni degli pneumatici montati sul veicolo.

authorisedSpeed è la velocità autorizzata del veicolo.

oldOdometerValue, newOdometerValue sono i valori vecchio e nuovo dell'odometro.

oldTimeValue, newTimeValue sono i valori vecchio e nuovo di data e ora.

nextCalibrationDate è la data della prossima taratura del tipo specificato in CalibrationPurpose che dovrà essere effettuata dall'organismo incaricato dei controlli.

Seconda generazione:

```
VuCalibrationRecord ::= SEQUENCE {
   calibrationPurpose                    CalibrationPurpose,
   workshopName                          Name,
   workshopAddress                       Address,
   workshopCardNumber                    FullCardNumber,
   workshopCardExpiryDate                TimeReal,
   vehicleIdentificationNumber           VehicleIdentificationNumber,
   vehicleRegistrationIdentification     VehicleRegistrationIdentification,
   wVehicleCharacteristicConstant        W-VehicleCharacteristicConstant,
   kConstantOfRecordingEquipment         K-ConstantOfRecordingEquipment,
   lTyreCircumference                    L-TyreCircumference,
   tyreSize                              TyreSize,
   authorisedSpeed                       SpeedAuthorised,
   oldOdometerValue                      OdometerShort,
   newOdometerValue                      OdometerShort,
   oldTimeValue                          TimeReal,
   newTimeValue                          TimeReal,
   nextCalibrationDate                   TimeReal,
   sealDataVu                            SealDataVu
}
```

Oltre alla prima generazione, è utilizzato il seguente elemento di dati:

sealDataVu dà informazioni sui sigilli apposti a diversi componenti del veicolo.

2.175. **VuCalibrationRecordArray**

Seconda generazione:

Informazioni, memorizzate in un'unità elettronica di bordo, relative alle tarature dell'apparecchio di controllo (requisiti 119 e 120 dell'allegato 1C).

▼B

```
VuCalibrationRecordArray ::= SEQUENCE {
   recordType                              RecordType,
   recordSize                              INTEGER(1..65535),
   noOfRecords                             INTEGER(0..65535),
   records                                 SET SIZE(noOfRecords) OF
                                           VuCalibrationRecord
}
```

recordType rappresenta il tipo di registrazione (VuCalibrationRecord).
Assegnazione valore: Cfr. RecordType

recordSize sono le dimensioni di VuCalibrationRecord in byte.

noOfRecords è il numero di registrazioni nella serie di registrazioni.

records è la serie di registrazioni di taratura.

2.176. **VuCardIWData**

Prima generazione:

Informazioni, memorizzate in un'unità elettronica di bordo, relative ai cicli di inserimento ed estrazione delle carte del conducente o delle carte dell'officina nell'unità elettronica di bordo (requisito 081 dell'allegato 1B e requisito 103 dell'allegato 1C).

```
VuCardIWData ::= SEQUENCE {
   noOfIWRecords                           INTEGER(0..2^16-1),
   vuCardIWRecords                         SET SIZE(noOfIWRecords) OF VuCardIWRecord
}
```

noOfIWRecords è il numero di registrazioni nella serie vuCardIWRecords.

vuCardIWRecords è una serie di registrazioni relative ai cicli di inserimento ed estrazione della carta.

2.177. **VuCardIWRecord**

Informazioni, memorizzate in un'unità elettronica di bordo, relative ad un ciclo di inserimento ed estrazione di una carta del conducente o di una carta dell'officina nell'unità elettronica di bordo (requisito 081 dell'allegato 1B e requisito 102 dell'allegato 1C).

Prima generazione:

```
VuCardIWRecord ::= SEQUENCE {
   cardHolderName                          HolderName,
   fullCardNumber                          FullCardNumber,
   cardExpiryDate                          TimeReal,
   cardInsertionTime                       TimeReal,
   vehicleOdometerValueAtInsertion         OdometerShort,
   cardSlotNumber                          CardSlotNumber,
   cardWithdrawalTime                      TimeReal,
   vehicleOdometerValueAtWithdrawal        OdometerShort,
   previousVehicleInfo                     PreviousVehicleInfo,
   manualInputFlag                         ManualInputFlag
}
```

cardHolderName contiene il cognome e il nome o i nomi del titolare della carta del conducente o dell'officina memorizzati nella carta.

fullCardNumber specifica il tipo di carta, lo Stato membro di rilascio e il numero della carta memorizzati nella carta stessa.

▼B

cardExpiryDate è la data di termine validità della carta memorizzata nella carta stessa.

cardInsertionTime specifica la data e l'ora di inserimento.

vehicleOdometerValueAtInsertion è il valore dell'odometro del veicolo all'atto dell'inserimento della carta.

cardSlotNumber è la sede (slot) in cui è inserita la carta.

cardWithdrawalTime specifica la data e l'ora di estrazione.

vehicleOdometerValueAtWithdrawal è il valore dell'odometro del veicolo all'atto dell'estrazione della carta.

previousVehicleInfo contiene informazioni, memorizzate nella carta, relative al veicolo precedentemente utilizzato dal conducente.

manualInputFlag è un indicatore (flag) che indica se, all'atto dell'inserimento della carta, il titolare della carta abbia o meno inserito manualmente le attività del conducente.

Seconda generazione:

```
VuCardIWRecord ::= SEQUENCE {
   cardHolderName                       HolderName,
   fullCardNumberAndGeneration          FullCardNumberAndGeneration,
   cardExpiryDate                       TimeReal,
   cardInsertionTime                    TimeReal,
   vehicleOdometerValueAtInsertion      OdometerShort,
   cardSlotNumber                       CardSlotNumber,
   cardWithdrawalTime                   TimeReal,
   vehicleOdometerValueAtWithdrawal     OdometerShort,
   previousVehicleInfo                  PreviousVehicleInfo,
   manualInputFlag                      ManualInputFlag
}
```

Anziché fullCardNumber la struttura dei dati della seconda generazione usa il seguente elemento di dati.

fullCardNumberAndGeneration specifica il tipo di carta, lo Stato membro di rilascio e il numero e la generazione della carta memorizzati nella carta stessa.

2.178. **VuCardIWRecordArray**

Seconda generazione:

Informazioni, memorizzate in un'unità elettronica di bordo, relative ai cicli di inserimento ed estrazione delle carte del conducente o delle carte dell'officina nell'unità elettronica di bordo (requisito 103 dell'allegato 1C).

```
VuCardIWRecordArray ::= SEQUENCE {
   recordType                           RecordType,
   recordSize                           INTEGER(1..65535),
   noOfRecords                          INTEGER(0..65535),
   records                              SET SIZE(noOfRecords) OF VuCardIWRecord
}
```

recordType rappresenta il tipo di registrazione (VuCardIWRecord). **Assegnazione valore**: Cfr. RecordType

recordSize sono le dimensioni di VuCardIWRecord in byte.

▼B

noOfRecords è il numero di registrazioni nella serie di registrazioni.

records è una serie di registrazioni relative ai cicli di inserimento ed estrazione della carta.

2.179. **VuCardRecord**

Seconda generazione:

Informazioni, memorizzate in un'unità elettronica di bordo, relative ad una carta tachigrafica utilizzata (requisito 132 dell'allegato 1C).

```
VuCardRecord ::= SEQUENCE {
   cardExtendedSerialNumber            ExtendedSerialNumber,
   cardPersonaliserID                  OCTET STRING(SIZE(1)),
   typeofTachographCardID              EquipmentType,
   cardStructureVersion                CardStructureVersion,
   cardNumber                          CardNumber
}
```

cardExtendedSerialNumber quale letto nel file EF_ICC contenuto nel MF della carta.

cardPersonaliserID quale letto nel file EF_ICC contenuto nel MF della carta.

typeOfTachographCardId quale letto nel file EF_Application_Identification contenuto nel DF_Tachograph_G2.

cardStructureVersion quale letta nel file EF_Application_Identification contenuto nel DF_Tachograph_G2.

cardNumber quale letto nel file EF_Identification contenuto nel DF_Tachograph_G2.

2.180. **VuCardRecordArray**

Seconda generazione:

Informazioni, memorizzate in un'unità elettronica di bordo, relative alle carte tachigrafiche utilizzate con tale unità elettronica di bordo. Questa informazione è destinata all'analisi dei problemi tra la VU e la carta (requisito 132 dell'allegato 1C).

```
VuCardRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF VuCardRecord
}
```

recordType rappresenta il tipo di registrazione (VuCardRecord). **Assegnazione valore**: Cfr. RecordType

recordSize sono le dimensioni di VuCardRecord in byte.

noOfRecords è il numero di registrazioni nella serie di registrazioni.

records è una serie di registrazioni relative alle carte tachigrafiche usate con la VU.

▼B

2.181. **VuCertificate**

Certificato della chiave pubblica di un'unità elettronica di bordo.

```
VuCertificate ::= Certificate
```

2.182. **VuCertificateRecordArray**

Seconda generazione:

Il certificato della VU più i metadati usati nel protocollo di trasferimento.

```
VuCertificateRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF VuCertificate
}
```

recordType rappresenta il tipo di registrazione (VuCertificate). **Assegnazione valore**: Cfr. RecordType

recordSize sono le dimensioni di VuCertificate in byte.

noOfRecords è il numero di registrazioni nella serie di registrazioni. Il valore deve essere fissato a 1 perché i certificati possono avere lunghezze diverse.

records è una serie di certificati della VU.

2.183. **VuCompanyLocksData**

Prima generazione:

Informazioni, memorizzate in un'unità elettronica di bordo, relative ai blocchi di un'impresa (requisito 104 dell'allegato 1B).

```
VuCompanyLocksData ::= SEQUENCE {
   noOfLocks                           INTEGER(0..255),
   vuCompanyLocksRecords               SET SIZE(noOfLocks) OF VuCompanyLocksRecord
}
```

noOfLocks è il numero di blocchi elencati in vuCompanyLocksRecords.

vuCompanyLocksRecords è la serie di registrazioni dei blocchi di un'impresa.

2.184. **VuCompanyLocksRecord**

Informazioni, memorizzate in un'unità elettronica di bordo, relative ad un blocco di un'impresa (requisito 104 dell'allegato 1B e requisito 128 dell'allegato 1C).

Prima generazione:

```
VuCompanyLocksRecord ::= SEQUENCE {
   lockInTime                          TimeReal,
   lockOutTime                         TimeReal,
   companyName                         Name,
   companyAddress                      Address,
   companyCardNumber                   FullCardNumber
}
```

▼B

lockInTime, lockOutTime specificano la data e l'ora di attivazione e di disattivazione del blocco.

companyName, companyAddress specificano il nome e l'indirizzo dell'impresa connessa all'attivazione del blocco.

companyCardNumber identifica la carta usata all'atto dell'attivazione del blocco.

Seconda generazione:

```
VuCompanyLocksRecord ::= SEQUENCE {
   lockInTime                          TimeReal,
   lockOutTime                         TimeReal,
   companyName                         Name,
   companyAddress                      Address,
   companyCardNumberAndGeneration      FullCardNumberAndGeneration
}
```

Anziché companyCardNumber la struttura dei dati della seconda generazione usa il seguente elemento di dati.

companyCardNumberAndGeneration identifica la carta, compresa la generazione, usata all'atto dell'attivazione del blocco.

2.185. **VuCompanyLocksRecordArray**

Seconda generazione:

Informazioni, memorizzate in un'unità elettronica di bordo, relative ai blocchi di un'impresa (requisito 128 dell'allegato 1C).

```
VuCompanyLocksRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF
                                       VuCompanyLocksRecord
}
```

recordType rappresenta il tipo di registrazione (VuCompanyLocksRecord). **Assegnazione valore**: Cfr. RecordType

recordSize sono le dimensioni di VuCompanyLocksRecord in byte.

noOfRecords è il numero di registrazioni nella serie di registrazioni. Valore 0..255.

records è la serie di registrazioni dei blocchi di un'impresa.

2.186. **VuControlActivityData**

Prima generazione:

Informazioni, memorizzate in un'unità elettronica di bordo, relative ai controlli eseguiti utilizzando tale VU (requisito 102 dell'allegato 1B).

```
VuControlActivityData ::= SEQUENCE {
   noOfControls                        INTEGER(0..20),
   vuControlActivityRecords            SET SIZE(noOfControls) OF
                                       VuControlActivityRecord
}
```

▼B

noOfControls è il numero di controlli elencati in vuControlActivityRecords.

vuControlActivityRecords è la serie di registrazioni di attività di controllo.

2.187. **VuControlActivityRecord**

Informazioni, memorizzate in un'unità elettronica di bordo, relative ad un controllo eseguito utilizzando tale VU (requisito 102 dell'allegato 1B e requisito 126 dell'allegato 1C).

Prima generazione:

```
VuControlActivityRecord ::= SEQUENCE {
   controlType                          ControlType,
   controlTime                          TimeReal,
   controlCardNumber                    FullCardNumber,
   downloadPeriodBeginTime              TimeReal,
   downloadPeriodEndTime                TimeReal
}
```

controlType è il tipo di controllo.

controlTime sono la data e l'ora del controllo.

controlCardNumber identifica la carta di controllo usata per il controllo.

downloadPeriodBeginTime è l'ora di inizio del periodo cui si riferiscono i dati trasferiti, in caso di trasferimento.

downloadPeriodEndTime è l'ora di fine del periodo cui si riferiscono i dati trasferiti, in caso di trasferimento.

Seconda generazione:

```
VuControlActivityRecord ::= SEQUENCE {
   controlType                          ControlType,
   controlTime                          TimeReal,
   controlCardNumberAndGeneration       FullCardNumberAndGeneration,
   downloadPeriodBeginTime              TimeReal,
   downloadPeriodEndTime                TimeReal
}
```

Anziché controlCardNumber la struttura dei dati della seconda generazione usa il seguente elemento di dati.

controlCardNumberAnd Generation identifica la carta di controllo, compresa la generazione, usata per il controllo.

2.188. **VuControlActivityRecordArray**

Seconda generazione:

Informazioni, memorizzate in un'unità elettronica di bordo, relative ai controlli eseguiti utilizzando tale VU (requisito 126 dell'allegato 1C).

▼B

```
VuControlActivityRecordArray ::= SEQUENCE {
   recordType                              RecordType,
   recordSize                              INTEGER(1..65535),
   noOfRecords                             INTEGER(0..65535),
   records                                 SET SIZE(noOfRecords) OF
                                           VuControlActivityRecord
}
```

recordType rappresenta il tipo di registrazione (VuControlActivityRecord). **Assegnazione valore**: Cfr. RecordType

recordSize sono le dimensioni di VuControlActivityRecord in byte.

noOfRecords è il numero di registrazioni nella serie di registrazioni.

records è la serie di registrazioni delle attività di controllo della VU.

2.189. **VuDataBlockCounter**

Contatore, memorizzato in una carta, che indica in ordine di sequenza i cicli di inserimento ed estrazione della carta nelle unità elettroniche di bordo.

```
VuDataBlockCounter ::= BCDString(SIZE(2))
```

Assegnazione valore: numero consecutivo con valore massimo 9 999, dopodiché la numerazione ricomincia da 0.

2.190. **VuDetailedSpeedBlock**

Informazioni, memorizzate in un'unità elettronica di bordo, relative alla velocità dettagliata del veicolo per un minuto di marcia del veicolo (requisito 093 dell'allegato 1B e requisito 116 dell'allegato 1C).

```
VuDetailedSpeedBlock ::= SEQUENCE {
   speedBlockBeginDate    TimeReal,
   speedsPerSecond        SEQUENCE SIZE(60) OF Speed
}
```

speedBlockBeginDate specifica la data e l'ora del primo valore di velocità all'interno del blocco.

speedsPerSecond è la sequenza cronologica della velocità misurata ogni secondo durante il minuto che comincia da speedBlockBeginDate (inclusa).

2.191. **VuDetailedSpeedBlockRecordArray**

Seconda generazione:

Informazioni, memorizzate in un'unità elettronica di bordo, relative alla velocità dettagliata del veicolo.

```
VuDetailedSpeedBlockRecordArray ::= SEQUENCE {
   recordType                              RecordType,
   recordSize                              INTEGER(1..65535),
   noOfRecords                             INTEGER(0..65535),
   records                                 SET SIZE(noOfRecords) OF
                                           VuDetailedSpeedBlock
}
```

recordType rappresenta il tipo di registrazione (VuDetailedSpeedBlock). **Assegnazione valore**: Cfr. RecordType

▼B

recordSize sono le dimensioni di VuDetailedSpeedBlock in byte.

noOfRecords è il numero di registrazioni nella serie di registrazioni.

records è la serie di blocchi di velocità dettagliata.

2.192. **VuDetailedSpeedData**

Prima generazione:

Informazioni, memorizzate in un'unità elettronica di bordo, relative alla velocità dettagliata del veicolo.

```
VuDetailedSpeedData ::= SEQUENCE {
   noOfSpeedBlocks                    INTEGER(0..2^16-1),
   vuDetailedSpeedBlocks              SET SIZE(noOfSpeedBlocks) OF
                                      VuDetailedSpeedBlock
}
```

noOfSpeedBlocks è il numero di blocchi di velocità nella serie vuDetailedSpeedBlocks.

vuDetailedSpeedBlocks è la serie di blocchi di velocità dettagliata.

2.193. **VuDownloadablePeriod**

Le date meno recente e più recente per le quali un'unità elettronica di bordo conserva i dati relativi alle attività dei conducenti (requisiti 081, 084 o 087 dell'allegato 1B e requisiti 102, 105, 108 dell'allegato 1C).

```
VuDownloadablePeriod ::= SEQUENCE {
   minDownloadableTime                TimeReal
   maxDownloadableTime                TimeReal
}
```

minDownloadableTime specifica la data e l'ora meno recenti di inserimento della carta o di cambio di attività o di immissione del luogo memorizzate nella VU.

maxDownloadableTime specifica la data e l'ora più recenti di estrazione della carta o di cambio di attività o di immissione del luogo memorizzate nella VU.

2.194. **VuDownloadablePeriodRecordArray**

Seconda generazione:

Il VUDownloadablePeriod più i metadati usati nel protocollo di trasferimento.

```
VuDownloadablePeriodRecordArray ::= SEQUENCE {
   recordType                         RecordType,
   recordSize                         INTEGER(1..65535),
   noOfRecords                        INTEGER(0..65535),
   records                            SET SIZE(noOfRecords) OF
                                      VuDownloadablePeriod
}
```

recordType rappresenta il tipo di registrazione (VuDownloadablePeriod). **Assegnazione valore**: Cfr. RecordType

▼B

recordSize sono le dimensioni di VuDownloadablePeriod in byte.

noOfRecords è il numero di registrazioni nella serie di registrazioni.

records è la serie di registrazioni del VuDownloadablePeriod.

2.195. **VuDownloadActivityData**

Informazioni, memorizzate in un'unità elettronica di bordo, relative all'ultimo trasferimento dei suoi dati (requisito 105 dell'allegato 1B e requisito 129 dell'allegato 1C).

Prima generazione:

```
VuDownloadActivityData ::= SEQUENCE {
   downloadingTime                    TimeReal,
   fullCardNumber                     FullCardNumber,
   companyOrWorkshopName              Name
}
```

downloadingTime specifica la data e l'ora del trasferimento di dati.

fullCardNumber identifica la carta usata per autorizzare il trasferimento di dati.

companyOrWorkshopName è il nome dell'impresa o dell'officina.

Seconda generazione:

```
VuDownloadActivityData ::= SEQUENCE {
   downloadingTime                    TimeReal,
   fullCardNumberAndGeneration        FullCardNumberAndGeneration,
   companyOrWorkshopName              Name
}
```

Anziché fullCardNumber la struttura dei dati della seconda generazione usa il seguente elemento di dati.

fullCardNumberAnd Generation identifica la carta, compresa la generazione, usata per autorizzare il trasferimento di dati.

2.196. **VuDownloadActivityDataRecordArray**

Seconda generazione:

Informazioni relative all'ultimo trasferimento di dati della VU (requisito 129 dell'allegato 1C).

```
VuDownloadActivityDataRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF VuDownloadActivityData
}
```

recordType rappresenta il tipo di registrazione (VuDownloadActivityData). **Assegnazione valore**: Cfr. RecordType

recordSize sono le dimensioni di VuDownloadActivityData in byte.

noOfRecords è il numero di registrazioni nella serie di registrazioni.

▼B

records è la serie di registrazioni dei dati relativi al trasferimento.

2.197. **VuEventData**

Prima generazione:

Informazioni, memorizzate in un'unità elettronica di bordo, relative alle anomalie (requisito 094 dell'allegato 1B eccetto per il superamento di velocità).

```
VuEventData ::= SEQUENCE {
   noOfVuEvents                          INTEGER(0..255),
   vuEventRecords                        SET SIZE(noOfVuEvents) OF VuEventRecord
}
```

noOfVuEvents è il numero di anomalie elencate nella serie vuEventRecords.

vuEventRecords è una serie di registrazioni di anomalie.

2.198. **VuEventRecord**

Informazioni, memorizzate in un'unità elettronica di bordo, relative ad un'anomalia (requisito 094 dell'allegato 1B e requisito 117 dell'allegato 1C, eccetto per il superamento di velocità).

Prima generazione:

```
VuEventRecord ::= SEQUENCE {
   eventType                             EventFaultType,
   eventRecordPurpose                    EventFaultRecordPurpose,
   eventBeginTime                        TimeReal,
   eventEndTime                          TimeReal,
   cardNumberDriverSlotBegin             FullCardNumber,
   cardNumberCodriverSlotBegin           FullCardNumber,
   cardNumberDriverSlotEnd               FullCardNumber,
   cardNumberCodriverSlotEnd             FullCardNumber,
   similarEventsNumber                   SimilarEventsNumber
}
```

eventType è il tipo di anomalia.

eventRecordPurpose è lo scopo per cui è stata registrata l'anomalia.

eventBeginTime specifica la data e l'ora di inizio dell'anomalia.

eventEndTime specifica la data e l'ora di fine dell'anomalia.

cardNumberDriverSlotBegin identifica la carta inserita nella sede (slot) del conducente all'inizio dell'anomalia.

cardNumberCodriverSlotBegin identifica la carta inserita nella sede (slot) del secondo conducente all'inizio dell'anomalia.

cardNumberDriverSlotEnd identifica la carta inserita nella sede (slot) del conducente al termine dell'anomalia.

cardNumberCodriverSlotEnd identifica la carta inserita nella sede (slot) del secondo conducente al termine dell'anomalia.

similarEventsNumber è il numero di anomalie analoghe verificatesi nel giorno in questione.

Questa sequenza si può usare per tutte le anomalie, eccetto quelle relative al superamento di velocità.

▼B

Seconda generazione:

```
VuEventRecord ::= SEQUENCE {
   eventType                              EventFaultType,
   eventRecordPurpose                     EventFaultRecordPurpose,
   eventBeginTime                         TimeReal,
   eventEndTime                           TimeReal,
   cardNumberAndGenDriverSlotBegin        FullCardNumberAndGeneration,
   cardNumberAndGenCodriverSlotBegin      FullCardNumberAndGeneration,
   cardNumberAndGenDriverSlotEnd          FullCardNumberAndGeneration,
   cardNumberAndGenCodriverSlotEnd        FullCardNumberAndGeneration,
   similarEventsNumber                    SimilarEventsNumber,
   manufacturerSpecificEventFaultData   ManufacturerSpecificEventFaultData
}
```

Oltre alla prima generazione, sono utilizzati i seguenti elementi di dati:

manufacturerSpecificEventFaultData contiene ulteriori informazioni specifiche del fabbricante relative all'anomalia.

Anziché cardNumberDriverSlotBegin, cardNumberCodriverSlotBegin, cardNumberDriverSlotEnd e cardNumberCodriverSlotEnd, la struttura dei dati della seconda generazione usa i seguenti elementi di dati:

cardNumberAndGenDriverSlotBegin identifica la carta, compresa la generazione, inserita nella sede (slot) del conducente all'inizio dell'anomalia.

cardNumberAndGenCodriverSlotBegin identifica la carta, compresa la generazione, inserita nella sede (slot) del secondo conducente all'inizio dell'anomalia.

cardNumberAndGenDriverSlotEnd identifica la carta, compresa la generazione, inserita nella sede (slot) del conducente al termine dell'anomalia.

cardNumberAndGenCodriverSlotEnd identifica la carta, compresa la generazione, inserita nella sede (slot) del secondo conducente al termine dell'anomalia.

Se l'anomalia è un conflitto di orari, l'eventBeginTime e l'eventEndTime devono essere interpretati come segue:

eventBeginTime specifica la data e l'ora dell'apparecchio di controllo.

eventEndTime specifica la data e l'ora del GNSS.

2.199. **VuEventRecordArray**

Seconda generazione:

Informazioni, memorizzate in un'unità elettronica di bordo, relative alle anomalie (requisito 117 dell'allegato 1C eccetto per il superamento di velocità).

```
VuEventRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF VuEventRecord
}
```

recordType rappresenta il tipo di registrazione (VuEventRecord). **Assegnazione valore**: Cfr. RecordType

▼B

recordSize sono le dimensioni di VuEventRecord in byte.

noOfRecords è il numero di registrazioni nella serie di registrazioni.

records è una serie di registrazioni di anomalie.

2.200. **VuFaultData**

Prima generazione:

Informazioni, memorizzate in un'unità elettronica di bordo, relative ai guasti (requisito 096 dell'allegato 1B).

```
VuFaultData ::= SEQUENCE {
   noOfVuFaults                         INTEGER(0..255),
   vuFaultRecords                       SET SIZE(noOfVuFaults) OF VuFaultRecord
}
```

noOfVuFaults è il numero di guasti elencati nella serie vuFaultRecords.

vuFaultRecords è una serie di registrazioni di guasti.

2.201. **VuFaultRecord**

Informazioni, memorizzate in un'unità elettronica di bordo, relative ad un guasto (requisito 096 dell'allegato 1B e requisito 118 dell'allegato 1C).

Prima generazione:

```
VuFaultRecord ::= SEQUENCE {
   faultType                            EventFaultType,
   faultRecordPurpose                   EventFaultRecordPurpose,
   faultBeginTime                       TimeReal,
   faultEndTime                         TimeReal,
   cardNumberDriverSlotBegin            FullCardNumber,
   cardNumberCodriverSlotBegin          FullCardNumber,
   cardNumberDriverSlotEnd              FullCardNumber,
   cardNumberCodriverSlotEnd            FullCardNumber
}
```

faultType è il tipo di guasto dell'apparecchio di controllo.

faultRecordPurpose è lo scopo per cui è stato registrato il guasto.

faultBeginTime specifica la data e l'ora di inizio del guasto.

faultEndTime specifica la data e l'ora di fine del guasto.

cardNumberDriverSlotBegin identifica la carta inserita nella sede (slot) del conducente all'inizio del guasto.

cardNumberCodriverSlotBegin identifica la carta inserita nella sede (slot) del secondo conducente all'inizio del guasto.

cardNumberDriverSlotEnd identifica la carta inserita nella sede (slot) del conducente al termine del guasto.

cardNumberCodriverSlotEnd identifica la carta inserita nella sede (slot) del secondo conducente al termine del guasto.

▼B

Seconda generazione:

```
VuFaultRecord ::= SEQUENCE {
   faultType                              EventFaultType,
   faultRecordPurpose                     EventFaultRecordPurpose,
   faultBeginTime                         TimeReal,
   faultEndTime                           TimeReal,
   cardNumberAndGenDriverSlotBegin        FullCardNumberAndGeneration,
   cardNumberAndGenCodriverSlotBegin      FullCardNumberAndGeneration,
   cardNumberAndGenDriverSlotEnd          FullCardNumberAndGeneration,
   cardNumberAndGenCodriverSlotEnd        FullCardNumberAndGeneration,
   manufacturerSpecificEventFaultData   ManufacturerSpecificEventFaultData
}
```

Oltre alla prima generazione, è utilizzato il seguente elemento di dati:

manufacturerSpecificEventFaultData contiene ulteriori informazioni specifiche del fabbricante relative al guasto.

Anziché cardNumberDriverSlotBegin, cardNumberCodriverSlotBegin, cardNumberDriverSlotEnd e cardNumberCodriverSlotEnd, la struttura dei dati della seconda generazione usa i seguenti elementi di dati:

cardNumberAndGenDriverSlotBegin identifica la carta, compresa la generazione, inserita nella sede (slot) del conducente all'inizio del guasto.

cardNumberAndGenCodriverSlotBegin identifica la carta, compresa la generazione, inserita nella sede (slot) del secondo conducente all'inizio del guasto.

cardNumberAndGenDriverSlotEnd identifica la carta, compresa la generazione, inserita nella sede (slot) del conducente al termine del guasto.

cardNumberAndGenCodriverSlotEnd identifica la carta, compresa la generazione, inserita nella sede (slot) del secondo conducente al termine del guasto.

2.202. **VuFaultRecordArray**

Seconda generazione:

Informazioni, memorizzate in un'unità elettronica di bordo, relative ai guasti (requisito 118 dell'allegato 1C).

```
VuFaultRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF VuFaultRecord
}
```

recordType rappresenta il tipo di registrazione (VuFaultRecord). **Assegnazione valore**: Cfr. RecordType

recordSize sono le dimensioni di VuFaultRecord in byte.

noOfRecords è il numero di registrazioni nella serie di registrazioni.

records è una serie di registrazioni di guasti.

▼B

2.203. **VuGNSSCDRecord**

Seconda generazione:

Informazioni, memorizzate in un'unità elettronica di bordo, relative alla posizione del veicolo rilevata dal GNSS, se il periodo di guida continuo del conducente raggiunge un multiplo di tre ore (requisiti 108 e 110 dell'allegato 1C).

```
VuGNSSCDRecord ::= SEQUENCE {
   timeStamp                          TimeReal,
   cardNumberAndGenDriverSlot         FullCardNumberAndGeneration,
   cardNumberAndGenCodriverSlot       FullCardNumberAndGeneration,
   gnssPlaceRecord                    GNSSPlaceRecord
}
```

timeStamp indica la data e l'ora in cui il periodo di guida continuo del titolare della carta raggiunge un multiplo di tre ore.

cardNumberAndGenDriverSlot identifica la carta, compresa la generazione, inserita nella sede (slot) del conducente.

cardNumberAndGenCodriverSlot identifica la carta, compresa la generazione, inserita nella sede (slot) del secondo conducente.

gnssPlaceRecord contiene informazioni relative alla posizione del veicolo.

2.204. **VuGNSSCDRecordArray**

Seconda generazione:

Informazioni, memorizzate in un'unità elettronica di bordo, relative alla posizione del veicolo rilevata dal GNSS, se il periodo di guida continuo del conducente raggiunge un multiplo di tre ore (requisiti 108 e 110 dell'allegato 1C).

```
VuGNSSCDRecordArray  ::= SEQUENCE {
   recordType                         RecordType,
   recordSize                         INTEGER(1..65535),
   noOfRecords                        INTEGER(0..65535),
   records                            SET SIZE(noOfRecords) OF VuGNSSCDRecord
}
```

recordType rappresenta il tipo di registrazione (VuGNSSCDRecord).
Assegnazione valore: Cfr. RecordType

recordSize sono le dimensioni di VuGNSSCDRecord in byte.

noOfRecords è il numero di registrazioni nella serie di registrazioni.

records è una serie di registrazioni di guida continua rilevata dal GNSS.

2.205. **VuIdentification**

Informazioni, memorizzate in un'unità elettronica di bordo, relative all'identificazione dell'unità stessa (requisito 075 dell'allegato 1B e requisiti 93 e 121 dell'allegato 1C).

▼B

Prima generazione:

```
VuIdentification ::= SEQUENCE {
   vuManufacturerName                    VuManufacturerName,
   vuManufacturerAddress                 VuManufacturerAddress,
   vuPartNumber                          VuPartNumber,
   vuSerialNumber                        VuSerialNumber,
   vuSoftwareIdentification              VuSoftwareIdentification,
   vuManufacturingDate                   VuManufacturingDate,
   vuApprovalNumber                      VuApprovalNumber
}
```

vuManufacturerName è il nome del fabbricante dell'unità elettronica di bordo.

vuManufacturerAddress è l'indirizzo del fabbricante dell'unità elettronica di bordo.

vuPartNumber è il codice componente dell'unità elettronica di bordo.

vuSerialNumber è il numero di serie dell'unità elettronica di bordo.

vuSoftwareIdentification identifica il software installato nell'unità elettronica di bordo.

vuManufacturingDate è la data di fabbricazione dell'unità elettronica di bordo.

vuApprovalNumber è il numero di omologazione dell'unità elettronica di bordo.

Seconda generazione:

```
VuIdentification ::= SEQUENCE {
   vuManufacturerName                    VuManufacturerName,
   vuManufacturerAddress                 VuManufacturerAddress,
   vuPartNumber                          VuPartNumber,
   vuSerialNumber                        VuSerialNumber,
   vuSoftwareIdentification              VuSoftwareIdentification,
   vuManufacturingDate                   VuManufacturingDate,
   vuApprovalNumber                      VuApprovalNumber,
   vuGeneration                          Generation,
   vuAbility                             VuAbility
}
```

Oltre alla prima generazione, sono utilizzati i seguenti elementi di dati:

vuGenerationidentifica la generazione dell'unità elettronica di bordo.

vuAbility fornisce informazioni in merito al fatto che la VU supporti o meno carte tachigrafiche di prima generazione.

2.206. **VuIdentificationRecordArray**

Seconda generazione:

La VuIdentification più i metadati usati nel protocollo di trasferimento.

▼B

```
VuIdentificationRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF VuIdentification
}
```

recordType rappresenta il tipo di registrazione (VuIdentification). **Assegnazione valore**: Cfr. RecordType

recordSize sono le dimensioni di VuIdentification in byte.

noOfRecords è il numero di registrazioni nella serie di registrazioni.

records è una serie di registrazioni di VuIdentification.

2.207. **VuITSConsentRecord**

Seconda generazione:

Informazioni, memorizzate in un'unità elettronica di bordo, relative al consenso di un conducente ad utilizzare sistemi di trasporto intelligenti.

```
VuITSConsentRecord ::= SEQUENCE {
   cardNumberAndGen                    FullCardNumberAndGeneration,
   consent                             BOOLEAN
}
```

cardNumberAndGen identifica la carta, compresa la generazione. Deve essere una carta del conducente o una carta dell'officina.

consent è un indicatore (flag) che indica se il conducente ha dato il suo consenso all'uso di sistemi di trasporto intelligenti con questo veicolo o con questa unità elettronica di bordo.

Assegnazione valore:

VERO	indica il consenso del conducente ad utilizzare sistemi di trasporto intelligenti
FALSO	indica il rifiuto del conducente ad utilizzare sistemi di trasporto intelligenti

2.208. **VuITSConsentRecordArray**

Seconda generazione:

Informazioni, memorizzate in un'unità elettronica di bordo, relative al consenso del conducente ad utilizzare sistemi di trasporto intelligenti (requisito 200 dell'allegato 1C).

```
VuITSConsentRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF VuITSConsentRecord
}
```

recordType rappresenta il tipo di registrazione (VuITSConsentRecord). **Assegnazione valore**: Cfr. RecordType

recordSize sono le dimensioni di VuITSConsentRecord in byte.

noOfRecords è il numero di registrazioni nella serie di registrazioni.

records è la serie di registrazioni dei consensi ad utilizzare ITS.

▼B

2.209. **VuManufacturerAddress**

Indirizzo del fabbricante dell'unità elettronica di bordo.

```
VuManufacturerAddress ::= Address
```

Assegnazione valore: non specificato.

2.210. **VuManufacturerName**

Nome del fabbricante dell'unità elettronica di bordo.

```
VuManufacturerName ::= Name
```

Assegnazione valore: non specificato.

2.211. **VuManufacturingDate**

Data di fabbricazione dell'unità elettronica di bordo.

```
VuManufacturingDate ::= TimeReal
```

Assegnazione valore: non specificato.

2.212. **VuOverSpeedingControlData**

Informazioni, memorizzate in un'unità elettronica di bordo, relative alle anomalie per superamento di velocità verificatesi dopo l'ultimo controllo del superamento di velocità (requisito 095 dell'allegato 1B e requisito 117 dell'allegato 1C).

```
VuOverSpeedingControlData ::= SEQUENCE {
   lastOverspeedControlTime             TimeReal,
   firstOverspeedSince                  TimeReal,
   numberOfOverspeedSince               OverspeedNumber
}
```

lastOverspeedControlTime specifica la data e l'ora dell'ultimo controllo del superamento di velocità.

firstOverspeedSince specifica la data e l'ora del primo superamento di velocità dopo tale controllo del superamento di velocità.

numberOfOverspeedSince è il numero di anomalie per superamento di velocità verificatesi dopo l'ultimo controllo del superamento di velocità.

2.213. **VuOverSpeedingControlDataRecordArray**

Seconda generazione:

I VuOverSpeedingControlData più i metadati usati nel protocollo di trasferimento.

```
VuOverSpeedingControlDataRecordArray ::= SEQUENCE {
   recordType                           RecordType,
   recordSize                           INTEGER(1..65535),
   noOfRecords                          INTEGER(0..65535),
   records                              SET SIZE(noOfRecords) OF
                                        VuOverSpeedingControlData
}
```

▼B

recordType rappresenta il tipo di registrazione (VuOverSpeedingControlData). **Assegnazione valore**: Cfr. RecordType

recordSize sono le dimensioni di VuOverSpeedingControlData in byte.

noOfRecords è il numero di registrazioni nella serie di registrazioni.

records è una serie di registrazioni dei dati di controllo del superamento di velocità.

2.214. **VuOverSpeedingEventData**

Prima generazione:

Informazioni, memorizzate in un'unità elettronica di bordo, relative alle anomalie per superamento di velocità (requisito 094 dell'allegato 1B).

```
VuOverSpeedingEventData ::= SEQUENCE {
   noOfVuOverSpeedingEvents              INTEGER(0..255),
   vuOverSpeedingEventRecords            SET SIZE(noOfVuOverSpeedingEvents) OF
                                         VuOverSpeedingEventRecord
}
```

noOfVuOverSpeedingEvents è il numero di anomalie elencate nella serie vuOverSpeedingEventRecords.

vuOverSpeedingEventRecords è una serie di registrazioni di anomalie per superamento di velocità.

2.215. **VuOverSpeedingEventRecord**

Prima generazione:

Informazioni, memorizzate in un'unità elettronica di bordo, relative ad anomalie per superamento di velocità (requisito 094 dell'allegato 1B e requisito 117 dell'allegato 1C).

```
VuOverSpeedingEventRecord ::= SEQUENCE {
   eventType                             EventFaultType,
   eventRecordPurpose                    EventFaultRecordPurpose,
   eventBeginTime                        TimeReal,
   eventEndTime                          TimeReal,
   maxSpeedValue                         SpeedMax,
   averageSpeedValue                     SpeedAverage,
   cardNumberDriverSlotBegin             FullCardNumber,
   similarEventsNumber                   SimilarEventsNumber
}
```

eventType è il tipo di anomalia.

eventRecordPurpose è lo scopo per cui è stata registrata l'anomalia.

eventBeginTime specifica la data e l'ora di inizio dell'anomalia.

eventEndTime specifica la data e l'ora di fine dell'anomalia.

maxSpeedValue è la velocità massima misurata durante l'anomalia.

averageSpeedValue è la media aritmetica della velocità misurata durante l'anomalia.

▼B

cardNumberDriverSlotBegin identifica la carta inserita nella sede (slot) del conducente all'inizio dell'anomalia.

similarEventsNumber è il numero di anomalie analoghe verificatesi nel giorno in questione.

Seconda generazione:

Informazioni, memorizzate in un'unità elettronica di bordo, relative ad anomalie per superamento di velocità (requisito 094 dell'allegato 1B e requisito 117 dell'allegato 1C).

```
VuOverSpeedingEventRecord ::= SEQUENCE {
   eventType                          EventFaultType,
   eventRecordPurpose                 EventFaultRecordPurpose,
   eventBeginTime                     TimeReal,
   eventEndTime                       TimeReal,
   maxSpeedValue                      SpeedMax,
   averageSpeedValue                  SpeedAverage,
   cardNumberAndGenDriverSlotBegin    FullCardNumberAndGeneration,
   similarEventsNumber                SimilarEventsNumber
}
```

Anziché cardNumberDriverSlotBegin la struttura dei dati della seconda generazione usa il seguente elemento di dati.

cardNumberAndGenDriverSlotBegin identifica la carta, compresa la generazione, inserita nella sede (slot) «conducente» all'inizio dell'anomalia.

2.216. **VuOverSpeedingEventRecordArray**

Seconda generazione:

Informazioni, memorizzate in un'unità elettronica di bordo, relative alle anomalie per superamento di velocità (requisito 117 dell'allegato 1C).

```
VuOverSpeedingEventRecordArray ::= SEQUENCE {
   recordType                         RecordType,
   recordSize                         INTEGER(1..65535),
   noOfRecords                        INTEGER(0..65535),
   records                            SET SIZE(noOfRecords) OF
                                      VuOverSpeedingEventRecord
}
```

recordType rappresenta il tipo di registrazione (VuOverSpeedingEventRecord). **Assegnazione valore**: Cfr. RecordType

recordSize sono le dimensioni di VuOverSpeedingEventRecord in byte.

noOfRecords è il numero di registrazioni nella serie di registrazioni.

records è una serie di registrazioni di anomalie per superamento di velocità.

2.217. **VuPartNumber**

Codice componente dell'unità elettronica di bordo.

```
VuPartNumber ::= IA5String(SIZE(16))
```

Assegnazione valore: a cura del fabbricante della VU.

▼B

2.218. **VuPlaceDailyWorkPeriodData**

Prima generazione:

Informazioni, memorizzate in un'unità elettronica di bordo, relative ai luoghi in cui i conducenti iniziano o terminano un periodo di lavoro giornaliero (requisito 087 dell'allegato 1B e requisiti 108 e 110 dell'allegato 1C).

```
VuPlaceDailyWorkPeriodData ::= SEQUENCE {
   noOfPlaceRecords                    INTEGER(0..255),
   vuPlaceDailyWorkPeriodRecords       SET SIZE(noOfPlaceRecords) OF
                                       VuPlaceDailyWorkPeriodRecord
}
```

noOfPlaceRecords è il numero di registrazioni elencate nella serie vuPlaceDailyWorkPeriodRecords.

vuPlaceDailyWorkPeriodRecords è una serie di registrazioni relative ai luoghi.

2.219. **VuPlaceDailyWorkPeriodRecord**

Prima generazione:

Informazioni, memorizzate in un'unità elettronica di bordo, relative al luogo in cui il conducente inizia o termina un periodo di lavoro giornaliero (requisito 087 dell'allegato 1B e requisiti 108 e 110 dell'allegato 1C).

```
VuPlaceDailyWorkPeriodRecord ::= SEQUENCE {
   fullCardNumber                      FullCardNumber,
   placeRecord                         PlaceRecord
}
```

fullCardNumber specifica il tipo di carta del conducente, lo Stato membro di rilascio e il numero della carta.

placeRecord contiene le informazioni relative al luogo inserito.

Seconda generazione:

Informazioni, memorizzate in un'unità elettronica di bordo, relative al luogo in cui il conducente inizia o termina un periodo di lavoro giornaliero (requisito 087 dell'allegato 1B e requisiti 108 e 110 dell'allegato 1C).

```
VuPlaceDailyWorkPeriodRecord ::= SEQUENCE {
   fullCardNumberAndGeneration         FullCardNumberAndGeneration,
   placeRecord                         PlaceRecord
}
```

Anziché fullCardNumber la struttura dei dati della seconda generazione usa il seguente elemento di dati:

fullCardNumberAndGeneration specifica il tipo di carta, lo Stato membro di rilascio e il numero e la generazione della carta memorizzati nella carta stessa.

▼B

2.220. **VuPlaceDailyWorkPeriodRecordArray**

Seconda generazione:

Informazioni, memorizzate in un'unità elettronica di bordo, relative ai luoghi in cui i conducenti iniziano o terminano un periodo di lavoro giornaliero (requisiti 108 e 110 dell'allegato 1C).

```
VuPlaceDailyWorkPeriodRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF
                                       VuPlaceDailyWorkPeriodRecord
}
```

recordType rappresenta il tipo di registrazione (VuPlaceDailyWorkPeriodRecord). **Assegnazione valore**: Cfr. RecordType

recordSize sono le dimensioni di VuPlaceDailyWorkPeriodRecord in byte.

noOfRecords è il numero di registrazioni nella serie di registrazioni.

records è una serie di registrazioni relative ai luoghi.

2.221. **VuPrivateKey**

Prima generazione:

La chiave privata di un'unità elettronica di bordo.

```
VuPrivateKey ::= RSAKeyPrivateExponent
```

2.222. **VuPublicKey**

Prima generazione:

La chiave pubblica di un'unità elettronica di bordo.

```
VuPublicKey ::= PublicKey
```

2.223. **VuSerialNumber**

Numero di serie dell'unità elettronica di bordo (requisito 075 dell'allegato 1B e requisito 93 dell'allegato 1C).

```
VuSerialNumber ::= ExtendedSerialNumber
```

2.224. **VuSoftInstallationDate**

Data di installazione del software dell'unità elettronica di bordo.

```
VuSoftInstallationDate ::= TimeReal
```

Assegnazione valore: non specificato.

▼B

2.225. **VuSoftwareIdentification**

Informazioni, memorizzate in un'unità elettronica di bordo, relative al software installato.

```
VuSoftwareIdentification ::= SEQUENCE {
   vuSoftwareVersion                    VuSoftwareVersion,
   vuSoftInstallationDate               VuSoftInstallationDate
}
```

vuSoftwareVersion è il numero della versione del software dell'unità elettronica di bordo.

vuSoftInstallationDate è la data di installazione del software.

2.226. **VuSoftwareVersion**

Numero della versione del software dell'unità elettronica di bordo.

```
VuSoftwareVersion ::= IA5String(SIZE(4))
```

Assegnazione valore: non specificato.

2.227. **VuSpecificConditionData**

Prima generazione:

Informazioni, memorizzate in un'unità elettronica di bordo, relative a condizioni particolari.

```
VuSpecificConditionData ::= SEQUENCE {
   noOfSpecificConditionRecords         INTEGER(0..2^16-1)
   specificConditionRecords             SET SIZE (noOfSpecificConditionRecords) OF
                                        SpecificConditionRecord
}
```

noOfSpecificConditionRecords è il numero di registrazioni elencate nella serie specificConditionRecords.

specificConditionRecords è una serie di registrazioni relative a condizioni particolari.

2.228. **VuSpecificConditionRecordArray**

Seconda generazione:

Informazioni, memorizzate in un'unità elettronica di bordo, relative a condizioni particolari (requisito 130 dell'allegato 1C).

```
VuSpecificConditionRecordArray ::= SEQUENCE {
   recordType                           RecordType,
   recordSize                           INTEGER(1..65535),
   noOfRecords                          INTEGER(0..65535),
   records                              SET SIZE(noOfRecords) OF
                                        SpecificConditionRecord
}
```

recordType rappresenta il tipo di registrazione (SpecificConditionRecord). **Assegnazione valore**: Cfr. RecordType

recordSize sono le dimensioni di SpecificConditionRecord in byte.

noOfRecords è il numero di registrazioni nella serie di registrazioni.

records è una serie di registrazioni relative a condizioni particolari.

▼B

2.229. **VuTimeAdjustmentData**

Prima generazione:

Informazioni, memorizzate in un'unità elettronica di bordo, relative alle regolazioni dell'ora effettuate al di fuori di un ciclo ordinario di taratura (requisito 101 dell'allegato 1B).

```
VuTimeAdjustmentData ::= SEQUENCE {
   noOfVuTimeAdjRecords                    INTEGER(0..6),
   vuTimeAdjustmentRecords                 SET SIZE(noOfVuTimeAdjRecords) OF
                                           VuTimeAdjustmentRecord
}
```

noOfVuTimeAdjRecords è il numero di registrazioni contenute in vuTimeAdjustmentRecords.

vuTimeAdjustmentRecords è una serie di registrazioni di regolazioni dell'ora.

2.230. **VuTimeAdjustmentGNSSRecord**

Seconda generazione:

Informazioni, memorizzate in un'unità elettronica di bordo, relative ad una regolazione dell'ora basata sui dati relativi all'ora trasmessi dal GNSS (requisiti 124 e 125 dell'allegato 1C).

```
VuTimeAdjustmentGNSSRecord ::= SEQUENCE {
   oldTimeValue                            TimeReal,
   newTimeValue                            TimeReal
}
```

oldTimeValue, newTimeValue sono i valori vecchio e nuovo di data e ora.

2.231. **VuTimeAdjustmentGNSSRecordArray**

Seconda generazione:

Informazioni, memorizzate in un'unità elettronica di bordo, relative ad una regolazione dell'ora effettuata dal GNSS o basata sui dati relativi all'ora trasmessi dal GNSS (requisiti 124 e 125 dell'allegato 1C).

```
VuTimeAdjustmentGNSSRecordArray ::= SEQUENCE {
   recordType                              RecordType,
   recordSize                              INTEGER(1..65535),
   noOfRecords                             INTEGER(0..65535),
   records                                 SET SIZE(noOfRecords) OF
                                           VuTimeAdjustmentGNSSRecord
}
```

recordType rappresenta il tipo di registrazione (VuTimeAdjustmentGNSSRecord). **Assegnazione valore**: Cfr. RecordType

recordSize è la dimensione di VuTimeAdjustmentGNSSRecord in byte.

noOfRecords è il numero di registrazioni nella serie di registrazioni.

records è una serie di registrazioni delle regolazioni dell'ora del GNSS.

▼B

2.232. **VuTimeAdjustmentRecord**

Informazioni, memorizzate in un'unità elettronica di bordo, relative ad una regolazione dell'ora effettuata al di fuori di un ciclo ordinario di taratura (requisito 101 dell'allegato 1B e requisiti 124 e 125 dell'allegato 1C).

Prima generazione:

```
VuTimeAdjustmentRecord ::= SEQUENCE {
   oldTimeValue                         TimeReal,
   newTimeValue                         TimeReal,
   workshopName                         Name,
   workshopAddress                      Address,
   workshopCardNumber                   FullCardNumber
}
```

oldTimeValue, newTimeValue sono i valori vecchio e nuovo di data e ora.

workshopName, workshopAddress sono il nome e l'indirizzo dell'officina.

workshopCardNumber identifica la carta dell'officina utilizzata per effettuare la regolazione dell'ora.

Seconda generazione:

```
VuTimeAdjustmentRecord ::= SEQUENCE {
   oldTimeValue                         TimeReal,
   newTimeValue                         TimeReal,
   workshopName                         Name,
   workshopAddress                      Address,
   workshopCardNumberAndGeneration      FullCardNumberAndGeneration
}
```

Anziché workshopCardNumber, la struttura dei dati della seconda generazione usa il seguente elemento di dati.

workshopCardNumberAnd Generation identifica la carta dell'officina, compresa la generazione, utilizzata per effettuare la regolazione dell'ora.

2.233. **VuTimeAdjustmentRecordArray**

Seconda generazione:

Informazioni, memorizzate in un'unità elettronica di bordo, relative alle regolazioni dell'ora effettuate al di fuori di un ciclo ordinario di taratura (requisiti 124 e 125 dell'allegato 1C).

```
VuTimeAdjustmentRecordArray ::= SEQUENCE {
   recordType                           RecordType,
   recordSize                           INTEGER(1..65535),
   noOfRecords                          INTEGER(0..65535),
   records                              SET SIZE(noOfRecords) OF
                                        VuTimeAdjustmentRecord
}
```

recordType rappresenta il tipo di registrazione (VuTimeAdjustmentRecord). **Assegnazione valore**: Cfr. RecordType

recordSize è la dimensione di VuTimeAdjustmentRecord in byte.

▼B

noOfRecords è il numero di registrazioni nella serie di registrazioni.

records è una serie di registrazioni di regolazioni dell'ora.

2.234. **WorkshopCardApplicationIdentification**

Informazioni, memorizzate in una carta dell'officina, relative all'identificazione dell'applicazione della carta (requisiti 307 e 330 dell'allegato 1C).

Prima generazione:

```
WorkshopCardApplicationIdentification ::= SEQUENCE {
   typeOfTachographCardId               EquipmentType,
   cardStructureVersion                 CardStructureVersion,
   noOfEventsPerType                    NoOfEventsPerType,
   noOfFaultsPerType                    NoOfFaultsPerType,
   activityStructureLength              CardActivityLengthRange,
   noOfCardVehicleRecords               NoOfCardVehicleRecords,
   noOfCardPlaceRecords                 NoOfCardPlaceRecords,
   noOfCalibrationRecords               NoOfCalibrationRecords
}
```

typeOfTachographCardId specifica il tipo di carta.

cardStructureVersion specifica la versione della struttura utilizzata nella carta.

noOfEventsPerType è il numero di anomalie per tipo di anomalia che la carta è in grado di registrare.

noOfFaultsPerType è il numero di guasti per tipo di guasto che la carta è in grado di registrare.

activityStructureLength indica il numero di byte disponibili per memorizzare le registrazioni delle attività.

noOfCardVehicleRecords è il numero di registrazioni del veicolo che la carta è in grado di contenere.

noOfCardPlaceRecords è il numero di luoghi che la carta è in grado di registrare.

noOfCalibrationRecords è il numero di registrazioni di tarature che la carta è in grado di memorizzare.

Seconda generazione:

```
WorkshopCardApplicationIdentification ::= SEQUENCE {
   typeOfTachographCardId               EquipmentType,
   cardStructureVersion                 CardStructureVersion,
   noOfEventsPerType                    NoOfEventsPerType,
   noOfFaultsPerType                    NoOfFaultsPerType,
   activityStructureLength              CardActivityLengthRange,
   noOfCardVehicleRecords               NoOfCardVehicleRecords,
   noOfCardPlaceRecords                 NoOfCardPlaceRecords,
   noOfCalibrationRecords               NoOfCalibrationRecords,
   noOfGNSSCDRecords                    NoOfGNSSCDRecords,
   noOfSpecificConditionRecords         NoOfSpecificConditionRecords
}
```

Oltre alla prima generazione, sono utilizzati i seguenti elementi di dati:

noOfGNSSCDRecords è il numero di registrazioni di guida continua del GNSS che la carta è in grado di memorizzare.

▼B

noOfSpecificConditionRecords è il numero di registrazioni di condizioni particolari che la carta è in grado di memorizzare.

2.235. **WorkshopCardCalibrationData**

Informazioni, memorizzate in una carta dell'officina, relative alle attività dell'officina eseguite con la carta (requisiti 314, 316, 337 e 339 dell'allegato 1C).

```
WorkshopCardCalibrationData ::= SEQUENCE {
   calibrationTotalNumber              INTEGER(0 .. 2^16-1),
   calibrationPointerNewestRecord      INTEGER(0 .. NoOfCalibrationRecords-1),
   calibrationRecords                  SET SIZE(NoOfCalibrationRecords) OF
                                       WorkshopCardCalibrationRecord
}
```

calibrationTotalNumber è il numero totale di tarature effettuate con la carta.

calibrationPointerNewestRecord è l'indice della registrazione di taratura più aggiornata.

Assegnazione valore: numero corrispondente al numeratore della registrazione di taratura, a partire da ′0′ per la prima volta in cui tale registrazione compare nella struttura.

calibrationRecords è la serie di registrazioni contenenti le informazioni relative alle tarature e/o regolazioni dell'ora.

2.236. **WorkshopCardCalibrationRecord**

Informazioni, memorizzate in una carta dell'officina, relative ad una taratura eseguita con la carta (requisiti 314 e 337 dell'allegato 1C).

Prima generazione:

```
WorkshopCardCalibrationRecord ::= SEQUENCE {
   calibrationPurpose                  CalibrationPurpose,
   vehicleIdentificationNumber         VehicleIdentificationNumber,
   vehicleRegistration                 VehicleRegistrationIdentification,
   wVehicleCharacteristicConstant      W-VehicleCharacteristicConstant,
   kConstantOfRecordingEquipment       K-ConstantOfRecordingEquipment,
   lTyreCircumference                  L-TyreCircumference,
   tyreSize                            TyreSize,
   authorisedSpeed                     SpeedAuthorised,
   oldOdometerValue                    OdometerShort,
   newOdometerValue                    OdometerShort,
   oldTimeValue                        TimeReal,
   newTimeValue                        TimeReal,
   nextCalibrationDate                 TimeReal,
   vuPartNumber                        VuPartNumber,
   vuSerialNumber                      VuSerialNumber,
   sensorSerialNumber                  SensorSerialNumber
}
```

calibrationPurpose è lo scopo della taratura.

vehicleIdentificationNumber è il VIN.

vehicleRegistration contiene il VRN e lo Stato membro di immatricolazione.

wVehicleCharacteristicConstant è il coefficiente caratteristico del veicolo.

▼B

kConstantOfRecordingEquipment è la costante dell'apparecchio di controllo.

lTyreCircumference è la circonferenza effettiva degli pneumatici delle ruote.

tyreSize è l'indicazione delle dimensioni degli pneumatici montati sul veicolo.

authorisedSpeed è la velocità massima autorizzata del veicolo.

oldOdometerValue, newOdometerValue sono i valori vecchio e nuovo dell'odometro.

oldTimeValue, newTimeValue sono i valori vecchio e nuovo di data e ora.

nextCalibrationDate è la data della prossima taratura del tipo specificato in CalibrationPurpose che dovrà essere effettuata dall'organismo incaricato dei controlli.

vuPartNumber, **vuSerialNumber** e **sensorSerialNumber** contengono gli elementi di dati per l'identificazione dell'apparecchio di controllo.

Seconda generazione:

```
WorkshopCardCalibrationRecord ::= SEQUENCE {
   calibrationPurpose                  CalibrationPurpose,
   vehicleIdentificationNumber         VehicleIdentificationNumber,
   vehicleRegistration                 VehicleRegistrationIdentification,
   wVehicleCharacteristicConstant      W-VehicleCharacteristicConstant,
   kConstantOfRecordingEquipment       K-ConstantOfRecordingEquipment,
   lTyreCircumference                  L-TyreCircumference,
   tyreSize                            TyreSize,
   authorisedSpeed                     SpeedAuthorised,
   oldOdometerValue                    OdometerShort,
   newOdometerValue                    OdometerShort,
   oldTimeValue                        TimeReal,
   newTimeValue                        TimeReal,
   nextCalibrationDate                 TimeReal,
   vuPartNumber                        VuPartNumber,
   vuSerialNumber                      VuSerialNumber,
   sensorSerialNumber                  SensorSerialNumber,
   sensorGNSSSerialNumber              SensorGNSSSerialNumber,
   rcmSerialNumber                     RemoteCommunicationModuleSerialNumber,
   sealDataCard                        SealDataCard
}
```

Oltre alla prima generazione, sono utilizzati i seguenti elementi di dati:

sensorGNSSSerialNumber identifica un dispositivo GNSS esterno.

rcmSerialNumber identifica un modulo di comunicazione remota.

sealDataCard dà informazioni sui sigilli apposti a diversi componenti del veicolo.

▼B

2.237. **WorkshopCardHolderIdentification**

Informazioni, memorizzate in una carta dell'officina, relative all'identificazione del titolare della carta (requisiti 311 e 334 dell'allegato 1C).

```
WorkshopCardHolderIdentification ::= SEQUENCE {
   workshopName                        Name,
   workshopAddress                     Address,
   cardHolderName                      HolderName,
   cardHolderPreferredLanguage         Language
}
```

workshopName è il nome dell'officina del titolare della carta.

workshopAddress è l'indirizzo dell'officina del titolare della carta.

cardHolderName specifica il cognome e il/i nome/i del titolare (per esempio il nome del meccanico).

cardHolderPreferredLanguage è la lingua abituale del titolare della carta.

2.238. **WorkshopCardPIN**

Numero di identificazione personale (PIN) della carta dell'officina (requisiti 309 e 332 dell'allegato 1C).

```
WorkshopCardPIN ::= IA5String(SIZE(8))
```

Assegnazione valore: il PIN noto al titolare della carta, riempito a destra con byte 'FF' fino a raggiungere 8 byte.

2.239. **W-VehicleCharacteristicConstant**

Coefficiente caratteristico del veicolo [definizione k)].

```
W-VehicleCharacteristicConstant ::= INTEGER(0..2^16-1))
```

Assegnazione valore: impulsi per chilometro nell'intervallo operativo 0-64 255 impulsi/km.

2.240. **VuPowerSupplyInterruptionRecord**

Seconda generazione:

Informazioni, memorizzate in un'unità elettronica di bordo, relative alle interruzioni dell'alimentazione di energia (requisito 117 dell'allegato 1C).

```
VuPowerSupplyInterruptionRecord ::= SEQUENCE {
   eventType                           EventFaultType,
   eventRecordPurpose                  EventFaultRecordPurpose,
   eventBeginTime                      TimeReal,
   eventEndTime                        TimeReal,
   cardNumberAndGenDriverSlotBegin     FullCardNumberAndGeneration,
   cardNumberAndGenDriverSlotEnd       FullCardNumberAndGeneration,
   cardNumberAndGenCodriverSlotBegin   FullCardNumberAndGeneration,
   cardNumberAndGenCodriverSlotEnd     FullCardNumberAndGeneration,
   similarEventsNumber                 SimilarEventsNumber
}
```

eventType è il tipo di anomalia.

eventRecordPurpose è lo scopo per cui è stata registrata l'anomalia.

eventBeginTime specifica la data e l'ora di inizio dell'anomalia.

▼B

eventEndTime specifica la data e l'ora di fine dell'anomalia.

cardNumberAndGenDriverSlotBegin identifica la carta, compresa la generazione, inserita nella sede (slot) del conducente all'inizio dell'anomalia.

cardNumberAndGenDriverSlotEnd identifica la carta, compresa la generazione, inserita nella sede (slot) del conducente al termine dell'anomalia.

cardNumberAndGenCodriverSlotBegin identifica la carta, compresa la generazione, inserita nella sede (slot) del secondo conducente all'inizio dell'anomalia.

cardNumberAndGenCodriverSlotEnd identifica la carta, compresa la generazione, inserita nella sede (slot) del secondo conducente al termine dell'anomalia.

similarEventsNumber è il numero di anomalie analoghe verificatesi nel giorno in questione.

2.241. **VuPowerSupplyInterruptionRecordArray**

Seconda generazione:

Informazioni, memorizzate in un'unità elettronica di bordo, relative alle interruzioni dell'alimentazione di energia (requisito 117 dell'allegato 1C).

```
VuPowerSupplyInterruptionRecordArray ::= SEQUENCE {
   recordType                           RecordType,
   recordSize                           INTEGER(1..65535),
   noOfRecords                          INTEGER(0..65535),
   records                              SET SIZE(noOfRecords) OF
                                        VuPowerSupplyInterruptionRecord
}
```

recordType rappresenta il tipo di registrazione (VuPowerSupplyInterruptionRecord). **Assegnazione valore**: Cfr. RecordType

recordSize sono le dimensioni di VuPowerSupplyInterruptionRecord in byte.

noOfRecords è il numero di registrazioni nella serie di registrazioni.

records è una serie di registrazioni di interruzioni dell'alimentazione di energia.

2.242. **VuSensorExternalGNSSCoupledRecordArray**

Seconda generazione:

Una serie di SensorExternalGNSSCoupledRecord più i metadati usati nel protocollo di trasferimento.

```
VuSensorExternalGNSSCoupledRecordArray ::= SEQUENCE {
   recordType                           RecordType,
   recordSize                           INTEGER(1..65535),
   noOfRecords                          INTEGER(0..65535),
   records                              SET SIZE(noOfRecords) OF
                                        SensorExternalGNSSCoupledRecord
}
```

recordType rappresenta il tipo di registrazione (SensorExternalGNSSCoupledRecord). **Assegnazione valore**: Cfr. RecordType

▼B

recordSize sono le dimensioni di SensorExternalGNSSCoupledRecord in byte.

noOfRecords è il numero di registrazioni nella serie di registrazioni.

records è una serie di registrazioni degli accoppiamenti del sensore del dispositivo GNSS esterno.

2.243. **VuSensorPairedRecordArray**

Seconda generazione:

Una serie di SensorPairedRecord più i metadati usati nel protocollo di trasferimento.

```
VuSensorPairedRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF SensorPairedRecord
}
```

recordType rappresenta il tipo di registrazione (SensorPairedRecord).
Assegnazione valore: Cfr. RecordType

recordSize sono le dimensioni di SensorPairedRecord in byte.

noOfRecords è il numero di registrazioni nella serie di registrazioni.

records è una serie di registrazioni di abbinamenti del sensore.

3. DEFINIZIONI DEI CAMPI DI VALORI E DIMENSIONI

Definizione dei valori delle variabili usati per le definizioni nel paragrafo 2.

```
TimeRealRange ::= 2^32-1
```

4. SET DI CARATTERI

Le stringhe IA5 utilizzano i caratteri ASCII definiti nella norma ISO/IEC 8824-1. A fini di migliore leggibilità e di semplice riferimento, si riporta di seguito l'assegnazione dei valori. In caso di discordanza, la norma ISO/IEC 8824-1 prevale sulla presente nota informativa.

```
  ! " # $ % & ' ( ) * + , - . / 0 1 2 3 4 5 6 7 8 9 : ; < = > ?
@ A B C D E F G H I J K L M N O P Q R S T U V W X Y Z [ \ ] ^ _
` a b c d e f g h i j k l m n o p q r s t u v w x y z { | } ~
```

Altre stringhe di caratteri (Address, Name, VehicleRegistrationNumber) utilizzano anche i caratteri definiti dai codici dei caratteri decimali 161 — 255 del seguente insieme standard di caratteri a 8 bit, specificati dal loro numero di pagina di codice: Insieme standard di caratteri	Pagina di codice (decimale)
ISO/IEC 8859-1 Latino-1 Europa occidentale	1
ISO/IEC 8859-2 Latino-2 Europa centrale	2
ISO/IEC 8859-3 Latino-3 Europa meridionale	3
ISO/IEC 8859-5 Latino/Cirillico	5
ISO/IEC 8859-7 Latino/Greco	7
ISO/IEC 8859-9 Latino-5 Turco	9

▼B

Altre stringhe di caratteri (Address, Name, VehicleRegistrationNumber) utilizzano anche i caratteri definiti dai codici dei caratteri decimali 161 — 255 del seguente insieme standard di caratteri a 8 bit, specificati dal loro numero di pagina di codice: Insieme standard di caratteri	Pagina di codice (decimale)
ISO/IEC 8859-13 Latino-7 Baltico	13
ISO/IEC 8859-15 Latino-9	15
ISO/IEC 8859-16 Latino-10 Europa sudorientale	16
KOI8-R Latino/Cirillico	80
KOI8-U Latino / Cirillico	85

5. CODIFICA

Se la codifica viene effettuata in base alle regole ASN.1, tutti i tipi di dati definiti devono essere codificati in conformità alla norma ISO/IEC 8825-2, variante allineata.

6. IDENTIFICATIVI DI OGGETTO E IDENTIFICATIVI DI APPLICAZIONE

6.1. **Identificativi di oggetto**

Gli identificativi di oggetto (OID) elencati nel presente capitolo sono pertinenti solo per la seconda generazione. Questi OID sono specificati nelle linee guida tecniche TR-03110-3 e ripetuti qui per ragioni di completezza. Questi OID sono contenuti nel sottoalbero di bsi-de:

```
bsi-de OBJECT IDENTIFIER ::= {
   itu-t(0) identified-organization(4) etsi(0)
   reserved(127) etsi-identified-organization(0) 7
}
```

Identificativi del protocollo di autenticazione della VU

```
id-TA          OBJECT IDENTIFIER ::= {bsi-de protocols(2) smartcard(2) 2}

id-TA-ECDSA                 OBJECT IDENTIFIER ::= {id-TA 2}

id-TA-ECDSA-SHA-256 OBJECT IDENTIFIER ::= {id-TA-ECDSA 3}

id-TA-ECDSA-SHA-384 OBJECT IDENTIFIER ::= {id-TA-ECDSA 4}

id-TA-ECDSA-SHA-512 OBJECT IDENTIFIER ::= {id-TA-ECDSA 5}
```

Esempio: Supponiamo che l'autenticazione della VU debba essere fatta con SHA-384; allora l'identificativo di oggetto da usare è (nella notazione ASN. 1) `bsi-de protocols(2) smartcard(2) 2 2 4`. Il valore di tale identificativo di oggetto nella dot notation (notazione col punto) è `0.4.0.127.0.7.2.2.2.2.4`.

	Dot notation	Byte notation
id-TA-ECDSA-SHA-256	0.4.0.127.0.7.2.2.2.2.3	‘04 00 7F 00 07 02 02 02 02 03’
id-TA-ECDSA-SHA-384	0.4.0.127.0.7.2.2.2.2.4	‘04 00 7F 00 07 02 02 02 02 04’
id-TA-ECDSA-SHA-512	0.4.0.127.0.7.2.2.2.2.5	‘04 00 7F 00 07 02 02 02 02 05’

▼B

Identificativi del protocollo di autenticazione del chip

```
id-CA         OBJECT IDENTIFIER ::= {bsi-de protocols(2) smartcard(2) 3}

id-CA-ECDH                        OBJECT IDENTIFIER ::= {id-CA 2}

id-CA-ECDH-AES-CBC-CMAC-128       OBJECT IDENTIFIER ::= {id-CA-ECDH 2}

id-CA-ECDH-AES-CBC-CMAC-192       OBJECT IDENTIFIER ::= {id-CA-ECDH 3}

id-CA-ECDH-AES-CBC-CMAC-256       OBJECT IDENTIFIER ::= {id-CA-ECDH 4}
```

Esempio: Supponiamo che l'autenticazione del chip debba essere effettuata utilizzando l'algoritmo ECDH, che dà come risultato una lunghezza della chiave di sessione AES di 128 bit. Tale chiave di sessione sarà successivamente utilizzata nel modo operativo CBC per garantire la riservatezza dei dati e con l'algoritmo CMAC per assicurare l'autenticità dei dati. Di conseguenza, l'identificativo di oggetto da usare è (nella notazione ASN. 1) `bsi-de protocols(2) smartcard(2) 3 2 2`. Il valore di tale identificativo di oggetto nella dot notation (notazione col punto) è `0.4.0.127.0.7.2.2.3.2.2`.

	Dot notation	Byte notation
id-CA-ECDH-AES-CBC-CMAC-128	0.4.0.127.0.7.2.2.3.2.2	‘04 00 7F 00 07 02 02 03 02 02’
id-CA-ECDH-AES-CBC-CMAC-192	0.4.0.127.0.7.2.2.3.2.3	‘04 00 7F 00 07 02 02 03 02 03’
id-CA-ECDH-AES-CBC-CMAC-256	0.4.0.127.0.7.2.2.3.2.4	‘04 00 7F 00 07 02 02 03 02 04’

6.2. **Identificativi di applicazione**

Seconda generazione:

L'identificativo di applicazione (AID) per il dispositivo GNSS esterno (di seconda generazione) è dato da ‘FF 44 54 45 47 4D’. Si tratta di un AID proprietario secondo la norma ISO/IEC 7816-4.

Nota: gli ultimi 5 byte codificano DTEGM per il dispositivo GNSS esterno del tachigrafo intelligente.

L'identificativo di applicazione per l'applicazione della carta tachigrafica di seconda generazione è dato da ‘FF 53 4D 52 44 54’. Si tratta di un AID proprietario secondo la norma ISO/IEC 7816-4.

▼B

Appendice 2

SPECIFICHE RIGUARDANTI LE CARTE TACHIGRAFICHE

INDICE

1. INTRODUZIONE

1.1. Abbreviazioni

1.2. Riferimenti

2. CARATTERISTICHE ELETTRICHE E FISICHE

2.1. Tensione di alimentazione e assorbimento di corrente

2.2. Tensione di programmazione V_{pp}

2.3. Generazione e frequenza dell'orologio

2.4. Contatto I/O (ingresso/uscita)

2.5. Condizioni di funzionamento della carta

3. HARDWARE E COMUNICAZIONE

3.1. Introduzione

3.2. Protocollo di trasmissione

3.2.1 Protocolli

3.2.2 ATR

3.2.3 PTS

3.3. Regole di accesso

3.4. Panoramica dei comandi e dei codici di errore

3.5. Descrizione dei comandi

3.5.1 SELECT

3.5.2 READ BINARY

3.5.3 UPDATE BINARY

3.5.4 GET CHALLENGE

3.5.5 VERIFY

3.5.6 GET RESPONSE

3.5.7 PSO: VERIFY CERTIFICATE

3.5.8 INTERNAL AUTHENTICATE

3.5.9 EXTERNAL AUTHENTICATE

3.5.10 GENERAL AUTHENTICATE

3.5.11 MANAGE SECURITY ENVIRONMENT

3.5.12 PSO: HASH

▼B

3.5.13 PERFORM HASH of FILE

3.5.14 PSO: COMPUTE DIGITAL SIGNATURE

3.5.15 PSO: VERIFY DIGITAL SIGNATURE

3.5.16 PROCESS DSRC MESSAGE

4. STRUTTURA DELLE CARTE TACHIGRAFICHE

4.1. Master file MF

4.2. Applicazioni della carta del conducente

4.2.1 Applicazione della carta del conducente di prima generazione

4.2.2 Applicazione della carta del conducente di seconda generazione

4.3. Applicazioni della carta dell'officina

4.3.1 Applicazione della carta dell'officina di prima generazione

4.3.2 Applicazione della carta dell'officina di seconda generazione

4.4. Applicazioni della carta di controllo

4.4.1 Applicazione della carta di controllo di prima generazione

4.4.2 Applicazione della carta di controllo di seconda generazione

4.5. Applicazioni della carta dell'azienda

4.5.1 Applicazione della carta dell'azienda di prima generazione

4.5.2 Applicazione della carta dell'azienda di seconda generazione

1. INTRODUZIONE

1.1. **Abbreviazioni**

Ai fini della presente appendice, si applicano le seguenti abbreviazioni.

AC	Criteri di accesso
AES	Norma di cifratura avanzata (Advanced Encryption Standard)
AID	Identificativo dell'applicazione (Application Identifier)
ALW	Sempre
APDU	Unità dati del protocollo di applicazione (struttura di un comando)
ATR	Risposta al reset
AUT	Autenticato
C6, C7	Contatti nn. 6 e 7 della carta, secondo la definizione ISO/IEC 7816-2
cc	Cicli dell'orologio
CHV	Informazioni di verifica del titolare della carta
CLA	Byte di classe di un comando APDU

▼B

DSRC	Comunicazione dedicata a corto raggio
DF	File dedicato. Un DF può contenere altri file (EF o DF)
ECC	Crittografia a curve ellittiche
EF	File elementare
etu	Unità di tempo elementare
G1	Prima generazione
G2	Seconda generazione
IC	Circuito integrato
ICC	Carta a circuito integrato (Integrated Circuit Card)
ID	Identificativo
IFD	Dispositivo di interfaccia (Interface Device)
IFS	Dimensioni del campo informazioni
IFSC	Dimensioni del campo informazioni per la carta
IFSD	Dimensioni del campo informazioni per il dispositivo (per il terminale)
INS	Byte di istruzioni di un comando APDU
Lc	Lunghezza dei dati in ingresso per un comando APDU
Le	Lunghezza dei dati attesi (dati in uscita per un comando)
MF	File principale (root DF)
NAD	Indirizzo di nodo usato nel protocollo T=1
NEV	Mai
P1-P2	Byte dei parametri
PIN	Numero di identificazione personale
PRO SM	Protezione con messaggistica sicura
PTS	Selezione della trasmissione del protocollo
RFU	Riservato per uso futuro
RST	Reset (della carta)
SFID	Identificativo breve dell'EF
SM	Messaggistica sicura (Secure Messaging)
SW1-SW2	Byte di stato
TS	Carattere ATR iniziale
VPP	Tensione di programmazione
VU	Unità elettronica di bordo
XXh	Valore XX in notazione esadecimale
‘XXh’	Valore XX in notazione esadecimale
||	Simbolo di concatenamento 03||04=0304

▼B

1.2. **Riferimenti**

Nella presente appendice si rimanda alle seguenti norme:

ISO/IEC 7816-2 Carte di identificazione — Carte a circuiti integrati — Parte 2: Dimensioni e posizione dei contatti. ISO/IEC 7816-2:2007.

ISO/IEC 7816-3 Carte di identificazione — Carte a circuiti integrati — Parte 3: Interfaccia elettrica e protocolli di trasmissione. ISO/IEC 7816-3:2006.

ISO/IEC 7816-4 Carte di identificazione — Carte a circuiti integrati — Parte 4: Organizzazione, sicurezza e comandi di interscambio. ISO/IEC 7816-4:2013 + Cor 1: 2014.

ISO/IEC 7816-6 Carte di identificazione — Carte a circuiti integrati — Parte 6: Elementi di dati per lo scambio intrasettoriale. ISO/IEC 7816-6:2004 + Cor 1: 2006.

ISO/IEC 7816-8 Carte di identificazione — Carte a circuiti integrati — Parte 8: Comandi per le operazioni di sicurezza. ISO/IEC 7816-8:2004.

ISO/IEC 9797-2 Tecnologia dell'informazione — Tecniche di sicurezza — Codici di autenticazione del messaggio (MAC) — Parte 2: Meccanismi che usano una funzione di hash dedicata. ISO/IEC 9797-2:2011

2. CARATTERISTICHE ELETTRICHE E FISICHE

TCS_01 Se non diversamente specificato, tutti i segnali elettronici devono essere conformi alla norma ISO/IEC 7816-3.

TCS_02 La posizione e le dimensioni dei contatti della carta devono essere conformi alla norma ISO/IEC 7816-2.

2.1. **Tensione di alimentazione e assorbimento di corrente**

TCS_03 La carta deve funzionare in conformità alle specifiche, entro i limiti di assorbimento previsti nella norma ISO/IEC 7816-3.

TCS_04 La carta deve funzionare a Vcc = 3V (± 0,3V) o a Vcc = 5V (± 0,5V).

La tensione deve essere selezionata in conformità alla norma ISO/IEC 7816-3.

2.2. **Tensione di programmazione V_{pp}**

TCS_05 La carta non deve richiedere una tensione di programmazione sul pin C6. Si prevede che il pin C6 non sia collegato in un IFD. Il contatto C6 può essere collegato alla V_{cc} nella carta, ma non va collegato a massa. Non sono ammesse altre interpretazioni della tensione di programmazione.

2.3. **Generazione e frequenza dell'orologio**

TCS_06 La carta deve funzionare entro un campo di frequenze tra 1 e 5 MHz e può operare anche a frequenze più elevate. In una sessione della carta, la frequenza dell'orologio può variare di ± 2 %. La frequenza dell'orologio è generata dall'unità elettronica di bordo e non dalla carta. Il fattore di utilizzo può variare tra il 40 e il 60 %.

TCS_07 Nelle condizioni specificate nel file EF ICC della carta, l'orologio esterno può essere arrestato. Il primo byte del file EF ICC codifica le condizioni della modalità «Clock-stop»:

▼B

Basso	Alto		
Bit 3	Bit 2	Bit 1	
0	0	1	Clockstop ammesso, nessun livello preferito
0	1	1	Clockstop ammesso, livello alto preferito
1	0	1	Clockstop ammesso, livello basso preferito
0	0	0	Clockstop non ammesso
0	1	0	Clockstop ammesso solo al livello alto
1	0	0	Clockstop ammesso solo al livello basso

I bit da 4 a 8 non sono utilizzati.

2.4. **Contatto I/O (ingresso/uscita)**

TCS_08 Il contatto I/O C7 è utilizzato per ricevere e trasmettere dati da e verso l'IFD. Durante il funzionamento, la modalità di trasmissione deve essere attiva solo nella carta o solo nell'IFD. Se la modalità di trasmissione è attiva in entrambi i dispositivi, la carta non deve essere danneggiata. A condizione che non sia in fase di trasmissione, la carta deve passare alla modalità di ricezione.

2.5. **Condizioni di funzionamento della carta**

TCS_09 Con la tensione di alimentazione inserita, la carta prevede due condizioni di funzionamento:

condizione di funzionamento durante l'esecuzione di comandi o l'interfacciamento con l'unità digitale,

condizione di riposo in tutti gli altri casi; in questa condizione, la carta deve conservare tutti i dati.

3. HARDWARE E COMUNICAZIONE

3.1. **Introduzione**

Il presente paragrafo descrive la funzionalità minima richiesta per le carte tachigrafiche e le VU al fine di garantirne il corretto funzionamento e l'interoperabilità.

Le carte tachigrafiche devono essere il più possibile conformi alle norme ISO/IEC applicabili in vigore (in particolare ISO/IEC 7816). Si fornisce comunque una descrizione completa dei comandi e dei protocolli al fine di specificare alcune limitazioni d'uso o le differenze eventualmente esistenti. Se non diversamente indicato, i comandi specificati sono pienamente conformi alle norme citate.

3.2. **Protocollo di trasmissione**

TCS_10 Il protocollo di trasmissione deve essere conforme alla norma ISO/IEC 7816-3 per T = 0 e T = 1. In particolare, la VU deve riconoscere le proroghe del tempo di attesa inviate dalla carta.

3.2.1 *Protocolli*

TCS_11 La carta deve prevedere sia il protocollo **T=0** sia il protocollo **T=1**. La carta può inoltre supportare ulteriori protocolli orientati al contatto.

TCS_12 **T=0** è il protocollo predefinito ed è quindi necessario un comando **PTS** per passare al protocollo **T=1**.

▼B

TCS_13 I dispositivi devono prevedere l'impiego della **convenzione diretta** in entrambi i protocolli: la convenzione diretta è quindi obbligatoria per la carta.

TCS_14 Il byte di **dimensione del campo di informazioni per la carta** deve essere presentato all'ATR nel carattere TA3. Questo valore deve essere almeno pari a 'F0h' (= 240 byte).

Ai protocolli si applicano le restrizioni seguenti.

TCS_15 **T=0**

— L'interfaccia deve prevedere una risposta all'I/O dopo il fronte di salita del segnale all'RST da 400 cc.

— L'interfaccia deve essere in grado di leggere caratteri separati da 12 etu.

— L'interfaccia deve leggere un carattere errato e la sua ripetizione se separati da 13 etu. Se viene rilevato un carattere errato, il segnale di errore all'I/O può verificarsi tra 1 e 2 etu. Il dispositivo deve prevedere un ritardo di 1 etu.

— L'interfaccia deve accettare un'ATR da 33 byte (TS+32).

— In presenza di TC1 nell'ATR, deve essere previsto un Extra Guard Time (tempo di protezione supplementare) per i caratteri inviati dall'interfaccia, anche se i caratteri inviati dalla carta possono comunque essere separati da 12 etu. Questo vale anche per il carattere ACK inviato dalla carta dopo un carattere P3 emesso dall'interfaccia.

— L'interfaccia deve tener conto di un carattere NUL (nullo) emesso dalla carta.

— L'interfaccia deve accettare la modalità complementare per ACK.

— Il comando GET RESPONSE non può essere usato nella modalità di concatenamento per ottenere dati la cui lunghezza può superare 255 byte.

TCS_16 **T=1**

— Byte NAD: non utilizzato (il byte NAD deve essere impostato a '00').

— S-block ABORT: non utilizzato.

— S-block VPP state error: non utilizzato.

— La lunghezza totale di concatenamento per un campo di dati non deve essere superiore a 255 byte (accertato dall'IFD).

— La dimensione del campo di informazioni per il dispositivo (IFSD) deve essere indicata dall'IFD immediatamente dopo l'ATR: l'IFD deve trasmettere la richiesta dell'S-Block IFS dopo l'ATR e la carta deve rispondere con l'S-Block IFS. Il valore consigliato per l'IFSD è 254 byte.

— La carta non chiede un riadeguamento dell'IFS.

▼B

3.2.2 *ATR*

TCS_17 Il dispositivo controlla i byte ATR, secondo la norma ISO/IEC 7816-3. Non si devono effettuare verifiche dei caratteri storici dell'ATR.

Esempio di biprotocollo ATR di base secondo la norma ISO/IEC 7816-3

Carattere	Valore	Osservazioni
TS	'3Bh'	Indica la convenzione diretta
T0	'85h'	TD1 presente; sono presenti 5 byte storici
TD1	'80h'	TD2 presente; si deve usare T = 0
TD2	'11h'	TA3 presente; si deve usare T = 1
TA3	'XXh' (almeno 'F0h')	Dimensione del campo di informazioni per la carta (IFSC)
da TH1 a TH5	'XXh'	Caratteri storici
TCK	'XXh'	Carattere di controllo (OR esclusivo)

TCS_18 In seguito alla risposta al reset (ATR), il file principale (MF) è implicitamente selezionato e diventa la directory attiva.

3.2.3 *PTS*

TCS_19 Il protocollo predefinito è T=0. Per impostare il protocollo T=1, il dispositivo deve inviare un PTS (anche noto come PPS) alla carta.

TCS_20 Poiché entrambi i protocolli T=0 e T=1 sono obbligatori per la carta, anche il PTS di base per il cambio di protocollo è obbligatorio per la carta.

Come indicato nella norma ISO/IEC 7816-3, il PTS si può utilizzare per passare a velocità di dati più elevate rispetto a quella predefinita, proposta dalla carta nell'ATR, se presente (TA(1) byte).

Velocità di dati più elevate per la carta sono facoltative.

TCS_21 Se non sono previste velocità di dati diverse da quella predefinita (o se non è prevista la velocità di dati selezionata), la carta deve rispondere correttamente al PTS, secondo la norma ISO/IEC 7816-3, omettendo il byte PPS1.

Si riportano di seguito alcuni esempi di PTS di base per la selezione del protocollo.

Carattere	Valore	Osservazioni
PPSS	'FFh'	Il carattere iniziale
PPS0	'00h' o '01h'	I caratteri da PPS1 a PPS3 non sono presenti; '00h' per selezionare T0, '01h' per selezionare T1.
PK	'XXh'	Carattere di controllo: 'XXh' = 'FFh' se PPS0 = '00h', 'XXh' = 'FEh' se PPS0 = '01h'.

▼B

3.3. **Regole di accesso**

TCS_22 Una regola di accesso specifica per una modalità di accesso, vale a dire un comando, le condizioni di sicurezza corrispondenti. Se queste condizioni di sicurezza sono soddisfatte, il comando corrispondente è elaborato.

TCS_23 Le seguenti condizioni di sicurezza sono usate per la carta tachigrafica:

Abbreviazione	Significato
ALW	L'azione è sempre possibile e può essere eseguita senza limitazioni. Il comando e la risposta APDU sono inviati in testo semplice, vale a dire senza messaggistica sicura.
NEV	L'azione non è mai possibile.
PLAIN-C	Il comando APDU è inviato in testo semplice, vale a dire senza messaggistica sicura.
PWD	L'azione può essere eseguita solo se il PIN della carta dell'officina è stato correttamente verificato, vale a dire se la condizione di sicurezza interna della carta «PIN_Verified» è impostata. Il comando deve essere inviato senza messaggistica sicura.
EXT-AUT-G1	L'azione può essere eseguita solo se il comando External Authenticate per l'autenticazione di prima generazione (cfr. anche appendice 11, parte A) è stato eseguito correttamente.
SM-MAC-G1	L'APDU (comando e risposta) deve essere applicata con messaggistica sicura di prima generazione in modalità di sola autenticazione (cfr. appendice 11, parte A).
SM-C-MAC-G1	Il comando APDU deve essere applicato con messaggistica sicura di prima generazione in modalità di sola autenticazione (cfr. appendice 11, parte A).
SM-R-ENC-G1	La risposta APDU deve essere applicata con messaggistica sicura di prima generazione in modalità cifratura (cfr. appendice 11, parte A), vale a dire senza che sia inviato in risposta un codice di autenticazione del messaggio.
SM-R-ENC-MAC-G1	La risposta APDU deve essere applicata con messaggistica sicura di prima generazione in modalità cifratura seguita da autenticazione (cfr. appendice 11, parte A).
SM-MAC-G2	L'APDU (comando e risposta) deve essere applicata con messaggistica sicura di seconda generazione in modalità di sola autenticazione (cfr. appendice 11, parte B).
SM-C-MAC-G2	Il comando APDU deve essere applicato con messaggistica sicura di seconda generazione in modalità di sola autenticazione (cfr. appendice 11, parte B).
SM-R-ENC-MAC-G2	La risposta APDU deve essere applicata con messaggistica sicura di seconda generazione in modalità cifratura seguita da autenticazione (cfr. appendice 11, parte B).

TCS_24 Queste condizioni di sicurezza possono essere collegate nei seguenti modi:

AND **(E)**: devono essere soddisfatte tutte le condizioni di sicurezza

OR **(O)**: deve essere soddisfatta almeno una condizione di sicurezza

Le norme di accesso per il file system, vale a dire per i comandi SELECT, UPDATE BINARY e READ BINARY, sono specificate nel capitolo 4. Le norme di accesso per gli altri comandi sono specificate nelle seguenti tabelle.

▼B

TCS_25 Nell'applicazione DF Tachograph G1 sono utilizzate le seguenti norme di accesso:

Comando	Carta del conducente	Carta dell'officina	Carta di controllo	Carta dell'azienda
External Authenticate				
— Per l'autenticazione di prima generazione	ALW	ALW	ALW	ALW
— Per l'autenticazione di seconda generazione	ALW	PWD	ALW	ALW
Internal Authenticate	ALW	PWD	ALW	ALW
General Authenticate	ALW	ALW	ALW	ALW
Get Challenge	ALW	ALW	ALW	ALW
MSE:SET AT	ALW	ALW	ALW	ALW
MSE:SET DST	ALW	ALW	ALW	ALW
Process DSRC Message	Non applicabile	Non applicabile	Non applicabile	Non applicabile
PSO: Compute Digital Signature	ALW OR SM-MAC-G2	ALW OR SM-MAC-G2	Non applicabile	Non applicabile
PSO: Hash	Non applicabile	Non applicabile	ALW	Non applicabile
PSO: Hash of File	ALW OR SM-MAC-G2	ALW OR SM-MAC-G2	Non applicabile	Non applicabile
PSO: Verify Certificate	ALW	ALW	ALW	ALW
PSO: Verify Digital Signature	Non applicabile	Non applicabile	ALW	Non applicabile
Verify	Non applicabile	ALW	Non applicabile	Non applicabile

TCS_26 Nell'applicazione DF Tachograph_G2 sono utilizzate le seguenti norme di accesso:

Comando	Carta del conducente	Carta dell'officina	Carta di controllo	Carta dell'azienda
External Authenticate				
— Per l'autenticazione di prima generazione	Non applicabile	Non applicabile	Non applicabile	Non applicabile
— Per l'autenticazione di seconda generazione	ALW	PWD	ALW	ALW
Internal Authenticate	Non applicabile	Non applicabile	Non applicabile	Non applicabile

▼B

Comando	Carta del conducente	Carta dell'officina	Carta di controllo	Carta dell'azienda
General Authenticate	ALW	ALW	ALW	ALW
Get Challenge	ALW	ALW	ALW	ALW
MSE:SET AT	ALW	ALW	ALW	ALW
MSE:SET DST	ALW	ALW	ALW	ALW
Process DSRC Message	Non applicabile	ALW	ALW	Non applicabile
PSO: Compute Digital Signature	ALW OR SM-MAC-G2	ALW OR SM-MAC-G2	Non applicabile	Non applicabile
PSO: Hash	Non applicabile	Non applicabile	ALW	Non applicabile
PSO: Hash of File	ALW OR SM-MAC-G2	ALW OR SM-MAC-G2	Non applicabile	Non applicabile
PSO: Verify Certificate	ALW	ALW	ALW	ALW
PSO: Verify Digital Signature	Non applicabile	Non applicabile	ALW	Non applicabile
Verify	Non applicabile	ALW	Non applicabile	Non applicabile

TCS_27 Nell'MF sono utilizzate le seguenti norme di accesso:

Comando	Carta del conducente	Carta dell'officina	Carta di controllo	Carta dell'azienda
External Authenticate				
— Per l'autenticazione di prima generazione	Non applicabile	Non applicabile	Non applicabile	Non applicabile
— Per l'autenticazione di seconda generazione	ALW	PWD	ALW	ALW
Internal Authenticate	Non applicabile	Non applicabile	Non applicabile	Non applicabile
General Authenticate	ALW	ALW	ALW	ALW
Get Challenge	ALW	ALW	ALW	ALW
MSE:SET AT	ALW	ALW	ALW	ALW
MSE:SET DST	ALW	ALW	ALW	ALW
Process DSRC Message	Non applicabile	Non applicabile	Non applicabile	Non applicabile

▼B

Comando	Carta del conducente	Carta dell'officina	Carta di controllo	Carta dell'azienda
PSO: Compute Digital Signature	Non applicabile	Non applicabile	Non applicabile	Non applicabile
PSO: Hash	Non applicabile	Non applicabile	Non applicabile	Non applicabile
PSO: Hash of File	Non applicabile	Non applicabile	Non applicabile	Non applicabile
PSO: Verify Certificate	ALW	ALW	ALW	ALW
Verify	Non applicabile	ALW	Non applicabile	Non applicabile

TCS_28 Una carta tachigrafica può accettare o meno un comando con un livello di sicurezza più elevato rispetto a quello specificato nelle condizioni di sicurezza. Ciò significa che se la condizione di sicurezza è ALW (o PLAIN-C) la carta può accettare un comando con messaggistica sicura (modalità cifratura e/o autenticazione). Se la condizione di sicurezza richiede la messaggistica sicura con modalità di autenticazione, la carta tachigrafica può accettare un comando con messaggistica sicura della stessa generazione in modalità autenticazione e cifratura.

Nota: le descrizioni del comando forniscono maggiori informazioni sul supporto dei comandi per i diversi tipi di carte tachigrafiche e i diversi DF.

3.4. **Panoramica dei comandi e dei codici di errore**

I comandi e l'organizzazione dei file si desumono dalla norma ISO/IEC 7816-4, cui sono conformi.

La presente sezione descrive le seguenti coppie comando-risposta APDU. Le varianti di comandi che sono supportate da un'applicazione di prima e di seconda generazione sono specificate nelle descrizioni dei comandi corrispondenti.

Comando	INS
SELECT	‘A4h’
READ BINARY	‘B0h’, ‘B1h’
UPDATE BINARY	‘D6h’, ‘D7h’
GET CHALLENGE	‘84h’
VERIFY	‘20h’
GET RESPONSE	‘C0h’
PERFORM SECURITY OPERATION	‘2Ah’

▼B

Comando	INS
— VERIFY CERTIFICATE	
— COMPUTE DIGITAL SIGNATURE	
— VERIFY DIGITAL SIGNATURE	
— HASH	
— PERFORM HASH OF FILE	
— PROCESS DSRC MESSAGE	
INTERNAL AUTHENTICATE	‘88h’
EXTERNAL AUTHENTICATE	‘82h’
MANAGE SECURITY ENVIRONMENT	‘22h’
— SET DIGITAL SIGNATURE TEMPLATE	
— SET AUTHENTICATION TEMPLATE	
GENERAL AUTHENTICATE	‘86h’

TCS_29 Le parole di stato SW1 SW2 sono inviate in ogni messaggio di risposta ed indicano lo stato di elaborazione del comando.

SW1	SW2	Significato
90	00	Elaborazione normale
61	XX	Elaborazione normale XX = numero di byte di risposta disponibili
62	81	Elaborazione con avvertimento. Parte dei dati inviati in risposta potrebbero essere danneggiati
63	00	Autenticazione fallita (avvertimento)
63	CX	CHV (PIN) errato. Contatore tentativi rimasti fornito da ‘X’
64	00	Errore di esecuzione — Stato della memoria non volatile immutato. Errore di integrità
65	00	Errore di esecuzione — Stato della memoria non volatile mutato
65	81	Errore di esecuzione — Stato della memoria non volatile mutato — Errore di memoria
66	88	Errore di sicurezza: totale di controllo crittografico errato (durante messaggistica sicura) o certificato errato (durante verifica certificato) o crittogramma errato (durante autenticazione esterna) o firma errata (durante verifica firma)
67	00	Lunghezza errata (Lc o Le errata)

▼B

SW1	SW2	Significato
68	82	Messaggistica sicura non supportata
68	83	Ultimo comando della catena atteso
69	00	Comando vietato (risposta non disponibile in T = 0)
69	82	Condizione di sicurezza non soddisfatta
69	83	Metodo di autenticazione bloccato
69	85	Condizioni di impiego non soddisfatte
69	86	Comando non consentito (nessun EF corrente)
69	87	Oggetti di dati previsti in messaggistica sicura mancanti
69	88	Oggetti di dati in messaggistica sicura non corretti
6A	80	Parametri errati nel campo di dati
6A	82	File non trovato
6A	86	Parametri P1-P2 errati
6A	88	Dati indicati non trovati
6B	00	Parametri errati (scostamento al di fuori dell'EF)
6C	XX	Lunghezza errata, SW2 indica la lunghezza esatta. Non viene inviato alcun campo di dati in risposta
6D	00	Codice di istruzione non previsto o non valido
6E	00	Classe non prevista
6F	00	Altri errori di controllo

TCS_30 Se in un comando APDU è soddisfatta più di una condizione di errore, la carta può inviare in risposta una qualsiasi delle parole di stato appropriate.

3.5. Descrizione dei comandi

Nel presente capitolo sono descritti i comandi obbligatori per le carte tachigrafiche.

Altri particolari di rilievo, riguardanti le operazioni crittografiche, sono forniti nell'appendice 11 (Meccanismi comuni di sicurezza per i tachigrafi di prima e seconda generazione).

Tutti i comandi sono descritti a prescindere dal protocollo utilizzato (T=0 o T=1). I byte APDU CLA, INS, P1, P2, Lc e Le sono sempre indicati. Se i byte Lc o Le non sono necessari per il comando descritto, la lunghezza, il valore e la descrizione ad essi associati sono vuoti.

TCS_31 Se entrambi i byte di lunghezza (Lc e Le) sono necessari, e se l'IFD utilizza il protocollo T=0, il comando descritto dev'essere suddiviso in due parti: l'IFD invia il comando secondo quanto descritto con P3=Lc + dati e quindi invia un comando GET RESPONSE (cfr. paragrafo 3.5.6) con P3=Le.

TCS_32 Se sono necessari entrambi i byte di lunghezza e Le=0 (messaggistica sicura):

▼B

— se si usa il protocollo T=1, la carta deve rispondere a Le=0 inviando tutti i dati in uscita disponibili;

— se si usa il protocollo T=0, l'IFD deve inviare il primo comando con P3=Lc + dati e la carta deve rispondere (a questo implicito Le=0) con i byte di stato '**61La**', dove La è il numero di byte di risposta disponibili. L'IFD deve generare quindi un comando GET RESPONSE con P3=La per leggere i dati.

TCS_33 Una carta tachigrafica può supportare campi di lunghezza estesa conformemente alla norma ISO/IEC 7816-4 quale caratteristica opzionale. Una carta tachigrafica che supporta campi di lunghezza estesa:

— deve indicare che supporta i campi di lunghezza estesa nell'ATR;

— deve fornire la dimensione del buffer supportato tramite le informazioni di lunghezza estesa nell'ATR/INFO dell'EF, cfr. TCS_146;

— deve indicare se supporta campi di lunghezza estesa per T = 1 e/o T = 0 nella lunghezza estesa dell'EF, cfr. TCS_147;

— deve supportare campi di lunghezza estesa per l'applicazione tachigrafica di prima e seconda generazione.

Note:

tutti i comandi sono specificati per campi di lunghezza breve. L'uso di APDU di lunghezza estesa è specificato nella norma ISO/IEC 7816-4.

In generale i comandi sono specificati per la modalità in chiaro, vale a dire senza messaggistica sicura, poiché il livello della messaggistica sicura è specificato nell'appendice 11. È chiaro dalle norme di accesso di un comando se questo supporta la messaggistica sicura oppure no e se supporta la messaggistica sicura di prima e/o di seconda generazione. Alcune varianti di comandi sono descritte con messaggistica sicura per illustrarne l'uso.

TCS_34 La VU deve eseguire il protocollo completo di autenticazione reciproca tra la VU di seconda generazione e la carta per una sessione, compresa la verifica del certificato (se richiesta), in DF Tachograph, DF Tachograph_G2 o nell'MF.

3.5.1 *SELECT*

Questo comando è conforme alla norma ISO/IEC 7816-4, ma ha un impiego limitato rispetto al comando definito nella norma.

Il comando SELECT si usa per:

— selezionare un DF di applicazione (si deve usare la selezione per nome)

— selezionare un file elementare corrispondente all'ID del file indicato

3.5.1.1 Selezione in base al nome (AID)

Questo comando consente di selezionare un DF di applicazione nella carta.

TCS_35 Il comando può essere eseguito da qualsiasi punto della struttura del file (dopo l'ATR o in qualsiasi momento).

▼B

TCS_36 La selezione di un'applicazione azzera l'ambiente di sicurezza attivo. Dopo la selezione dell'applicazione non è più selezionata nessuna chiave pubblica corrente. Si perde anche la condizione di accesso EXT-AUT-G1. Se il comando è stato eseguito senza messaggistica sicura, le chiavi della precedente sessione di messaggistica sicura non sono più disponibili.

TCS_37 **Messaggio di comando**

Byte	Lunghezza	Valore	Descrizione
CLA	1	‘00h’	
INS	1	‘A4h’	
P1	1	‘04h’	Selezione in base al nome (AID)
P2	1	‘0Ch’	Nessuna risposta attesa
Lc	1	‘NNh’	Numero di byte inviati alla carta (lunghezza dell'AID): ‘06h’ per l'applicazione tachigrafica
#6-#(5 + NN)	NN	‘XX..XXh’	AID: ‘FF 54 41 43 48 4F’ per l'applicazione tachigrafica di prima generazione AID: ‘FF 53 4D 52 44 54’ per l'applicazione tachigrafica di seconda generazione

Non è necessaria una risposta al comando SELECT (Le assente in T=1 o nessuna risposta richiesta in T=0).

TCS_38 **Messaggio di risposta (nessuna risposta richiesta)**

Byte	Lunghezza	Valore	Descrizione
SW	2	‘XXXXh’	Parole di stato (SW1, SW2)

— Se il comando ha esito positivo, la carta risponde ‘**9000**’.

— Se l'applicazione corrispondente all'AID non viene trovata, lo stato di elaborazione inviato in risposta è ‘**6A82**’.

— In T=1, se il byte Le è presente, lo stato inviato in risposta è ‘**6700**’.

— In T=0, se è richiesta una risposta dopo il comando SELECT, lo stato inviato in risposta è ‘**6900**’.

— Se l'applicazione selezionata è considerata danneggiata (negli attributi del file è rilevato un errore di integrità), lo stato di elaborazione inviato in risposta è ‘**6400**’ o ‘**6581**’.

3.5.1.2 Selezione di un file elementare utilizzando il suo identificativo

TCS_39 **Messaggio di comando**

TCS_40 Una carta tachigrafica deve supportare la messaggistica sicura di seconda generazione, come specificato nell'appendice 11, parte B, per questa variante di comando.

Byte	Lunghezza	Valore	Descrizione
CLA	1	‘00h’	
INS	1	‘A4h’	
P1	1	‘02h’	Selezione di un EF sotto il DF corrente

▼B

Byte	Lun-ghezza	Valore	Descrizione
P2	1	‘0Ch’	Nessuna risposta attesa
Lc	1	‘02h’	Numero di byte inviati alla carta
#6-#7	2	‘XXXXh’	Identificativo del file

Non è necessaria una risposta al comando SELECT (Le assente in T=1 o nessuna risposta richiesta in T=0).

TCS_41 **Messaggio di risposta (nessuna risposta richiesta)**

Byte	Lun-ghezza	Valore	Descrizione
SW	2	‘XXXXh’	Parole di stato (SW1, SW2)

— Se il comando ha esito positivo, la carta risponde ‘**9000**’.

— Se il file corrispondente all'identificativo del file non viene trovato, lo stato di elaborazione inviato in risposta è ‘**6A82**’.

— In T=1, se il byte Le è presente, lo stato inviato in risposta è ‘**6700**’.

— In T=0, se è richiesta una risposta dopo il comando SELECT, lo stato inviato in risposta è ‘**6900**’.

— Se il file selezionato è considerato danneggiato (negli attributi del file è rilevato un errore di integrità), lo stato di elaborazione inviato in risposta è ‘**6400**’ o ‘**6581**’.

3.5.2 *READ BINARY*

Questo comando è conforme alla norma ISO/IEC 7816-4, ma ha un impiego limitato rispetto al comando definito nella norma.

Il comando READ BINARY è usato per leggere i dati di un file trasparente.

La risposta della carta consiste nell'invio dei dati letti, eventualmente incapsulati in una struttura di messaggistica sicura.

3.5.2.1 Comando con scostamento in P1-P2

Questo comando consente all'IFD di leggere i dati dell'EF selezionato, senza messaggistica sicura.

Nota: questo comando senza messaggistica sicura si può usare solo per leggere un file che supporta la condizione di sicurezza ALW per la modalità Read Access.

TCS_42 **Messaggio di comando**

Byte	Lun-ghezza	Valore	Descrizione
CLA	1	‘00h’	
INS	1	‘B0h’	Read Binary
P1	1	‘XXh’	Scostamento in byte dall'inizio del file: byte più significativo

▼B

Byte	Lunghezza	Valore	Descrizione
P2	1	‘XXh’	Scostamento in byte dall'inizio del file: byte meno significativo
Le	1	‘XXh’	Lunghezza dei dati attesi. Numero di byte da leggere

Nota: il bit 8 di P1 dev'essere impostato a 0.

TCS_43 **Messaggio di risposta**

Byte	Lunghezza	Valore	Descrizione
#1-#X	X	‘XX..XXh’	Dati letti
SW	2	‘XXXXh’	Parole di stato (SW1, SW2)

— Se il comando ha esito positivo, la carta risponde ‘**9000**’.

— Se non è selezionato un EF, lo stato di elaborazione inviato in risposta è ‘**6986**’.

— Se le condizioni di sicurezza del file selezionato non sono soddisfatte, il comando viene interrotto con ‘**6982**’.

— Se lo scostamento non è compatibile con la dimensione dell'EF (scostamento > dimensione EF), lo stato di elaborazione inviato in risposta è ‘**6B00**’.

— Se la dimensione dei dati da leggere non è compatibile con la dimensione dell'EF (scostamento + Le > dimensione EF), lo stato di elaborazione inviato in risposta è ‘**6700**’ o ‘**6Cxx**’, dove ‘xx’ indica la lunghezza esatta.

— Se negli attributi del file è rilevato un errore di integrità, la carta deve considerare tale file danneggiato e irrecuperabile; lo stato di elaborazione inviato in risposta è ‘**6400**’ o ‘**6581**’.

— Se nei dati memorizzati è rilevato un errore di integrità, la carta deve fornire i dati richiesti e inviare in risposta lo stato di elaborazione ‘**6281**’.

3.5.2.1.1 Comando con messaggistica sicura (esempi)

Questo comando consente all'IFD di leggere i dati dall'EF selezionato con messaggistica sicura, al fine di verificare l'integrità dei dati ricevuti e di proteggere la riservatezza dei dati se si applica la condizione di sicurezza SM-R-ENC-MAC-G1 (prima generazione) o SM-R-ENC-MAC-G2 (seconda generazione).

TCS_44 **Messaggio di comando**

Byte	Lunghezza	Valore	Descrizione
CLA	1	‘0Ch’	Richiesta messaggistica sicura
INS	1	‘B0h’	Read Binary
P1	1	‘XXh’	P1 (scostamento in byte dall'inizio del file): byte più significativo
P2	1	‘XXh’	P2 (scostamento in byte dall'inizio del file): byte meno significativo

▼B

Byte	Lunghezza	Valore	Descrizione
Lc	1	‘XXh’	Lunghezza dei dati in ingresso per messaggistica sicura
#6	1	‘97h’	T_{LE}: tag per la specificazione della lunghezza attesa
#7	1	‘01h’	L_{LE}: lunghezza della lunghezza attesa
#8	1	‘NNh’	Specificazione della lunghezza attesa (Le originale): numero di byte da leggere
#9	1	‘8Eh’	T_{CC}: tag per il totale di controllo crittografico
#10	1	‘XXh’	L_{CC}: lunghezza del totale di controllo crittografico successivo ‘04h’ per la messaggistica sicura di prima generazione (cfr. appendice 11, parte A) ‘08h’, ‘0Ch’ o ‘10h’ secondo la lunghezza della chiave AES per la messaggistica sicura di seconda generazione (cfr. appendice 11, parte B)
#11-#(10 + L)	L	‘XX..XXh’	Totale di controllo crittografico
Le	1	‘00h’	Secondo la norma ISO/IEC 7816-4

TCS_45 **Messaggio di risposta se SM-R-ENC-MAC-G1 (prima generazione) / SM-R-ENC-MAC-G2 (seconda generazione) non è necessario e se il formato di messaggistica sicura in ingresso è corretto:**

Byte	Lunghezza	Valore	Descrizione
#1	1	‘99h’	Tag per lo stato di elaborazione (SW1-SW2) — facoltativo per la messaggistica sicura di prima generazione
#2	1	‘02h’	Lunghezza dello stato di elaborazione
#3 — #4	2	‘XX XXh’	Stato di elaborazione della risposta APDU non protetta
#5	1	‘81h’	T_{PV}: tag per i dati in chiaro
#6	L	‘NNh’ o ‘81 NNh’	L_{PV}: lunghezza dei dati inviati in risposta (=Le originale). L è 2 byte se L_{PV} >127 byte
#(6 + L)-#(5 + L + NN)	NN	‘XX..XXh’	Dati in chiaro
#(6 + L + NN)	1	‘8Eh’	T_{CC}: tag per il totale di controllo crittografico
#(7 + L + NN)	1	‘XXh’	L_{CC}: lunghezza del totale di controllo crittografico successivo ‘04h’ per la messaggistica sicura di prima generazione (cfr. appendice 11, parte A) ‘08h’, ‘0Ch’ o ‘10h’ secondo la lunghezza della chiave AES per la messaggistica sicura di seconda generazione (cfr. appendice 11, parte B)
#(8 + L + NN)-#(7 + M + L + NN)	M	‘XX..XXh’	Totale di controllo crittografico
SW	2	‘XXXXh’	Parole di stato (SW1, SW2)

▼B

TCS_46 **Messaggio di risposta se SM-R-ENC-MAC-G1 (prima generazione) / SM-R-ENC-MAC-G2 (seconda generazione) è necessario e se il formato di messaggistica sicura in ingresso è corretto:**

Byte	Lunghezza	Valore	Descrizione
#1	1	'87h'	$T_{PI\ CG}$: tag per i dati criptati (crittogramma)
#2	L	'MMh' o '81 MMh'	$L_{PI\ CG}$: lunghezza dei dati criptati inviati in risposta (diversa da Le originale del comando a causa del riempimento) L è 2 byte se $L_{PI\ CG}$>127 byte
#(2+L)-#(1+L+MM)	MM	'01XX..XXh'	Dati criptati: indicatore di riempimento e crittogramma
#(2+L+MM)	1	'99h'	Tag per lo stato di elaborazione (SW1-SW2) — facoltativo per la messaggistica sicura di prima generazione
#(3+L+MM)	1	'02h'	Lunghezza dello stato di elaborazione
#(4+L+MM) — #(5+L+MM)	2	'XX XXh'	Stato di elaborazione della risposta APDU non protetta
#(6+L+MM)	1	'8Eh'	T_{CC}: tag per il totale di controllo crittografico
#(7+L+MM)	1	'XXh'	L_{CC}: lunghezza del totale di controllo crittografico successivo '04h' per la messaggistica sicura di prima generazione (cfr. appendice 11, parte A) '08h', '0Ch' o '10h' secondo la lunghezza della chiave AES per la messaggistica sicura di seconda generazione (cfr. appendice 11, parte B)
#(8+L+MM)-#(7+N+L+MM)	N	'XX..XXh'	Totale di controllo crittografico
SW	2	'XXXXh'	Parole di stato (SW1, SW2)

Il comando READ BINARY può inviare in risposta gli stati di elaborazione regolare elencati in TCS_43 con il tag '99h', come descritto in TCS_59, usando la struttura di risposta della messaggistica sicura.

Si possono inoltre verificare alcuni errori riguardanti in modo specifico la messaggistica sicura. In tal caso, viene inviato in risposta solo lo stato di elaborazione, senza strutture di messaggistica sicura.

TCS_47 **Messaggio di risposta se il formato di messaggistica sicura in ingresso è errato**

Byte	Lunghezza	Valore	Descrizione
SW	2	'XXXXh'	Parole di stato (SW1, SW2)

— Se non è disponibile una chiave di sessione corrente, viene inviato in risposta lo stato di elaborazione '**6A88**'. Questo si verifica se la chiave di sessione non è ancora stata generata o se è terminato il corso di validità della chiave di sessione (in questo caso l'IFD deve rieseguire un processo di autenticazione reciproca per impostare una nuova chiave di sessione).

▼B

— Se nel formato di messaggistica sicura mancano alcuni oggetti di dati attesi (secondo quanto sopra specificato), viene inviato in risposta lo stato di elaborazione '**6987**': questo errore si verifica se manca un tag atteso o se il comando non è costruito in modo corretto.

— Se alcuni oggetti di dati non sono corretti, lo stato di elaborazione inviato in risposta è '**6988**': questo errore si verifica se tutti i tag richiesti sono presenti, ma alcune lunghezze sono diverse da quelle attese.

— Se la verifica del totale di controllo crittografico ha esito negativo, lo stato di elaborazione inviato in risposta è '**6688**'.

3.5.2.2 Comando con identificativo breve dell'EF (file elementare)

Questa variante di comando consente all'IFD di selezionare un EF mediante un identificativo breve dell'EF e di leggere i dati da questo EF.

TCS_48 Una carta tachigrafica deve supportare questa variante di comando per tutti i file elementari con un identificativo breve dell'EF determinato. Questi identificativi brevi dell'EF sono specificati nel capitolo 4.

TCS_49 **Messaggio di comando**

Byte	Lunghezza	Valore	Descrizione
CLA	1	'00h'	
INS	1	'B0h'	Read Binary
P1	1	'XXh'	Il bit 8 è pari a 1 I bit 7 e 6 sono pari a 00 I bit 5 — 1 codificano l'identificativo breve dell'EF corrispondente
P2	1	'XXh'	Codifica uno scostamento da 0 a 255 byte nell'EF al quale si riferisce P1
Le	1	'XXh'	Lunghezza dei dati attesi. Numero di byte da leggere

Nota: gli identificativi brevi dell'EF utilizzati per l'applicazione tachigrafica di seconda generazione sono specificati nel capitolo 4.

Se P1 codifica un identificativo breve dell'EF e il comando ha esito positivo, l'EF identificato diventa l'EF selezionato in quel momento (EF corrente).

TCS_50 **Messaggio di risposta**

Byte	Lunghezza	Valore	Descrizione
#1-#L	L	'XX..XXh'	Dati letti
SW	2	'XXXXh'	Parole di stato (SW1, SW2)

— Se il comando ha esito positivo, la carta risponde '**9000**'.

— Se il file corrispondente all'identificativo breve dell'EF non viene trovato, lo stato di elaborazione inviato in risposta è '**6A82**'.

— Se le condizioni di sicurezza del file selezionato non sono soddisfatte, il comando viene interrotto con '**6982**'.

▼B

— Se lo scostamento non è compatibile con la dimensione dell'EF (scostamento > dimensione EF), lo stato di elaborazione inviato in risposta è '**6B00**'.

— Se la dimensione dei dati da leggere non è compatibile con la dimensione dell'EF (scostamento + Le > dimensione EF), lo stato di elaborazione inviato in risposta è '**6700**' o '**6Cxx**', dove 'xx' indica la lunghezza esatta.

— Se negli attributi del file è rilevato un errore di integrità, la carta deve considerare tale file danneggiato e irrecuperabile; lo stato di elaborazione inviato in risposta è '**6400**' o '**6581**'.

— Se nei dati memorizzati è rilevato un errore di integrità, la carta deve fornire i dati richiesti e inviare in risposta lo stato di elaborazione \'**6281**'.

3.5.2.3 Comando con byte di istruzioni dispari

Questa variante di comando consente all'IFD di leggere i dati da un EF con 32 768 byte o più.

TCS_51 Una carta tachigrafica che supporta EF con 32 768 byte o più deve supportare questa variante di comando per questi EF. Una carta tachigrafica può supportare o meno questa variante di comando per altri EF ad eccezione dell'EF Sensor_Installation_Data, cfr. TCS_156 e TCS_160.

TCS_52 **Messaggio di comando**

Byte	Lunghezza	Valore	Descrizione
CLA	1	'00h'	
INS	1	'B1h'	Read Binary
P1	1	'00h'	EF corrente
P2	1	'00h'	
Lc	1	'NNh'	Lc Lunghezza dell'oggetto di dati di scostamento
#6-#(5+NN)	NN	'XX..XXh'	Oggetto di dati di scostamento: Tag '54h' Lunghezza '01h' o '02h' Valore scostamento
Le	1	'XXh'	Numero di byte da leggere

L'IFD deve codificare la lunghezza dell'oggetto di dati di scostamento con il numero minimo possibile di ottetti, ovvero utilizzando il byte di lunghezza '01h', l'IFD deve codificare uno scostamento da 0 a 255 e, utilizzando il byte di lunghezza '02h', uno scostamento da '256' fino a '65 535' byte.

TCS_53 **Messaggio di risposta**

Byte	Lunghezza	Valore	Descrizione
#1-#L	L	'XX..XXh'	Dati letti incapsulati in un oggetto di dati discrezionale con tag '53h'.
SW	2	'XXXXh'	Parole di stato (SW1, SW2)

▼B

— Se il comando ha esito positivo, la carta risponde '**9000**'.

— Se non è selezionato un EF, lo stato di elaborazione inviato in risposta è '**6986**'.

— Se le condizioni di sicurezza del file selezionato non sono soddisfatte, il comando viene interrotto con '**6982**'.

— Se lo scostamento non è compatibile con la dimensione dell'EF (scostamento > dimensione EF), lo stato di elaborazione inviato in risposta è '**6B00**'.

— Se la dimensione dei dati da leggere non è compatibile con la dimensione dell'EF (scostamento + Le > dimensione EF), lo stato di elaborazione inviato in risposta è '**6700**' o '**6Cxx**', dove 'xx' indica la lunghezza esatta.

— Se negli attributi del file è rilevato un errore di integrità, la carta deve considerare tale file danneggiato e irrecuperabile; lo stato di elaborazione inviato in risposta è '**6400**' o '**6581**'.

— Se nei dati memorizzati è rilevato un errore di integrità, la carta deve fornire i dati richiesti e inviare in risposta lo stato di elaborazione '**6281**'.

3.5.2.3.1 Comando con messaggistica sicura (esempio)

Il seguente esempio illustra l'uso della messaggistica sicura se si applica la condizione di sicurezza SM-MAC-G2.

TCS_54 Messaggio di comando

Byte	Lunghezza	Valore	Descrizione
CLA	1	'0Ch'	Richiesta messaggistica sicura
INS	1	'B1h'	Read Binary
P1	1	'00h'	EF corrente
P2	1	'00h'	
Lc	1	'XXh'	Lunghezza del campo di dati sicuri
#6	1	'B3h'	Tag per i dati in chiaro codificati in BER-TLV
#7	1	'NNh'	L_{PV}: lunghezza dei dati trasmessi
#(8)-#(7+NN)	NN	'XX..XXh'	Dati in chiaro codificati in BER-TLV, vale a dire l'oggetto di dati di scostamento con tag '54'
#(8+NN)	1	'97h'	T_{LE}: tag per la specificazione della lunghezza attesa
#(9+NN)	1	'01h'	L_{LE}: lunghezza della lunghezza attesa
#(10+NN)	1	'XXh'	Specificazione della lunghezza attesa (Le originale): numero di byte da leggere
#(11+NN)	1	'8Eh'	T_{CC}: tag per il totale di controllo crittografico
#(12+NN)	1	'XXh'	L_{CC}: lunghezza del totale di controllo crittografico successivo '08h', '0Ch' o '10h' secondo la lunghezza della chiave AES per la messaggistica sicura di seconda generazione (cfr. appendice 11, parte B)
#(13+NN)-#(12+M+NN)	M	'XX..XXh'	Totale di controllo crittografico
Le	1	'00h'	Secondo la norma ISO/IEC 7816-4

▼B

TCS_55 Messaggio di risposta se il comando ha esito positivo

Byte	Lunghezza	Valore	Descrizione
#1	1	‘B3h’	Dati in chiaro codificati in BER-TLV
#2	L	‘NNh’ o ‘81 NNh’	L_{PV}: lunghezza dei dati inviati in risposta (=Le originale). L è 2 byte se L_{PV}>127 byte
#(2+L)-#(1+L+NN)	NN	‘XX..XXh’	Dati in chiaro codificati in BER-TLV, vale a dire dati letti incapsulati in un oggetto di dati discrezionale con tag ‘53h’
#(2+L+NN)	1	‘99h’	Stato di elaborazione della risposta APDU non protetta
#(3+L+NN)	1	‘02h’	Lunghezza dello stato di elaborazione
#(4+L+NN) — #(5+L+NN)	2	‘XX XXh’	Stato di elaborazione della risposta APDU non protetta
#(6+L+NN)	1	‘8Eh’	T_{CC}: tag per il totale di controllo crittografico
#(7+L+NN)	1	‘XXh’	L_{CC}: lunghezza del totale di controllo crittografico successivo ‘08h’, ‘0Ch’ o ‘10h’ secondo la lunghezza della chiave AES per la messaggistica sicura di seconda generazione (cfr. appendice 11, parte B)
#(8+L+NN)-#(7+M+L+NN)	M	‘XX..XXh’	Totale di controllo crittografico
SW	2	‘XXXXh’	Parole di stato (SW1, SW2)

3.5.3 *UPDATE BINARY*

Questo comando è conforme alla norma ISO/IEC 7816-4, ma ha un impiego limitato rispetto al comando definito nella norma.

Il messaggio di comando UPDATE BINARY avvia l'aggiornamento (cancellazione + scrittura) dei bit già presenti in un EF binario con i bit indicati nel comando APDU.

3.5.3.1 Comando con scostamento in P1-P2

Questo comando consente all'IFD di scrivere dati nell'EF selezionato, senza che la carta verifichi l'integrità dei dati ricevuti.

Nota: questo comando senza messaggistica sicura si può usare solo per aggiornare un file che supporta la condizione di sicurezza ALW per la modalità Update Access.

TCS_56 **Messaggio di comando**

Byte	Lunghezza	Valore	Descrizione
CLA	1	‘00h’	
INS	1	‘D6h’	Update Binary
P1	1	‘XXh’	Scostamento in byte dall'inizio del file: byte più significativo
P2	1	‘XXh’	Scostamento in byte dall'inizio del file: byte meno significativo

▼B

Byte	Lunghezza	Valore	Descrizione
Lc	1	‘NNh’	Lc Lunghezza dei dati da aggiornare. Numero di byte da scrivere
#6-#(5+NN)	NN	‘XX..XXh’	Dati da scrivere

Nota: il bit 8 di P1 dev'essere impostato a 0.

TCS_57 **Messaggio di risposta**

Byte	Lunghezza	Valore	Descrizione
SW	2	‘XXXXh’	Parole di stato (SW1, SW2)

— Se il comando ha esito positivo, la carta risponde ‘**9000**’.

— Se non è selezionato un EF, lo stato di elaborazione inviato in risposta è ‘**6986**’.

— Se le condizioni di sicurezza del file selezionato non sono soddisfatte, il comando viene interrotto con ‘**6982**’.

— Se lo scostamento non è compatibile con la dimensione dell'EF (scostamento > dimensione EF), lo stato di elaborazione inviato in risposta è ‘**6B00**’.

— Se la dimensione dei dati da scrivere non è compatibile con la dimensione dell'EF (scostamento + Lc > dimensione EF), lo stato di elaborazione inviato in risposta è ‘**6700**’.

— Se negli attributi del file è rilevato un errore di integrità, la carta deve considerare tale file danneggiato e irrecuperabile; lo stato di elaborazione inviato in risposta è ‘**6400**’ o ‘**6500**’.

— Se l'operazione di scrittura fallisce, lo stato di elaborazione inviato in risposta è ‘**6581**’.

3.5.3.1.1 Comando con messaggistica sicura (esempi)

Questo comando consente all'IFD di scrivere dati nell'EF selezionato, con verifica da parte della carta dell'integrità dei dati ricevuti. Poiché non è richiesta la riservatezza, i dati non sono criptati.

TCS_58 **Messaggio di comando**

Byte	Lunghezza	Valore	Descrizione
CLA	1	‘0Ch’	Richiesta messaggistica sicura
INS	1	‘D6h’	Update Binary
P1	1	‘XXh’	Scostamento in byte dall'inizio del file: byte più significativo
P2	1	‘XXh’	Scostamento in byte dall'inizio del file: byte meno significativo
Lc	1	‘XXh’	Lunghezza del campo di dati sicuri
#6	1	‘81h’	T_{PV}: tag per i dati in chiaro
#7	L	‘NNh’ o ‘81 NNh’	L_{PV}: lunghezza dei dati trasmessi L è 2 byte se L_{PV} >127 byte

▼B

Byte	Lunghezza	Valore	Descrizione
#(7+L)-#(6+L+NN)	NN	‘XX..XXh’	Valore dei dati in chiaro (dati da scrivere)
#(7+L+NN)	1	‘8Eh’	T_{CC}: tag per il totale di controllo crittografico
#(8+L+NN)	1	‘XXh’	L_{CC}: lunghezza del totale di controllo crittografico seguente ‘04h’ per la messaggistica sicura di prima generazione (cfr. appendice 11, parte A) ‘08h’, ‘0Ch’ o ‘10h’ secondo la lunghezza della chiave AES per la messaggistica sicura di seconda generazione (cfr. appendice 11, parte B)
#(9+L+NN)-#(8+M+L+NN)	M	‘XX..XXh’	Totale di controllo crittografico
Le	1	‘00h’	Secondo la norma ISO/IEC 7816-4

TCS_59 **Messaggio di risposta se il formato di messaggistica sicura in ingresso è corretto**

Byte	Lunghezza	Valore	Descrizione
#1	1	‘99h’	T_{SW}: tag per le parole di stato (deve essere protetto da CC)
#2	1	‘02h’	L_{SW}: lunghezza delle parole di stato inviate in risposta
#3-#4	2	‘XXXXh’	Stato di elaborazione della risposta APDU non protetta
#5	1	‘8Eh’	T_{CC}: tag per il totale di controllo crittografico
#6	1	‘XXh’	L_{CC}: lunghezza del totale di controllo crittografico successivo ‘04h’ per la messaggistica sicura di prima generazione (cfr. appendice 11, parte A) ‘08h’, ‘0Ch’ o ‘10h’ secondo la lunghezza della chiave AES per la messaggistica sicura di seconda generazione (cfr. appendice 11, parte B)
#7-#(6+L)	L	‘XX..XXh’	Totale di controllo crittografico
SW	2	‘XXXXh’	Parole di stato (SW1, SW2)

Gli stati di elaborazione «regolari», descritti per il comando UPDATE BINARY senza messaggistica sicura (cfr. §3.5.3.1), possono essere inviati in risposta utilizzando la struttura del messaggio di risposta sopra descritta.

Si possono inoltre verificare alcuni errori riguardanti in modo specifico la messaggistica sicura. In tal caso, viene inviato in risposta solo lo stato di elaborazione, senza strutture di messaggistica sicura.

TCS_60 **Messaggio di risposta in caso di errore di messaggistica sicura**

Byte	Lunghezza	Valore	Descrizione
SW	2	‘XXXXh’	Parole di stato (SW1, SW2)

▼B

— Se non è disponibile una chiave di sessione corrente, viene inviato in risposta lo stato di elaborazione '**6A88**'.

— Se nel formato di messaggistica sicura mancano alcuni oggetti di dati attesi (secondo quanto sopra specificato), viene inviato in risposta lo stato di elaborazione '**6987**': questo errore si verifica se manca un tag atteso o se il comando non è costruito in modo corretto.

— Se alcuni oggetti di dati non sono corretti, lo stato di elaborazione inviato in risposta è '**6988**': questo errore si verifica se tutti i tag richiesti sono presenti, ma alcune lunghezze sono diverse da quelle attese.

— Se la verifica del totale di controllo crittografico ha esito negativo, lo stato di elaborazione inviato in risposta è '**6688**'.

3.5.3.2 Comando con identificativo breve dell'EF

Questa variante di comando consente all'IFD di selezionare un EF mediante un identificativo breve dell'EF e di scrivere dati da questo EF.

TCS_61 Una carta tachigrafica deve supportare questa variante di comando per tutti i file elementari con un identificativo breve dell'EF determinato. Questi identificativi brevi dell'EF sono specificati nel capitolo 4.

TCS_62 **Messaggio di comando**

Byte	Lunghezza	Valore	Descrizione
CLA	1	'00h'	
INS	1	'D6h'	Update Binary
P1	1	'XXh'	Il bit 8 è pari a 1 I bit 7 e 6 sono pari a 00 I bit 5 — 1 codificano l'identificativo breve dell'EF corrispondente
P2	1	'XXh'	Codifica uno scostamento da 0 a 255 byte nell'EF al quale si riferisce P1
Lc	1	'NNh'	Lc Lunghezza dei dati da aggiornare. Numero di byte da scrivere
#6-#(5+NN)	NN	'XX..XXh'	Dati da scrivere

TCS_63 **Messaggio di risposta**

Byte	Lunghezza	Valore	Descrizione
SW	2	'XXXXh'	Parole di stato (SW1, SW2)

Nota: gli identificativi brevi dell'EF utilizzati per l'applicazione tachigrafica di seconda generazione sono specificati nel capitolo 4.

Se P1 codifica un identificativo breve dell'EF e il comando ha esito positivo, l'EF identificato diventa l'EF selezionato in quel momento (EF corrente).

▼B

— Se il comando ha esito positivo, la carta risponde '**9000**'.

— Se il file corrispondente all'identificativo breve dell'EF non viene trovato, lo stato di elaborazione inviato in risposta è '**6A82**'.

— Se le condizioni di sicurezza del file selezionato non sono soddisfatte, il comando viene interrotto con '**6982**'.

— Se lo scostamento non è compatibile con la dimensione dell'EF (scostamento > dimensione EF), lo stato di elaborazione inviato in risposta è '**6B00**'.

— Se la dimensione dei dati da scrivere non è compatibile con la dimensione dell'EF (scostamento + Lc > dimensione EF), lo stato di elaborazione inviato in risposta è '**6700**'.

— Se negli attributi del file è rilevato un errore di integrità, la carta deve considerare tale file danneggiato e irrecuperabile; lo stato di elaborazione inviato in risposta è '**6400**' o '**6581**'.

— Se l'operazione di scrittura fallisce, lo stato di elaborazione inviato in risposta è '**6581**'.

3.5.3.3 Comando con byte di istruzioni dispari

Questa variante di comando consente all'IFD di scrivere i dati in un EF con 32 768 byte o più.

TCS_64 Una carta tachigrafica che supporta EF con 32 768 byte o più deve supportare questa variante di comando per questi EF. Una carta tachigrafica può supportare o meno questa variante di comando per altri EF.

TCS_65 **Messaggio di comando**

Byte	Lunghezza	Valore	Descrizione
CLA	1	'00h'	
INS	1	'D7h'	Update Binary
P1	1	'00h'	EF corrente
P2	1	'00h'	
Lc	1	'NNh'	Lc Lunghezza dei dati nel campo di dati del comando
#6-#(5+NN)	NN	'XX..XXh'	Oggetto di dati di scostamento con tag '54h' || Oggetto di dati discrezionale con tag '53h' che incapsula i dati da scrivere

L'IFD deve codificare la lunghezza dell'oggetto di dati di scostamento e la lunghezza dell'oggetto di dati discrezionale con il numero minimo possibile di ottetti, ovvero utilizzando il byte di lunghezza '01h', l'IFD deve codificare uno scostamento / una lunghezza da 0 a 255 e, utilizzando il byte di lunghezza '02h', uno scostamento / una lunghezza da '256' fino a '65 535' byte.

TCS_66 **Messaggio di risposta**

Byte	Lunghezza	Valore	Descrizione
SW	2	'XXXXh'	Parole di stato (SW1, SW2)

▼B

— Se il comando ha esito positivo, la carta risponde '**9000**'.

— Se non è selezionato un EF, lo stato di elaborazione inviato in risposta è '**6986**'.

— Se le condizioni di sicurezza del file selezionato non sono soddisfatte, il comando viene interrotto con '**6982**'.

— Se lo scostamento non è compatibile con la dimensione dell'EF (scostamento > dimensione EF), lo stato di elaborazione inviato in risposta è '**6B00**'.

— Se la dimensione dei dati da scrivere non è compatibile con la dimensione dell'EF (scostamento + Lc > dimensione EF), lo stato di elaborazione inviato in risposta è '**6700**'.

— Se negli attributi del file è rilevato un errore di integrità, la carta deve considerare tale file danneggiato e irrecuperabile; lo stato di elaborazione inviato in risposta è '**6400**' o '**6500**'.

— Se l'operazione di scrittura fallisce, lo stato di elaborazione inviato in risposta è '**6581**'.

3.5.3.3.1 Comando con messaggistica sicura (esempio)

Il seguente esempio illustra l'uso della messaggistica sicura se si applica la condizione di sicurezza SM-MAC-G2.

TCS_67 Messaggio di comando

Byte	Lunghezza	Valore	Descrizione
CLA	1	'0Ch'	Richiesta messaggistica sicura
INS	1	'D7h'	Update Binary
P1	1	'00h'	EF corrente
P2	1	'00h'	
Lc	1	'XXh'	Lunghezza del campo di dati sicuri
#6	1	'B3h'	Tag per i dati in chiaro codificati in BER-TLV
#7	L	'NNh' o '81 NNh'	L_{PV}: lunghezza dei dati trasmessi L è 2 byte se L_{PV} >127 byte
#(7+L)-#(6+L+NN)	NN	'XX..XXh'	Dati in chiaro codificati in BER-TLV, vale a dire l'oggetto di dati di scostamento con tag '54h' || Oggetto di dati discrezionale con tag '53h' che incapsula i dati da scrivere
#(7+L+NN)	1	'8Eh'	T_{CC}: tag per il totale di controllo crittografico
#(8+L+NN)	1	'XXh'	L_{CC}: lunghezza del totale di controllo crittografico successivo '08h', '0Ch' o '10h' secondo la lunghezza della chiave AES per la messaggistica sicura di seconda generazione (cfr. appendice 11, parte B)
#(9+L+NN)-#(8+M+L+NN)	M	'XX..XXh'	Totale di controllo crittografico
Le	1	'00h'	Secondo la norma ISO/IEC 7816-4

▼B

TCS_68 Messaggio di risposta se il comando ha esito positivo

Byte	Lunghezza	Valore	Descrizione
#1	1	‘99h’	T_{SW}: tag per le parole di stato (deve essere protetto da CC)
#2	1	‘02h’	L_{SW}: lunghezza delle parole di stato inviate in risposta
#3-#4	2	‘XXXXh’	Stato di elaborazione della risposta APDU non protetta
#5	1	‘8Eh’	T_{CC}: tag per il totale di controllo crittografico
#6	1	‘XXh’	L_{CC}: lunghezza del totale di controllo crittografico successivo ‘08h’, ‘0Ch’ o ‘10h’ secondo la lunghezza della chiave AES per la messaggistica sicura di seconda generazione (cfr. appendice 11, parte B)
#7-#(6+L)	L	‘XX..XXh’	Totale di controllo crittografico
SW	2	‘XXXXh’	Parole di stato (SW1, SW2)

3.5.4 *GET CHALLENGE*

Questo comando è conforme alla norma ISO/IEC 7816-4, ma ha un impiego limitato rispetto al comando definito nella norma.

Il comando GET CHALLENGE chiede alla carta di generare una Challenge da utilizzare in una procedura di sicurezza, in cui un crittogramma o alcuni dati cifrati vengono inviati alla carta.

TCS_69 La Challenge generata dalla carta è valida solo per il comando successivo, che utilizza una Challenge, inviato alla carta.

TCS_70 **Messaggio di comando**

Byte	Lunghezza	Valore	Descrizione
CLA	1	‘00h’	
INS	1	‘84h’	INS
P1	1	‘00h’	P1
P2	1	‘00h’	P2
Le	1	‘08h’	Le (lunghezza della Challenge attesa).

TCS_71 **Messaggio di risposta**

Byte	Lunghezza	Valore	Descrizione
#1-#8	8	‘XX..XXh’	Challenge
SW	2	‘XXXXh’	Parole di stato (SW1, SW2)

— Se il comando ha esito positivo, la carta risponde ‘**9000**’.

— Se Le è diversa da ‘08h’, lo stato di elaborazione è ‘**6700**’.

— Se i parametri P1-P2 sono errati, lo stato di elaborazione è ‘**6A86**’.

▼B

3.5.5 *VERIFY*

Questo comando è conforme alla norma ISO/IEC 7816-4, ma ha un impiego limitato rispetto al comando definito nella norma.

Solo la carta dell'officina deve supportare questo comando.

Altri tipi di carte tachigrafiche possono eseguire o meno questo comando, ma per tali carte nessun CHV di riferimento è personalizzato. Tali carte non possono dunque eseguire questo comando con esito positivo. Per altri tipi di carte tachigrafiche diverse dalle carte dell'officina, il comportamento, cioè il codice di errore inviato in risposta, esula dal campo di applicazione delle presenti specifiche, se tale comando è inviato.

Il comando VERIFY avvia il confronto nella carta dei dati CHV (PIN) inviati dal comando con il CHV di riferimento memorizzato nella carta.

TCS_72 Il PIN inserito dall'utente dev'essere codificato in ASCI e riempito a destra con byte 'FFh' dall'IFD, fino a raggiungere la lunghezza di 8 byte, cfr. anche il tipo di dati WorkshopCardPIN nell'appendice 1.

TCS_73 Le applicazioni tachigrafiche di prima e seconda generazione devono usare lo stesso CHV di riferimento.

TCS_74 La carta tachigrafica deve verificare se il comando è codificato correttamente. Se il comando non è codificato correttamente, la carta non deve confrontare i valori CHV, non deve decrementare il contatore dei tentativi rimasti per il CHV e non deve azzerare lo stato di sicurezza «PIN_Verified», ma deve interrompere la trasmissione del comando. Un comando è codificato correttamente se i byte CLA, INS, P1, P2 e Lc hanno i valori specificati, Le è assente e il campo di dati del comando ha la lunghezza corretta.

TCS_75 Se il comando è eseguito correttamente, il contatore dei tentativi rimasti per il CHV è reinizializzato. Il valore iniziale del contatore dei tentativi rimasti per il CHV è 5. Se il comando è eseguito correttamente, la carta deve impostare lo stato di sicurezza interna «PIN_Verified». La carta deve azzerare tale stato di sicurezza se è reimpostata o se il codice CHV trasmesso nel comando non corrisponde al CHV di riferimento memorizzato.

Nota: l'uso dello stesso CHV di riferimento e di uno stato di sicurezza globale evita che un dipendente dell'officina debba reinserire il PIN dopo aver selezionato un altro DF dell'applicazione tachigrafica.

TCS_76 Se il confronto ha esito negativo, l'informazione viene registrata nella carta, vale a dire che il contatore dei tentativi rimasti per il CHV è decrementato di uno, al fine di limitare il numero di ulteriori tentativi d'uso del CHV di riferimento.

TCS_77 **Messaggio di comando**

Byte	Lunghezza	Valore	Descrizione
CLA	1	'00h'	
INS	1	'20h'	INS
P1	1	'00h'	P1

▼B

Byte	Lunghezza	Valore	Descrizione
P2	1	‘00h’	P2 (il CHV di riferimento verificato è implicitamente noto)
Lc	1	‘08h’	Lunghezza del codice CHV trasmesso
#6-#13	8	‘XX..XXh’	CHV

TCS_78 **Messaggio di risposta**

Byte	Lunghezza	Valore	Descrizione
SW	2	‘XXXXh’	Parole di stato (SW1, SW2)

— Se il comando ha esito positivo, la carta risponde ‘**9000**’.

— Se il CHV di riferimento non viene trovato, lo stato di elaborazione inviato in risposta è ‘**6A88**’.

— Se il CHV è bloccato (il contatore dei tentativi rimasti per il CHV è nullo), lo stato di elaborazione inviato in risposta è ‘**6983**’. In presenza di tale stato, il CHV non può più essere presentato con esito positivo.

— Se il confronto ha esito negativo, il contatore dei tentativi rimasti è decrementato e viene inviato in risposta lo stato ‘**63CX**’ (X > 0 e X è uguale al contatore dei tentativi rimasti per il CHV).

— Se il CHV di riferimento è considerato danneggiato, lo stato di elaborazione inviato in risposta è ‘**6400**’ o ‘**6581**’.

— Se Lc è diversa da ‘08h’, lo stato di elaborazione è ‘**6700**’.

3.5.6 *GET RESPONSE*

Questo comando è conforme alla norma ISO/IEC 7816-4.

Il comando (necessario e disponibile solo per il protocollo T=0) è utilizzato per trasmettere all'interfaccia i dati preparati dalla carta (caso in cui un comando include sia Lc che Le).

Il comando GET RESPONSE dev'essere inviato immediatamente dopo il comando di preparazione dei dati, altrimenti i dati in questione sono persi. Dopo l'esecuzione del comando GET RESPONSE (eccetto per il caso in cui si verifichi l'errore ‘**61xx**’ o ‘**6Cxx**’, cfr. sotto), i dati precedentemente preparati non sono più disponibili.

TCS_79 **Messaggio di comando**

Byte	Lunghezza	Valore	Descrizione
CLA	1	‘00h’	
INS	1	‘C0h’	
P1	1	‘00h’	
P2	1	‘00h’	
Le	1	‘XXh’	Numero di byte attesi

▼B

TCS_80 **Messaggio di risposta**

Byte	Lunghezza	Valore	Descrizione
#1-#X	X	'XX..XXh'	Dati
SW	2	'XXXXh'	Parole di stato (SW1, SW2)

— Se il comando ha esito positivo, la carta risponde '**9000**'.

— Se i dati non sono stati preparati dalla carta, lo stato di elaborazione inviato in risposta è '**6900**' o '**6F00**'.

— Se Le supera il numero di byte disponibili o è nullo, lo stato di elaborazione inviato in risposta è '**6Cxx**', dove 'xx' indica il numero esatto di byte disponibili. In tal caso, i dati preparati restano disponibili per un successivo comando GET RESPONSE.

— Se Le non è nullo ed è inferiore al numero di byte disponibili, i dati richiesti vengono inviati normalmente dalla carta e lo stato di elaborazione inviato in risposta è '**61xx**', dove 'xx' indica il numero di byte ancora disponibili per un ulteriore comando GET RESPONSE.

— Se il comando non è previsto (protocollo T = 1), la carta risponde '**6D00**'.

3.5.7 *PSO: VERIFY CERTIFICATE*

Questo comando è conforme alla norma ISO/IEC 7816-8, ma ha un impiego limitato rispetto al comando definito nella norma.

Il comando VERIFY CERTIFICATE è utilizzato dalla carta per ottenere una chiave pubblica dall'esterno e per verificarne la validità.

3.5.7.1 Coppia comando-risposta di prima generazione

TCS_81 Questa variante di comando è supportata solo da un'applicazione tachigrafica di prima generazione.

TCS_82 Se il comando VERIFY CERTIFICATE ha esito positivo, la chiave pubblica viene memorizzata per uso futuro nell'ambiente di sicurezza. Questa chiave è esplicitamente impostata dal comando MSE (cfr. § 3.5.11), utilizzando il suo identificativo della chiave, per l'impiego in comandi relativi alla sicurezza (INTERNAL AUTHENTICATE, EXTERNAL AUTHENTICATE o VERIFY CERTIFICATE).

TCS_83 In ogni caso, il comando VERIFY CERTIFICATE utilizza la chiave pubblica precedentemente selezionata dal comando MSE per aprire il certificato. Tale chiave pubblica deve essere quella di uno degli Stati membri o quella dell'Europa.

TCS_84 **Messaggio di comando**

Byte	Lunghezza	Valore	Descrizione
CLA	1	'00h'	
INS	1	'2Ah'	Esecuzione operazione di sicurezza
P1	1	'00h'	P1

▼B

Byte	Lunghezza	Valore	Descrizione
P2	1	‘AEh’	P2: dati non codificati BER-TLV (concatenamento di elementi di dati)
Lc	1	‘C2h’	Lc: lunghezza del certificato, 194 byte
#6-#199	194	‘XX..XXh’	Certificato: concatenamento di elementi di dati (secondo la descrizione di cui all'appendice 11)

TCS_85 **Messaggio di risposta**

Byte	Lunghezza	Valore	Descrizione
SW	2	‘XXXXh’	Parole di stato (SW1, SW2)

— Se il comando ha esito positivo, la carta risponde ‘**9000**’.

— Se la verifica del certificato fallisce, lo stato di elaborazione inviato in risposta è ‘**6688**’. Il processo di verifica e di apertura del certificato è descritto nell'appendice 11 per G1 e G2.

— Se nell'ambiente di sicurezza non è presente una chiave pubblica, viene inviato in risposta ‘**6A88**’.

— Se la chiave pubblica selezionata (usata per aprire il certificato) è considerata danneggiata, lo stato di elaborazione inviato in risposta è ‘**6400**’ o ‘**6581**’.

— Solo prima generazione: se la chiave pubblica selezionata (usata per aprire il certificato) ha una CHA.LSB (`CertificateHolderAuthorisation.equipmentType`) diversa da ‘00’ (ovvero non è quella di uno degli Stati membri o quella dell'Europa), lo stato di elaborazione inviato in risposta è ‘**6985**’.

3.5.7.2 Coppia comando-risposta di seconda generazione

Secondo le dimensioni della curva, i certificati ECC possono essere così lunghi da non poter essere trasmessi in un unico APDU. In questo caso è necessario applicare il concatenamento dei comandi conformemente alla norma ISO/IEC 7816-4 e il certificato deve essere trasmesso in due PSO consecutivi: Verify Certificate APDUs.

La struttura del certificato e i parametri del dominio sono definiti nell'appendice 11.

TCS_86 Il comando può essere eseguito in MF, DF Tachograph e DF Tachograph_G2, cfr. anche TCS_33.

TCS_87 **Messaggio di comando**

Byte	Lunghezza	Valore	Descrizione
CLA	1	‘X0h’	Byte CLA indicante il concatenamento dei comandi: ‘00h’ l'unico o l'ultimo comando della catena ‘10h’ non l'ultimo comando di una catena
INS	1	‘2Ah’	Esecuzione operazione di sicurezza
P1	1	‘00h’	
P2	1	‘BEh’	Verifica del certificato autodescrittivo

▼B

Byte	Lunghezza	Valore	Descrizione
Lc	1	'XXh'	Lunghezza del campo di dati del comando, cfr. TCS_88 e TCS_89
#6-#5+L	L	'XX..XXh'	Dati codificati DER-TLV: oggetto di dati del corpo del certificato ECC quale primo oggetto di dati concatenato all'oggetto di dati della firma del certificato ECC quale secondo oggetto di dati o parte di questa concatenazione. Il tag "7F21" e la lunghezza corrispondente non devono essere trasmessi. L'ordine di questi oggetti di dati è fisso.

TCS_88 Agli APDU di lunghezza breve si applicano le seguenti disposizioni: l'IFD deve utilizzare il numero minimo di APDU richiesti per trasmettere il payload del comando e deve trasmettere il numero massimo di byte nel primo comando APDU secondo il valore del byte di dimensione del campo di informazioni per la carta, cfr. TCS_14. Se l'IFD si comporta in modo diverso, il comportamento della carta è fuori del campo di applicazione.

TCS_89 Agli APDU di lunghezza estesa si applicano le seguenti disposizioni: se il certificato non entra in un unico APDU, la carta deve supportare il concatenamento dei comandi. L'IFD deve utilizzare il numero minimo di APDU richiesti per trasmettere il payload del comando e deve trasmettere il numero massimo di byte nel primo comando APDU. Se l'IFD si comporta in modo diverso, il comportamento della carta è fuori del campo di applicazione.

Nota: secondo l'appendice 11, la carta memorizza il certificato o i contenuti pertinenti del certificato e ne aggiorna il currentAuthenticatedTime.

La struttura del messaggio di risposta e le parole di stato sono come definite in TCS_85.

TCS_90 Oltre ai codici di errore elencati in TCS_85, la carta può inviare in risposta i seguenti codici di errore:

— Se la chiave pubblica selezionata (usata per aprire il certificato) ha una CHA.LSB (CertificateHolderAuthorisation.equipmentType) non idonea alla verifica del certificato secondo l'appendice 11, lo stato di elaborazione inviato in risposta è '**6985**'.

— Se il currentAuthenticatedTime della carta è successivo alla data di scadenza del certificato, lo stato di elaborazione inviato in risposta è '**6985**'.

— Se si aspetta l'ultimo comando della catena, la carta invia in risposta '**6883**'.

— Se nel campo di dati del comando sono trasmessi parametri non corretti, la carta invia in risposta '**6A80**' (usato anche nel caso in cui gli oggetti di dati non siano inviati nell'ordine specificato).

▼B

3.5.8 *INTERNAL AUTHENTICATE*

Questo comando è conforme alla norma ISO/IEC 7816-4.

TCS_91 Tutte le carte tachigrafiche devono supportare questo comando in DF Tachograph_G1. Il comando può essere accessibile o meno nell'MF e/o in DF Tachograph_G2. In caso sia accessibile, il comando deve finire con un codice di errore idoneo, poiché la chiave privata della carta (Card.SK) per il protocollo di autenticazione di prima generazione è accessibile unicamente in DF_Tachograph_G1.

Utilizzando il comando INTERNAL AUTHENTICATE, l'IFD può autenticare la carta. Il processo di autenticazione è descritto nell'appendice 11. Esso include i seguenti enunciati.

TCS_92 Il comando INTERNAL AUTHENTICATE utilizza la chiave privata della carta (selezionata implicitamente) per firmare dati di autenticazione, compresi K1 (primo elemento per l'accordo sulla chiave di sessione) e RND1, ed utilizza la chiave pubblica selezionata (mediante l'ultimo comando MSE) per criptare la firma e formare il token di autenticazione (cfr. appendice 11 per maggiori particolari).

TCS_93 **Messaggio di comando**

Byte	Lunghezza	Valore	Descrizione
CLA	1	‘00h’	CLA
INS	1	‘88h’	INS
P1	1	‘00h’	P1
P2	1	‘00h’	P2
Lc	1	‘10h’	Lunghezza dei dati inviati alla carta
#6 — #13	8	‘XX..XXh’	Challenge usata per autenticare la carta
#14 -#21	8	‘XX..XXh’	VU.CHR (cfr. appendice 11)
Le	1	‘80h’	Lunghezza dei dati attesi dalla carta

TCS_94 **Messaggio di risposta**

Byte	Lunghezza	Valore	Descrizione
#1-#128	128	‘XX..XXh’	Token di autenticazione della carta (cfr. appendice 11)
SW	2	‘XXXXh’	Parole di stato (SW1, SW2)

— Se il comando ha esito positivo, la carta risponde ‘**9000**’.

— Se nell'ambiente di sicurezza non è presente una chiave pubblica, lo stato di elaborazione inviato in risposta è ‘**6A88**’.

— Se nell'ambiente di sicurezza non è presente una chiave privata, lo stato di elaborazione inviato in risposta è ‘**6A88**’.

— Se VU.CHR non corrisponde all'identificativo della chiave pubblica corrente, lo stato di elaborazione inviato in risposta è ‘**6A88**’.

▼B

— Se la chiave privata selezionata è considerata danneggiata, lo stato di elaborazione inviato in risposta è '**6400**' o '**6581**'.

TCS_95 Se il comando INTERNAL AUTHENTICATE ha esito positivo, la chiave di sessione corrente, se presente, viene cancellata e non è più disponibile. Per avere a disposizione una nuova chiave di sessione, il comando EXTERNAL AUTHENTICATE per il meccanismo di autenticazione di prima generazione dev'essere eseguito con esito positivo.

3.5.9 *EXTERNAL AUTHENTICATE*

Questo comando è conforme alla norma ISO/IEC 7816-4.

Utilizzando il comando EXTERNAL AUTHENTICATE, la carta può autenticare l'IFD. Il processo di autenticazione è descritto nell'appendice 11 per i tachigrafi di prima e di seconda generazione (autenticazione della VU).

TCS_96 La variante di comando per il meccanismo di autenticazione reciproca di prima generazione è supportata solo da un'applicazione tachigrafica di prima generazione.

TCS_97 La variante di comando per l'autenticazione reciproca VU-carta di seconda generazione può essere eseguita nell'MF, in DF Tachograph e in DF Tachograph_G2, cfr. anche TCS_34.

TCS_98 **Messaggio di comando**

Byte	Lunghezza	Valore	Descrizione
CLA	1	'00h'	CLA
INS	1	'82h'	INS
P1	1	'00h'	Chiavi e algoritmi implicitamente noti
P2	1	'00h'	
Lc	1	'XXh'	Lc (lunghezza dei dati inviati alla carta)
#6-#(5+L)	L	'XX..XXh'	Autenticazione di prima generazione: crittogramma (cfr. appendice 11, parte A) Autenticazione di seconda generazione: firma generata dall'IFD (cfr. appendice 11, parte B)

TCS_99 **Messaggio di risposta**

Byte	Lunghezza	Valore	Descrizione
SW	2	'XXXXh'	Parole di stato (SW1, SW2)

— Se il comando ha esito positivo, la carta risponde '**9000**'.

— Se il CHA della chiave pubblica impostata non è il concatenamento dell'AID dell'applicazione tachigrafica e di un tipo di apparecchio VU, lo stato di elaborazione inviato in risposta è '**6F00**'.

— Se il comando non è immediatamente preceduto da un comando GET CHALLENGE, lo stato di elaborazione inviato in risposta è '**6985**'.

▼B

L'applicazione tachigrafica di prima generazione può inviare in risposta gli ulteriori codici di errore a seguire:

— Se nell'ambiente di sicurezza non è presente una chiave pubblica, viene inviato in risposta '**6A88**'.

— Se nell'ambiente di sicurezza non è presente una chiave privata, lo stato di elaborazione inviato in risposta è '**6A88**'.

— Se la verifica del crittogramma è errata, lo stato di elaborazione inviato in risposta è '**6688**'.

— Se la chiave privata selezionata è considerata danneggiata, lo stato di elaborazione inviato in risposta è '**6400**' o '**6581**'.

La variante di comando per l'autenticazione di seconda generazione può inviare in risposta il seguente codice di errore supplementare:

— Se la verifica della firma non è andata a buon fine, la carta invia in risposta '**6300**'.

3.5.10 *GENERAL AUTHENTICATE*

Questo comando è usato per il protocollo di autenticazione del chip di seconda generazione specificato nell'appendice 11, parte B, ed è conforme alla norma ISO/IEC 7816-4.

TCS_100 Il comando può essere eseguito nell'MF, in DF Tachograph e in DF Tachograph_G2, cfr. anche TCS_34.

TCS_101 **Messaggio di comando**

Byte	Lunghezza	Valore	Descrizione
CLA	1	'00h'	
INS	1	'86h'	
P1	1	'00h'	Chiavi e protocollo implicitamente noti
P2	1	'00h'	
Lc	1	'NNh'	Lc: lunghezza del campo di dati successivo
#6-#(5+L)	L	'7Ch' + L_{7C} + '80h' + L_{80} + 'XX..XXh'	Valore della chiave pubblica temporanea codificato DER-TLV (cfr. appendice 11) La VU deve inviare gli oggetti di dati in quest'ordine

TCS_102 **Messaggio di risposta**

Byte	Lunghezza	Valore	Descrizione
#1-#L	L	'7Ch' + L_{7C} + '81h' + '08h' + 'XX..XXh' + '82h' + L_{82} + 'XX..XXh'	Dati di autenticazione dinamica codificati DER-TLV: nonce e token di autenticazione (cfr. appendice 11)
SW	2	'XXXXh'	Parole di stato (SW1, SW2)

— Se il comando ha esito positivo, la carta risponde '**9000**'.

— La carta invia in risposta '**6A80**' per indicare parametri errati nel campo di dati.

▼B

— La carta invia in risposta '**6982**' se il comando External Authenticate non è stato eseguito correttamente.

L'oggetto di dati di autenticazione dinamica della risposta '7Ch':

— deve essere presente se l'operazione è riuscita, vale a dire se le parole di stato sono '**9000**',

— deve essere assente in caso di errore di esecuzione o di controllo, vale a dire se le parole di stato rientrano nell'intervallo '**6400**' — '**6FFF**' e

— può essere assente in caso di avvertimento, vale a dire se le parole di stato rientrano nell'intervallo '**6200**' — '**63FFF**'.

3.5.11 *MANAGE SECURITY ENVIRONMENT*

Questo comando è usato per impostare una chiave pubblica a scopo di autenticazione.

3.5.11.1 Coppia comando-risposta di prima generazione

Questo comando è conforme alla norma ISO/IEC 7816-4. L'uso del comando è limitato rispetto a quello previsto dalla norma.

TCS_103 Questo comando è supportato solo da un'applicazione tachigrafica di prima generazione.

TCS_104 La chiave indicata nel campo di dati MSE rimane la chiave pubblica corrente fino al successivo comando MSE corretto, finché non si seleziona un DF o non si azzera la carta.

TCS_105 Se la chiave indicata non è (già) presente nella carta, l'ambiente di sicurezza resta invariato.

TCS_106 **Messaggio di comando**

Byte	Lunghezza	Valore	Descrizione
CLA	1	'00h'	CLA
INS	1	'22h'	INS
P1	1	'C1h'	P1: chiave indicata valida per tutte le operazioni crittografiche
P2	1	'B6h'	P2: dati indicati riguardanti la firma digitale
Lc	1	'0Ah'	Lc: lunghezza del campo di dati successivo
#6	1	'83h'	Tag per indicare una chiave pubblica in casi asimmetrici
#7	1	'08h'	Lunghezza del riferimento della chiave (identificativo della chiave)
#8-#15	8	'XX..XXh'	Identificativo della chiave, secondo quanto specificato nell'appendice 11

TCS_107 **Messaggio di risposta**

Byte	Lunghezza	Valore	Descrizione
SW	2	'XXXXh'	Parole di stato (SW1, SW2)

▼B

— Se il comando ha esito positivo, la carta risponde '**9000**'.

— Se la chiave indicata non è presente nella carta, lo stato di elaborazione inviato in risposta è '**6A88**'.

— Se mancano alcuni oggetti di dati attesi nel formato di messaggistica sicura, viene inviato in risposta lo stato di elaborazione '**6987**'. Ciò si può verificare se manca il tag '83h'.

— Se alcuni oggetti di dati non sono corretti, lo stato di elaborazione inviato in risposta è '**6988**'. Ciò si può verificare se la lunghezza dell'identificativo della chiave è diversa da '08h'.

— Se la chiave selezionata è considerata danneggiata, lo stato di elaborazione inviato in risposta è '**6400**' o '**6581**'.

3.5.11.2 Coppie comando-risposta di seconda generazione

Per l'autenticazione di seconda generazione, la carta tachigrafica supporta le seguenti versioni del comando MSE: SET, che sono conformi alla norma ISO/IEC 7816-4. Queste versioni di comando non sono supportate per l'autenticazione di prima generazione.

3.5.11.2.1 MSE:SET AT per l'autenticazione del chip

Il seguente comando MSE:SET AT è usato per selezionare i parametri per l'autenticazione del chip, che è eseguita da un comando successivo General Authenticate.

TCS_108 Il comando può essere eseguito nell'MF, in DF Tachograph e in DF Tachograph_G2, cfr. anche TCS_34.

TCS_109 **Messaggio di comando MSE:SET AT per l'autenticazione del chip**

Byte	Lunghezza	Valore	Descrizione
CLA	1	'00h'	
INS	1	'22h'	
P1	1	'41h'	Impostato per l'autenticazione interna
P2	1	'A4h'	Autenticazione
Lc	1	'NNh'	Lc: lunghezza del campo di dati successivo
#6-#(5+L)	L	'80h' + '0Ah' + 'XX..XXh'	Riferimento del meccanismo crittografico codificato DER-TLV: identificativo dell'oggetto dell'autenticazione del chip (solo valore, il tag '06h' è omesso). Cfr. appendice 1 per i valori degli identificativi degli oggetti; si deve usare la notazione in byte. Cfr. appendice 11 per informazioni su come scegliere uno di questi identificativi degli oggetti.

3.5.11.2.2 MSE:SET AT per l'autenticazione della VU

Il seguente comando MSE:SET AT è usato per selezionare i parametri e le chiavi per l'autenticazione della VU, che è eseguita da un comando successivo General Authenticate.

▼B

TCS_110 Il comando può essere eseguito nell'MF, in DF Tachograph e in DF Tachograph_G2, cfr. anche TCS_34.

TCS_111 **Messaggio di comando MSE:SET AT per l'autenticazione della VU**

Byte	Lunghezza	Valore	Descrizione
CLA	1	‘00h’	
INS	1	‘22h’	
P1	1	‘81h’	Impostato per l'autenticazione esterna
P2	1	‘A4h’	Autenticazione
Lc	1	‘NNh’	Lc: lunghezza del campo di dati successivo
#6-#(5+L)	L	‘80h’ + ‘0Ah’ + ‘XX..XXh’	Riferimento del meccanismo crittografico codificato DER-TLV: identificativo dell'oggetto dell'autenticazione della VU (solo valore, il tag ‘06h’ è omesso). Cfr. appendice 1 per i valori degli identificativi degli oggetti; si deve usare la notazione in byte. Cfr. appendice 11 per informazioni su come scegliere uno di questi identificativi degli oggetti.
		‘83h’ + ‘08h’ + ‘XX..XXh’	Riferimento codificato DER-TLV della chiave pubblica della VU da parte del Certificate Holder Reference indicato nel rispettivo certificato
		‘91h’ + L_{91} + ‘XX..XXh’	Rappresentazione compressa codificata DER-TLV della chiave pubblica temporanea della VU che sarà usata durante l'autenticazione del chip (cfr. appendice 11)

3.5.11.2.3 MSE:SET DST

Il seguente comando MSE:SET DST è usato per impostare una chiave pubblica:

— per la verifica di una firma che figura in un PSO successivo: comando Verify Digital Signature o

— per la verifica della firma di un certificato che figura in un PSO successivo: comando Verify Certificate

TCS_112 Il comando può essere eseguito in MF, DF Tachograph e DF Tachograph_G2, cfr. anche TCS_33.

TCS_113 **Messaggio di comando MSE:SET DST**

Byte	Lunghezza	Valore	Descrizione
CLA	1	‘00h’	
INS	1	‘22h’	
P1	1	‘81h’	Impostato per la verifica
P2	1	‘B6h’	Firma digitale

▼B

Lc	1	‘NNh’	Lc: lunghezza del campo di dati successivo
#6-#(5+L)	L	‘83h’ + ‘08h’ + ‘XX...XXh’	Riferimento codificato DER-TLV di una chiave pubblica, vale a dire il Certificate Holder Reference nel certificato della chiave pubblica (cfr. appendice 11)

Per tutte le versioni di comando, la struttura del messaggio di risposta e le parole di stato sono date da:

TCS_114 **Messaggio di risposta**

Byte	Lunghezza	Valore	Descrizione
SW	2	‘XXXXh’	Parole di stato (SW1, SW2)

— Se il comando ha esito positivo, la carta risponde ‘**9000**’. Il protocollo è stato selezionato e inizializzato.

— ‘**6A80**’ indica parametri non corretti nel campo di dati del comando.

— ‘**6A88**’ indica che i dati indicati (ossia una chiave indicata) non sono disponibili.

3.5.12 *PSO: HASH*

Questo comando si usa per trasferire alla carta il risultato del calcolo di una funzione di hash di alcuni dati. Questo comando è usato per verificare le firme digitali. Il valore di hash è memorizzato temporaneamente per il successivo comando PSO: Verify Digital Signature

Questo comando è conforme alla norma ISO/IEC 7816-8. L'uso del comando è limitato rispetto a quello previsto dalla norma.

Solo la carta di controllo deve supportare questo comando in DF Tachograph e DF Tachograph_G2.

Altri tipi di carte tachigrafiche possono eseguire o meno questo comando. Il comando può essere accessibile o meno nell'MF.

L'applicazione della carta di controllo di prima generazione supporta solo SHA-1.

TCS_115 Il valore di hash temporaneamente memorizzato deve essere cancellato se è calcolato un nuovo valore di hash tramite il comando PSO: HASH, se un DF è selezionato e se la carta tachigrafica è azzerata.

TCS_116 **Messaggio di comando**

Byte	Lunghezza	Valore	Descrizione
CLA	1	‘00h’	CLA
INS	1	‘2Ah’	Esecuzione operazione di sicurezza
P1	1	‘90h’	Codice Hash di risposta

▼B

Byte	Lunghezza	Valore	Descrizione
P2	1	‘A0h’	Tag: il campo dati contiene DO interessati alla funzione di hash
Lc	1	‘XXh’	Lunghezza Lc del campo di dati successivo
#6	1	‘90h’	Tag per il codice hash
#7	1	‘XXh’	Lunghezza L del codice hash: ‘14h’ nell'applicazione di prima generazione (cfr. appendice 11, parte A) ‘20h’, ‘30h’ o ‘40h’ nell'applicazione di seconda generazione (cfr. appendice 11, parte B)
#8-#(7+L)	L	‘XX..XXh’	Codice hash

TCS_117 **Messaggio di risposta**

Byte	Lunghezza	Valore	Descrizione
SW	2	‘XXXXh’	Parole di stato (SW1, SW2)

— Se il comando ha esito positivo, la carta risponde ‘**9000**’.

— Se mancano alcuni oggetti di dati attesi (secondo quanto sopra specificato), viene inviato in risposta lo stato di elaborazione ‘**6987**’. Ciò si può verificare se manca uno dei tag ‘90h’.

— Se alcuni oggetti di dati non sono corretti, lo stato di elaborazione inviato in risposta è ‘**6988**’. Questo errore si verifica se il tag richiesto è presente, ma con una lunghezza diversa da ‘14h’ per SHA-1, ‘20h’ per SHA-256, ‘30h’ per SHA-384 e ‘40h’ per SHA-512 (applicazione di seconda generazione).

3.5.13 *PERFORM HASH of FILE*

Questo comando non è conforme alla norma ISO/IEC 7816-8. Pertanto il byte CLA di questo comando indica che il comando PERFORM SECURITY OPERATION/HASH viene utilizzato in modo esclusivo e riservato.

Solo la carta del conducente e la carta dell'officina devono supportare questo comando in DF Tachograph e DF Tachograph_G2.

Altri tipi di carte tachigrafiche possono eseguire o meno questo comando. Se una carta dell'azienda o una carta di controllo esegue questo comando, il comando deve essere eseguito come specificato nel presente capitolo.

Il comando può essere accessibile o meno nell'MF. Se lo è, il comando deve essere eseguito come specificato nel presente capitolo, vale a dire non deve consentire il calcolo di un valore di hash, ma deve finire con un codice di errore opportuno.

TCS_118 Il comando PERFORM HASH of FILE è usato per eseguire la funzione di hash dell'area di dati dell'EF trasparente selezionato.

TCS_119 Una carta tachigrafica deve supportare questo comando solo per gli EF che sono elencati nel capitolo 4 sotto DF_Tachograph e DF_Tachograph_G2 con la seguente eccezione. Una carta tachigrafica non deve supportare il comando per Sensor_Installation_Data dell'EF di DF Tachograph_G2.

▼B

TCS_120 Il risultato dell'operazione di hash è memorizzato temporaneamente nella carta. Può poi essere usato per ottenere una firma digitale del file, utilizzando il comando PSO: COMPUTE DIGITAL SIGNATURE.

TCS_121 Il valore Hash of File temporaneamente memorizzato deve essere cancellato se è calcolato un nuovo valore Hash of File tramite il comando PSO: HASH of File, se un DF è selezionato e se la carta tachigrafica è azzerata.

TCS_122 L'applicazione del tachigrafo di prima generazione deve supportare SHA-1.

TCS_123 L'applicazione del tachigrafo di seconda generazione deve supportare SHA-1 e SHA-2 (256, 384 e 512 bit).

TCS_124 **Messaggio di comando**

Byte	Lunghezza	Valore	Descrizione
CLA	1	‘80h’	CLA
INS	1	‘2Ah’	Esecuzione operazione di sicurezza
P1	1	‘90h’	Tag: Hash
P2	1	‘XXh’	P2: indica l'algoritmo da usare per eseguire la funzione di hash dei dati del file trasparente selezionato: ‘00h’ per SHA-1 ‘01h’ per SHA-256 ‘02h’ per SHA-384 ‘03h’ per SHA-512

TCS_125 **Messaggio di risposta**

Byte	Lunghezza	Valore	Descrizione
SW	2	‘XXXXh’	Parole di stato (SW1, SW2)

— Se il comando ha esito positivo, la carta risponde ‘**9000**’.

— Se l'EF corrente non consente questo comando (EF Sensor_Installation_Data in DF Tachograph_G2), lo stato di elaborazione inviato in risposta è ‘**6985**’.

— Se l'EF selezionato è considerato danneggiato (errori d'integrità negli attributi del file o nei dati registrati), lo stato di elaborazione inviato in risposta è ‘**6400**’ o ‘**6581**’.

— Se il file selezionato non è un file trasparente o se non c'è nessun EF corrente, lo stato di elaborazione inviato in risposta è ‘**6986**’.

3.5.14 *PSO: COMPUTE DIGITAL SIGNATURE*

Questo comando è usato per calcolare la firma digitale del codice hash precedentemente calcolato (cfr. PERFORM HASH OF FILE, § 3.5.13).

Solo la carta del conducente e la carta dell'officina devono supportare questo comando in DF Tachograph e DF Tachograph_G2.

▼B

Altri tipi di carte tachigrafiche possono eseguire o meno questo comando, ma non devono avere una chiave di firma. Tali carte quindi non possono eseguire il comando correttamente, ma finiscono con un codice di errore idoneo.

Il comando può essere accessibile o meno nell'MF. Se lo è, il comando deve finire con un codice di errore idoneo.

Questo comando è conforme alla norma ISO/IEC 7816-8. L'uso del comando è limitato rispetto a quello previsto dalla norma.

TCS_126 Questo comando non deve calcolare una firma digitale di un codice hash precedentemente calcolato con il comando PSO: HASH.

TCS_127 La chiave privata della carta è usata per calcolare la firma digitale ed è implicitamente nota alla carta.

TCS_128 L'applicazione tachigrafica di prima generazione esegue una firma digitale utilizzando un metodo di riempimento conforme a PKCS1 (cfr. appendice 11 per ulteriori particolari).

TCS_129 L'applicazione tachigrafica di seconda generazione calcola una firma digitale basata su una curva ellittica (cfr. appendice 11 per ulteriori particolari).

TCS_130 **Messaggio di comando**

Byte	Lunghezza	Valore	Descrizione
CLA	1	‘00h’	CLA
INS	1	‘2Ah’	Esecuzione operazione di sicurezza
P1	1	‘9Eh’	Firma digitale da inviare in risposta
P2	1	‘9Ah’	Tag: il campo di dati contiene dati da firmare. Poiché non è incluso un campo di dati, i dati sono considerati già presenti nella carta (hash del file)
Le	1	‘NNh’	Lunghezza della firma attesa

TCS_131 **Messaggio di risposta**

Byte	Lunghezza	Valore	Descrizione
#1-#L	L	‘XX..XXh’	Firma dell'hash precedentemente calcolato
SW	2	‘XXXXh’	Parole di stato (SW1, SW2)

— Se il comando ha esito positivo, la carta risponde ‘**9000**’.

— Se la chiave privata implicitamente selezionata è considerata danneggiata, lo stato di elaborazione inviato in risposta è ‘**6400**’ o ‘**6581**’.

— Se l'hash calcolato in un precedente comando Perform Hash of File non è disponibile, lo stato di elaborazione inviato in risposta è ‘**6985**’.

▼B

3.5.15 *PSO: VERIFY DIGITAL SIGNATURE*

Questo comando si usa per verificare la firma digitale, fornita come un input, il cui hash è noto alla carta. L'algoritmo della firma è implicitamente noto alla carta.

Questo comando è conforme alla norma ISO/IEC 7816-8. L'uso del comando è limitato rispetto a quello previsto dalla norma.

Solo la carta di controllo deve supportare questo comando in DF Tachograph e DF Tachograph_G2.

Altri tipi di carte tachigrafiche possono eseguire o meno questo comando. Il comando può essere accessibile o meno nell'MF.

TCS_132 Il comando VERIFY DIGITAL SIGNATURE usa sempre la chiave pubblica selezionata dal precedente comando MSE: Set DST e il codice hash precedente inserito da un comando PSO: HASH.

TCS_133 **Messaggio di comando**

Byte	Lunghezza	Valore	Descrizione
CLA	1	‘00h’	CLA
INS	1	‘2Ah’	Esecuzione operazione di sicurezza
P1	1	‘00h’	
P2	1	‘A8h’	Tag: il campo di dati contiene DO pertinenti per la verifica
Lc	1	‘83h’	Lunghezza Lc del campo di dati successivo
6	1	‘9Eh’	Tag per la firma digitale
#7-#8	2	‘81 XXh’	Lunghezza della firma digitale: 128 byte codificati conformemente all'appendice 11, parte A, per l'applicazione tachigrafica di prima generazione. Secondo la curva selezionata per l'applicazione tachigrafica di seconda generazione (cfr. appendice 11, parte B)
#9-#(8+L)	L	‘XX..XXh’	Contenuto della firma digitale

TCS_134 **Messaggio di risposta**

Byte	Lunghezza	Valore	Descrizione
SW	2	‘XXXXh’	Parole di stato (SW1, SW2)

— Se il comando ha esito positivo, la carta risponde ‘**9000**’.

— Se la verifica della firma fallisce, lo stato di elaborazione inviato in risposta è ‘**6688**’. Il processo di verifica è descritto nell'appendice 11.

— Se non è selezionata nessuna chiave pubblica, lo stato di elaborazione inviato in risposta è ‘**6A88**’.

— Se mancano alcuni oggetti di dati attesi (secondo quanto sopra specificato), viene inviato in risposta lo stato di elaborazione ‘**6987**’. Ciò si può verificare se manca uno dei tag richiesti.

▼B

— Se non è disponibile un codice hash per elaborare il comando (in conseguenza di un comando PSO: HASH precedente), lo stato di elaborazione inviato in risposta è '**6985**'.

— Se alcuni oggetti di dati non sono corretti, lo stato di elaborazione inviato in risposta è '**6988**'. Ciò si può verificare se la lunghezza di uno degli oggetti di dati richiesti non è corretta.

— Se la chiave pubblica selezionata è considerata danneggiata, lo stato di elaborazione inviato in risposta è '**6400**' o '**6581**'.

3.5.16 *PROCESS DSRC MESSAGE*

Questo comando è usato per verificare l'integrità e l'autenticità del messaggio DSRC e per decifrare i dati comunicati da una VU a un'autorità di controllo o a un'officina tramite il link DSRC. La carta calcola la chiave di cifratura e la chiave del MAC utilizzate per rendere sicuro il messaggio DSRC, come descritto nell'appendice 11, parte B, capitolo 13.

Solo la carta di controllo e la carta dell'officina devono supportare questo comando in DF Tachograph_G2.

Altri tipi di carte tachigrafiche possono eseguire o meno questo comando, ma non devono avere una chiave master DSRC. Tali carte quindi non possono eseguire il comando correttamente, ma finiscono con un codice di errore idoneo.

Il comando può essere accessibile o meno nell'MF e/o in DF Tachograph. Se lo è, il comando deve finire con un codice di errore idoneo.

TCS_135 La chiave master DSRC è accessibile solo in DF Tachograph_G2, vale a dire che la carta di controllo e la carta dell'officina devono supportare un'esecuzione corretta del comando solo in DF Tachograph_G2.

TCS_136 Il comando deve solo decriptare i dati DSRC e verificare il totale di controllo crittografico, ma non deve interpretare i dati in ingresso.

TCS_137 L'ordine degli oggetti di dati nel campo di dati del comando è fissato nelle presenti specifiche.

TCS_138 **Messaggio di comando**

Byte	Lunghezza	Valore	Descrizione
CLA	1	'80h'	CLA proprietaria
INS	1	'2Ah'	Esecuzione operazione di sicurezza
P1	1	'80h'	Dati della risposta: valore in chiaro
P2	1	'B0h'	Dati del comando: valore in chiaro codificato in BER-TLV e comprendente DO SM
Lc	1	'NNh'	Lunghezza Lc del campo di dati successivo

▼B

Byte	Lunghezza	Valore	Descrizione
#6-#(5+L)	L	'87h' + L_{87} + 'XX..XXh'	Byte indicatore di contenuto di riempimento codificato DER-TLV seguito dal payload criptato del tachigrafo. Per il byte indicatore di contenuto di riempimento si deve usare il valore '00h' («nessuna ulteriore indicazione» secondo la norma ISO/IEC 7816-4: 2013, tabella 52). Per il meccanismo di cifratura, cfr. appendice 11, parte B, capitolo 13. I valori consentiti per la lunghezza L_{87} sono i multipli della lunghezza dei blocchi AES più 1 per il byte indicatore di contenuto di riempimento, vale a dire da 17 byte fino a 193 byte compresi. *Nota:* cfr. ISO/IEC 7816-4: 2013, tabella 49, per l'oggetto di dati SM con tag '87h'.
		'81h' + '10h'	Modello di controllo di riferimento per la riservatezza codificato DER-TLV che annida la concatenazione dei seguenti elementi di dati (cfr. appendice 1 DSRCSecurityData e appendice 11, parte B, capitolo 13): — time stamp: 4 byte — contatore: 3 byte — numero di serie della VU: 8 byte — versione della chiave master DSRC: 1 byte *Nota:* cfr. ISO/IEC 7816-4: 2013, tabella 49, per l'oggetto di dati SM con tag '81h'.
		'8Eh' + L_{8E} + 'XX..XXh'	MAC codificato DER-TLV sul messaggio DSRC. Per l'algoritmo e il calcolo del MAC, cfr. appendice 11, parte B, capitolo 13. *Nota:* cfr. ISO/IEC 7816-4: 2013, tabella 49, per l'oggetto di dati SM con tag '8Eh'.

TCS_139 **Messaggio di risposta**

Byte	Lunghezza	Valore	Descrizione
#1-#L	L	'XX..XXh'	Assente (in caso di errore) o dati decodificati (riempimento eliminato)
SW	2	'XXXXh'	Parole di stato (SW1, SW2)

— Se il comando ha esito positivo, la carta risponde '**9000**'.

— '**6A80**' indica parametri non corretti nel campo di dati del comando (usato anche nel caso in cui gli oggetti di dati non siano inviati nell'ordine specificato).

— '**6A88**' indica che i dati indicati non sono disponibili, vale a dire che la chiave master DSRC indicata non è disponibile.

— '**6900**' indica che la verifica del totale di controllo crittografico o la decifrazione dei dati non è andata a buon fine.

4. STRUTTURA DELLE CARTE TACHIGRAFICHE

Il presente paragrafo specifica le strutture dei file delle carte tachigrafiche per la memorizzazione di dati accessibili.

▼B

Non specifica le strutture interne, che dipendono dal fabbricante della carta, come per esempio le intestazioni dei file, né la memorizzazione e la gestione degli elementi di dati necessari solo per uso interno, quali EuropeanPublicKey, CardPrivateKey, TdesSessionKey o WorkshopCardPin.

TCS_140 Una carta tachigrafica di seconda generazione deve ospitare il master file MF e un'applicazione tachigrafica di prima e di seconda generazione dello stesso tipo (ad esempio le applicazioni della carta del conducente).

TCS_141 Una carta tachigrafica deve supportare almeno il numero minimo di registrazioni specificate per le applicazioni corrispondenti e non deve supportare più registrazioni rispetto al numero massimo di registrazioni specificato per le applicazioni corrispondenti.

Il numero massimo e il numero minimo di registrazioni sono specificati nel presente capitolo per le diverse applicazioni.

Per le condizioni di sicurezza usate nelle norme di accesso nel presente capitolo si rimanda al capitolo 3.3. In generale, la modalità di accesso «leggi» indica il comando READ BINARY con il byte INS pari e, se supportato, dispari, ad eccezione di EF Sensor_Installation_Data sulla carta dell'officina, cfr. TCS_156 e TCS_160. La modalità di accesso «aggiorna» indica il comando UPDATE BINARY con il byte INS pari e, se supportato, dispari, e la modalità di accesso «seleziona» in dica il comando SELECT.

4.1. Master file MF

TCS_142 Dopo la personalizzazione, il master file MF deve avere la struttura dei file e le regole di accesso ai file permanenti a seguire:

Nota: l'identificativo breve dell'EF SFID è indicato come numero decimale: ad esempio, il valore 30 corrisponde a 11110 in formato binario.

			Regole di accesso	
File	**ID del file**	**SFID**	**Leggi/seleziona**	**Aggiorna**
MF	'3F00h'			
├─ EF ICC	'0002h'		ALW	NEV
├─ EF IC	'0005h'		ALW	NEV
├─ EF DIR	'2F00h'	30	ALW	NEV
├─ EF ATR/INFO (conditional)	'2F01h'	29	ALW	NEV
├─ EF Extended_Length (conditional)	'0006h'	28	ALW	NEV
├─ DF Tachograph	'0500h'		SC1	
└─ DF Tachograph_G2			SC1	

Nella tabella a seguire si usa la seguente abbreviazione per le condizioni di sicurezza:

SC1 ALW OR SM-MAC-G2

TCS_143 Le strutture di tutti gli EF devono essere trasparenti.

TCS_144 Il file principale MF deve avere la struttura dei dati seguente:

▼B

File / Elemento di dati	Numero di registrazioni	Dimensioni (byte) Min.	Max.	Valori standard
MF		*63*	*184*	
EF ICC		*25*	*25*	
CardIccIdentification		*25*	*25*	
clockStop		1	1	{00}
cardExtendedSerialNumber		8	8	{00..00}
cardApprovalNumber		8	8	{20..20}
cardPersonaliserID		1	1	{00}
embedderIcAssemblerId		5	5	{00..00}
icIdentifier		2	2	{00 00}
EF IC		*8*	*8*	
CardChipIdentification		*8*	*8*	
icSerialNumber		4	4	{00..00}
icManufacturingReferences		4	4	{00..00}
EF DIR		*20*	*20*	
See TCS_145		*20*	*20*	{00..00}
EF ATR/INFO		*7*	*128*	
See TCS_146		*7*	*128*	{00..00}
EF EXTENDED_LENGTH		*3*	*3*	
See TCS_147		*3*	*3*	{00..00}
DF Tachograph				
DF Tachograph_G2				

TCS_145 Il file elementare EF DIR deve contenere i seguenti oggetti di dati relativi all'applicazione: '61 08 4F 06 FF 54 41 43 48 4F 61 08 4F 06 FF 53 4D 52 44 54'

TCS_146 Il file elementare EF ATR/INFO deve essere presente se la carta tachigrafica indica nella sua ATR che supporta campi di lunghezza estesa. In questo caso, EF ATR/INFO deve contenere l'oggetto di dati di informazioni di lunghezza estesa (DO'7F66'), come specificato nella norma ISO/IEC 7816-4:2013, clausola 12.7.1.

TCS_147 Il file elementare EF Extended_Length deve essere presente se la carta tachigrafica indica nella sua ATR che supporta campi di lunghezza estesa. In questo caso l'EF deve contenere il seguente oggetto di dati: '02 01 xx' dove il valore 'xx' indica se i campi di lunghezza estesa sono supportati per il protocollo T = 1 e / o T = 0.

Il valore '01' indica che i campi di lunghezza estesa sono supportati per il protocollo T = 1.

Il valore '10' indica che i campi di lunghezza estesa sono supportati per il protocollo T = 0.

Il valore '11' indica che i campi di lunghezza estesa sono supportati per il protocollo T = 1 e T = 0.

4.2. Applicazioni della carta del conducente

4.2.1 *Applicazione della carta del conducente di prima generazione*

TCS_148 Dopo la personalizzazione, l'applicazione della carta del conducente di prima generazione deve avere la struttura dei file e le regole di accesso permanenti a seguire.

File	ID del file	Regole di accesso		
		Leggi	Seleziona	Aggiorna
DF Tachograph	'0500h'		SC1	
EF Application_Identification	'0501h'	SC2	SC1	NEV
EF Card_Certificate	'C100h'	SC2	SC1	NEV
EF CA_Certificate	'C108h'	SC2	SC1	NEV
EF Identification	'0520h'	SC2	SC1	NEV
EF Card_Download	'050Eh'	SC2	SC1	SC1
EF Driving_Licence_Info	'0521h'	SC2	SC1	NEV
EF Events_Data	'0502h'	SC2	SC1	SC3
EF Faults_Data	'0503h'	SC2	SC1	SC3
EF Driver_Activity_Data	'0504h'	SC2	SC1	SC3
EF Vehicles_Used	'0505h'	SC2	SC1	SC3
EF Places	'0506h'	SC2	SC1	SC3
EF Current_Usage	'0507h'	SC2	SC1	SC3
EF Control_Activity_Data	'0508h'	SC2	SC1	SC3
EF Specific_Conditions	'0522h'	SC2	SC1	SC3

▼B

Nella tabella a seguire si usano le seguenti abbreviazioni per le condizioni di sicurezza:

SC1 ALW OR SM-MAC-G2

SC2 ALW OR SM-MAC-G1 OR SM-MAC-G2

SC3 SM-MAC-G1 OR SM-MAC-G2

TCS_149 Le strutture di tutti gli EF devono essere trasparenti.

TCS_150 L'applicazione della carta del conducente di prima generazione deve avere la seguente struttura dei dati:

File / Elemento di dati	Numero di registrazioni	Dimensioni (in byte) Min.	Max.	Valori standard
DF Tachograph		*11378*	*24926*	
EF Application_Identification		*10*	*10*	
DriverCardApplicationIdentification		*10*	*10*	
typeOfTachographCardId		1	1	{00}
cardStructureVersion		2	2	{00 00}
noOfEventsPerType		1	1	{00}
noOfFaultsPerType		1	1	{00}
activityStructureLength		2	2	{00 00}
noOfCardVehicleRecords		2	2	{00 00}
noOfCardPlaceRecords		1	1	{00}
EF Card_Certificate		*194*	*194*	
CardCertificate		194	194	{00..00}
EF CA_Certificate		*194*	*194*	
MemberStateCertificate		194	194	{00..00}
EF Identification		*143*	*143*	
CardIdentification		*65*	*65*	
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
cardIssuingAuthorityName		36	36	{20..20}
cardIssueDate		4	4	{00..00}
cardValidityBegin		4	4	{00..00}
cardExpiryDate		4	4	{00..00}
DriverCardHolderIdentification		*78*	*78*	
cardHolderName		*72*	*72*	
holderSurname		36	36	{00, 20..20}
holderFirstNames		36	36	{00, 20..20}
cardHolderBirthDate		4	4	{00..00}
cardHolderPreferredLanguage		2	2	{20 20}
EF Card_Download		*4*	*4*	
LastCardDownload		4	4	
EF Driving_Licence_Info		*53*	*53*	
CardDrivingLicenceInformation		*53*	*53*	
drivingLicenceIssuingAuthority		36	36	{00, 20..20}
drivingLicenceIssuingNation		1	1	{00}
drivingLicenceNumber		16	16	{20..20}
EF Events_Data		*864*	*1728*	
CardEventData		*864*	*1728*	
cardEventRecords	6	*144*	*288*	
CardEventRecord	n_1	*24*	*24*	
eventType		1	1	{00}
eventBeginTime		4	4	{00..00}
eventEndTime		4	4	{00..00}
eventVehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
EF Faults_Data		*576*	*1152*	
CardFaultData		*576*	*1152*	
cardFaultRecords	2	*288*	*576*	
CardFaultRecord	n_2	*24*	*24*	
faultType		1	1	{00}
faultBeginTime		4	4	{00..00}
faultEndTime		4	4	{00..00}
faultVehicleRegistration				

▼B

vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
EF Driver_Activity_Data		*5548*	*13780*	
CardDriverActivity		*5548*	*13780*	
activityPointerOldestDayRecord		2	2	{00 00}
activityPointerNewestRecord		2	2	{00 00}
activityDailyRecords	n_6	5544	13776	{00..00}
EF Vehicles_Used		*2606*	*6202*	
CardVehiclesUsed		*2606*	*6202*	
vehiclePointerNewestRecord		2	2	{00 00}
cardVehicleRecords		*2604*	*6200*	
CardVehicleRecord	n_3	*31*	*31*	
vehicleOdometerBegin		3	3	{00..00}
vehicleOdometerEnd		3	3	{00..00}
vehicleFirstUse		4	4	{00..00}
vehicleLastUse		4	4	{00..00}
vehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
vuDataBlockCounter		2	2	{00 00}
EF Places		*841*	*1121*	
CardPlaceDailyWorkPeriod		*841*	*1121*	
placePointerNewestRecord		1	1	{00}
placeRecords		*840*	*1120*	
PlaceRecord	n_4	*10*	*10*	
entryTime		4	4	{00..00}
entryTypeDailyWorkPeriod		1	1	{00}
dailyWorkPeriodCountry		1	1	{00}
dailyWorkPeriodRegion		1	1	{00}
vehicleOdometerValue		3	3	{00..00}
EF Current_Usage		*19*	*19*	
CardCurrentUse		*19*	*19*	
sessionOpenTime		4	4	{00..00}
sessionOpenVehicle				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
EF Control_Activity_Data		*46*	*46*	
CardControlActivityDataRecord		*46*	*46*	
controlType		1	1	{00}
controlTime		4	4	{00..00}
controlCardNumber				
cardType		1	1	{00}
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
controlVehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
controlDownloadPeriodBegin		4	4	{00..00}
controlDownloadPeriodEnd		4	4	{00..00}
EF Specific_Conditions		*280*	*280*	
SpecificConditionRecord	56	*5*	*5*	
entryTime		4	4	{00..00}
SpecificConditionType		1	1	{00}

▼B

TCS_151 I valori sotto indicati, usati per fornire le dimensioni nella tabella precedente, sono i valori minimo e massimo del numero di registrazioni che la struttura dei dati della carta del conducente deve utilizzare per un'applicazione di prima generazione:

		Min.	Max.
n_1	NoOfEventsPerType	6	12
n_2	NoOfFaultsPerType	12	24
n_3	NoOfCardVehicleRecords	84	200
n_4	NoOfCardPlaceRecords	84	112
n_6	CardActivityLengthRange	5 544 byte (28 giorni * 93 cambi di attività)	13 776 byte (28 giorni * 240 cambi di attività)

4.2.2 *Applicazione della carta del conducente di seconda generazione*

TCS_152 Dopo la personalizzazione, l'applicazione della carta del conducente di seconda generazione deve avere la struttura dei file e le regole di accesso permanenti a seguire.

Nota: l'identificativo breve dell'EF SFID è indicato come numero decimale: ad esempio, il valore 30 corrisponde a 11110 in formato binario.

			Regole di accesso	
File	**ID del file**	**SFID**	**Leggi/seleziona**	**Aggiorna**
└─DF Tachograph_G2			SC1	
├─EF Application_Identification	'0501h'	1	SC1	NEV
├─EF CardMA_Certificate	'C100h'	2	SC1	NEV
├─EF CardSignCertificate	'C101h'	3	SC1	NEV
├─EF CA_Certificate	'C108h'	4	SC1	NEV
├─EF Link_Certificate	'C109h'	5	SC1	NEV
├─EF Identification	'0520h'	6	SC1	NEV
├─EF Card_Download	'050Eh'	7	SC1	SC1
├─EF Driving_Licence_Info	'0521h'	10	SC1	NEV
├─EF Events_Data	'0502h'	12	SC1	SM-MAC-G2
├─EF Faults_Data	'0503h'	13	SC1	SM-MAC-G2
├─EF Driver_Activity_Data	'0504h'	14	SC1	SM-MAC-G2
├─EF Vehicles_Used	'0505h'	15	SC1	SM-MAC-G2
├─EF Places	'0506h'	16	SC1	SM-MAC-G2
├─EF Current_Usage	'0507h'	17	SC1	SM-MAC-G2
├─EF Control_Activity_Data	'0508h'	18	SC1	SM-MAC-G2
├─EF Specific_Conditions	'0522h'	19	SC1	SM-MAC-G2
├─EF VehicleUnits_Used	'0523h'	20	SC1	SM-MAC-G2
└─EF GNSS_Places	'0524h'	21	SC1	SM-MAC-G2

Nella tabella a seguire si usa la seguente abbreviazione per le condizioni di sicurezza:

SC1 ALW OR SM-MAC-G2

TCS_153 Le strutture di tutti gli EF devono essere trasparenti.

TCS_154 L'applicazione della carta del conducente di seconda generazione deve avere la seguente struttura dei dati:

▼B

File / Elemento di dati	Numero di registrazioni	Dimensioni (in byte) Min.	Max.	Valori standard
DF Tachograph_G2		*19510*	*39306*	
EF Application_Identification		*15*	*15*	
DriverCardApplicationIdentification		*15*	*15*	
typeOfTachographCardId		1	1	{00}
cardStructureVersion		2	2	{00 00}
noOfEventsPerType		1	1	{00}
noOfFaultsPerType		1	1	{00}
activityStructureLength		2	2	{00 00}
noOfCardVehicleRecords		2	2	{00 00}
noOfCardPlaceRecords		2	2	{00}
noOfGNSSCDRecords		2	2	{00 00}
noOfSpecificConditionRecords		2	2	{00}
EF CardMA_Certificate		*204*	*341*	
CardMACertificate		204	341	{00..00}
EF CardSignCertificate		*204*	*341*	
CardSignCertificate		204	341	{00..00}
EF CA_Certificate		*204*	*341*	
MemberStateCertificate		204	341	{00..00}
EF Link_Certificate		*204*	*341*	
LinkCertificate		204	341	{00..00}
EF Identification		*143*	*143*	
CardIdentification		*65*	*65*	
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
cardIssuingAuthorityName		36	36	{20..20}
cardIssueDate		4	4	{00..00}
cardValidityBegin		4	4	{00..00}
cardExpiryDate		4	4	{00..00}
DriverCardHolderIdentification		*78*	*78*	
cardHolderName		*72*	*72*	
holderSurname		36	36	{00, 20..20}
holderFirstNames		36	36	{00, 20..20}
cardHolderBirthDate		4	4	{00..00}
cardHolderPreferredLanguage		2	2	{20 20}
EF Card_Download		*4*	*4*	
LastCardDownload		4	4	
EF Driving_Licence_Info		*53*	*53*	
CardDrivingLicenceInformation		*53*	*53*	
drivingLicenceIssuingAuthority		36	36	{00, 20..20}
drivingLicenceIssuingNation		1	1	{00}
drivingLicenceNumber		16	16	{20..20}
EF Events_Data		*1584*	*3168*	
CardEventData		*1584*	*3168*	
cardEventRecords	11	*144*	*288*	
CardEventRecord	n_1	*24*	*24*	
eventType		1	1	{00}
eventBeginTime		4	4	{00..00}
eventEndTime		4	4	{00..00}
eventVehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
EF Faults_Data		*576*	*1152*	
CardFaultData		*576*	*1152*	
cardFaultRecords	2	*288*	*576*	
CardFaultRecord	n_2	*24*	*24*	

▼B

├─faultType		1	1	{00}
├─faultBeginTime		4	4	{00..00}
├─faultEndTime		4	4	{00..00}
└─faultVehicleRegistration				
├─vehicleRegistrationNation		1	1	{00}
└─vehicleRegistrationNumber		14	14	{00, 20..20}
EF Driver_Activity_Data		*5548*	*13780*	
└CardDriverActivity		*5548*	*13780*	
├─activityPointerOldestDayRecord		2	2	{00 00}
├─activityPointerNewestRecord		2	2	{00 00}
└─activityDailyRecords	n_6	5544	13776	{00..00}
EF Vehicles_Used		*4034*	*9602*	
└CardVehiclesUsed		*4034*	*9602*	
├─vehiclePointerNewestRecord		2	2	{00 00}
└─cardVehicleRecords		*4032*	*9600*	
└─CardVehicleRecord	n_3	*48*	*48*	
├─vehicleOdometerBegin		3	3	{00..00}
├─vehicleOdometerEnd		3	3	{00..00}
├─vehicleFirstUse		4	4	{00..00}
├─vehicleLastUse		4	4	{00..00}
├─vehicleRegistration				
├─vehicleRegistrationNation		1	1	{00}
└─vehicleRegistrationNumber		14	14	{00, 20..20}
├─vuDataBlockCounter		2	2	{00 00}
└─vehicleIdentificationNumber		17	17	{20..20}
EF Places		*1766*	*2354*	
└CardPlaceDailyWorkPeriod		*1766*	*2354*	
├─placePointerNewestRecord		2	2	{00 00}
└─placeRecords		*1764*	*2352*	
└─PlaceRecord	n_4	*21*	*21*	
├─entryTime		4	4	{00..00}
├─entryTypeDailyWorkPeriod		1	1	{00}
├─dailyWorkPeriodCountry		1	1	{00}
├─dailyWorkPeriodRegion		1	1	{00}
├─vehicleOdometerValue		3	3	{00..00}
└─entryGNSSPlaceRecord		11	11	
├─timeStamp		4	4	{00..00}
├─gnssAccuracy		1	1	{00}
└─geoCoordinates		6	6	{00..00}
EF Current_Usage		*19*	*19*	
└CardCurrentUse		*19*	*19*	
├─sessionOpenTime		4	4	{00..00}
└─sessionOpenVehicle				
├─vehicleRegistrationNation		1	1	{00}
└─vehicleRegistrationNumber		14	14	{00, 20..20}
EF Control_Activity_Data		*46*	*46*	
└CardControlActivityDataRecord		*46*	*46*	
├─controlType		1	1	{00}
├─controlTime		4	4	{00..00}
├─controlCardNumber				
├─cardType		1	1	{00}
├─cardIssuingMemberState		1	1	{00}
└─cardNumber		16	16	{20..20}
├─controlVehicleRegistration				
├─vehicleRegistrationNation		1	1	{00}
└─vehicleRegistrationNumber		14	14	{00, 20..20}
├─controlDownloadPeriodBegin		4	4	{00..00}
└─controlDownloadPeriodEnd		4	4	{00..00}

▼B

EF Specific_Conditions		*282*	*562*	
SpecificConditions		*282*	*562*	
conditionPointerNewestRecord		2	2	{00 00}
specificConditionRecords		*280*	*560*	
SpecificConditionRecord	n_9	*5*	*5*	
entryTime		4	4	{00..00}
specificConditionType		1	1	{00}
EF VehicleUnits_Used		*842*	*2002*	
CardVehicleUnitsUsed		*842*	*2002*	
vehicleUnitPointerNewestRecord		2	2	{00 00}
cardVehicleUnitRecords		*840*	*2000*	
CardVehicleUnitRecord	n_7	*10*	*10*	
timeStamp		4	4	{00..00}
manufacturerCode		1	1	{00}
deviceID		1	1	{00}
vuSoftwareVersion		4	4	{00..00}
EF GNSS_Places		*3782*	*5042*	
GNSSContinuousDriving		*3782*	*5042*	
gnssCDPointerNewestRecord		2	2	{00 00}
gnssContinuousDrivingRecords		3780	5040	{00}
GNSSContinuousDrivingRecord	n_8	*15*	*15*	
timeStamp		4	4	{00..00}
gnssPlaceRecord		11	11	
timeStamp		4	4	{00..00}
gnssAccuracy		1	1	{00}
geoCoordinates		6	6	{00..00}

TCS_155 I valori sotto indicati, usati per fornire le dimensioni nella tabella precedente, sono i valori minimo e massimo del numero di registrazioni che la struttura dei dati della carta del conducente deve utilizzare per un'applicazione di seconda generazione:

		Min.	**Max.**
n_1	NoOfEventsPerType	6	12
n_2	NoOfFaultsPerType	12	24
n_3	NoOfCardVehicleRecords	84	200
n_4	NoOfCardPlaceRecords	84	112
n_6	CardActivityLengthRange	5 544 byte (28 giorni * 93 cambi di attività)	13 776 byte (28 giorni * 240 cambi di attività)
n_7	NoOfCardVehicleUnitRecords	84	200
n_8	NoOfGNSSCDRecords	252	336
n_9	NoOfSpecificConditionRecords	56	112

4.3. **Applicazioni della carta dell'officina**

4.3.1 *Applicazione della carta dell'officina di prima generazione*

TCS_156 Dopo la personalizzazione, l'applicazione della carta dell'officina di prima generazione deve avere la struttura dei file e le regole di accesso permanenti a seguire.

▼B

		Regole di accesso		
File	**ID del file**	**Leggi**	**Seleziona**	**Aggiorna**
└─DF Tachograph	'0500h'		SC1	
├─EF Application_Identification	'0501h'	SC2	SC1	NEV
├─EF Card_Certificate	'C100h'	SC2	SC1	NEV
├─EF CA_Certificate	'C108h'	SC2	SC1	NEV
├─EF Identification	'0520h'	SC2	SC1	NEV
├─EF Card_Download	'0509h'	SC2	SC1	**SC1**
├─EF Calibration	'050Ah'	SC2	SC1	SC3
├─EF Sensor_Installation_Data	'050Bh'	**SC4**	SC1	NEV
├─EF Events_Data	'0502h'	SC2	SC1	SC3
├─EF Faults_Data	'0503h'	SC2	SC1	SC3
├─EF Driver_Activity_Data	'0504h'	SC2	SC1	SC3
├─EF Vehicles_Used	'0505h'	SC2	SC1	SC3
├─EF Places	'0506h'	SC2	SC1	SC3
├─EF Current_Usage	'0507h'	SC2	SC1	SC3
├─EF Control_Activity_Data	'0508h'	SC2	SC1	SC3
└─EF Specific_Conditions	'0522h'	SC2	SC1	SC3

Nella tabella a seguire si usano le seguenti abbreviazioni per le condizioni di sicurezza:

SC1 ALW OR SM-MAC-G2

SC2 ALW OR SM-MAC-G1 OR SM-MAC-G2

SC3 SM-MAC-G1 OR SM-MAC-G2

SC4 Per il comando READ BINARY con byte INS pari:

(PLAIN-C E SM-R-ENC-G1) OR (SM-C-MAC-G1 E SM-R-ENC-MAC-G1) OR

(SM-C-MAC-G2 E SM-R-ENC-MAC-G2)

Per il comando READ BINARY con byte INS dispari (se supportato): NEV

TCS_157 Le strutture di tutti gli EF devono essere trasparenti.

TCS_158 L'applicazione della carta dell'officina di prima generazione deve avere la seguente struttura dei dati:

▼B

File / Elemento di dati	Numero di registrazioni	Dimensioni (byte) Min.	Dimensioni (byte) Max.	Valori standard
DF Tachograph		*11055*	*29028*	
EF Application_Identification		*11*	*11*	
WorkshopCardApplicationIdentification		*11*	*11*	
typeOfTachographCardId		1	1	{00}
cardStructureVersion		2	2	{00 00}
noOfEventsPerType		1	1	{00}
noOfFaultsPerType		1	1	{00}
activityStructureLength		2	2	{00 00}
noOfCardVehicleRecords		2	2	{00 00}
noOfCardPlaceRecords		1	1	{00}
noOfCalibrationRecords		1	1	{00}
EF Card_Certificate		*194*	*194*	
CardCertificate		194	194	{00..00}
EF CA_Certificate		*194*	*194*	
MemberStateCertificate		194	194	{00..00}
EF Identification		*211*	*211*	
CardIdentification		65	65	
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
cardIssuingAuthorityName		36	36	{00, 20..20}
cardIssueDate		4	4	{00..00}
cardValidityBegin		4	4	{00..00}
cardExpiryDate		4	4	{00..00}
WorkshopCardHolderIdentification		*146*	*146*	
workshopName		36	36	{00, 20..20}
workshopAddress		36	36	{00, 20..20}
cardHolderName				
holderSurname		36	36	{00, 20..20}
holderFirstNames		36	36	{00, 20..20}
cardHolderPreferredLanguage		2	2	{20 20}
EF Card_Download		*2*	*2*	
NoOfCalibrationsSinceDownload		2	2	{00 00}
EF Calibration		*9243*	*26778*	
WorkshopCardCalibrationData		*9243*	*26778*	
calibrationTotalNumber		2	2	{00 00}
calibrationPointerNewestRecord		1	1	{00}
calibrationRecords		*9240*	*26775*	
WorkshopCardCalibrationRecord	n_5	*105*	*105*	
calibrationPurpose		1	1	{00}
vehicleIdentificationNumber		17	17	{20..20}
vehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
wVehicleCharacteristicConstant		2	2	{00 00}
kConstantOfRecordingEquipment		2	2	{00 00}
lTyreCircumference		2	2	{00 00}
tyreSize		15	15	{20..20}
authorisedSpeed		1	1	{00}
oldOdometerValue		3	3	{00..00}
newOdometerValue		3	3	{00..00}
oldTimeValue		4	4	{00..00}
newTimeValue		4	4	{00..00}
nextCalibrationDate		4	4	{00..00}
vuPartNumber		16	16	{20..20}
vuSerialNumber		8	8	{00..00}
sensorSerialNumber		8	8	{00..00}

▼B

EF Sensor_Installation_Data		*16*	*16*	
SensorInstallationSecData		16	16	{00..00}
EF Events_Data		*432*	*432*	
CardEventData		*432*	*432*	
cardEventRecords	6	*72*	*72*	
CardEventRecord	n_1	*24*	*24*	
eventType		1	1	{00}
eventBeginTime		4	4	{00..00}
eventEndTime		4	4	{00..00}
eventVehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
EF Faults_Data		*288*	*288*	
CardFaultData		*288*	*288*	
cardFaultRecords	2	*144*	*144*	
CardFaultRecord	n_2	*24*	*24*	
faultType		1	1	{00}
faultBeginTime		4	4	{00..00}
faultEndTime		4	4	{00..00}
faultVehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
EF Driver_Activity_Data		*202*	*496*	
CardDriverActivity		*202*	*496*	
activityPointerOldestDayRecord		2	2	{00 00}
activityPointerNewestRecord		2	2	{00 00}
activityDailyRecords	n_6	198	492	{00..00}
EF Vehicles_Used		*126*	*250*	
CardVehiclesUsed		*126*	*250*	
vehiclePointerNewestRecord		2	2	{00 00}
cardVehicleRecords		*124*	*248*	
CardVehicleRecord	n_3	*31*	*31*	
vehicleOdometerBegin		3	3	{00..00}
vehicleOdometerEnd		3	3	{00..00}
vehicleFirstUse		4	4	{00..00}
vehicleLastUse		4	4	{00..00}
vehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
vuDataBlockCounter		2	2	{00 00}
EF Places		*61*	*81*	
CardPlaceDailyWorkPeriod		*61*	*81*	
placePointerNewestRecord		1	1	{00}
placeRecords		*60*	*80*	
PlaceRecord	n_4	*10*	*10*	
entryTime		4	4	{00..00}
entryTypeDailyWorkPeriod		1	1	{00}
dailyWorkPeriodCountry		1	1	{00}
dailyWorkPeriodRegion		1	1	{00}
vehicleOdometerValue		3	3	{00..00}
EF Current_Usage		*19*	*19*	
CardCurrentUse		*19*	*19*	
sessionOpenTime		4	4	{00..00}
sessionOpenVehicle				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}

▼B

EF Control_Activity_Data		*46*	*46*	
CardControlActivityDataRecord	2	*46*	*46*	
controlType		1	1	{00}
controlTime		4	4	{00..00}
controlCardNumber				
cardType		1	1	{00}
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
controlVehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
controlDownloadPeriodBegin		4	4	{00..00}
controlDownloadPeriodEnd		4	4	{00..00}
EF Specific_Conditions		*10*	*10*	
SpecificConditionRecord	2	*5*	*5*	
entryTime		4	4	{00..00}
SpecificConditionType		1	1	{00}

TCS_159 I valori sottoindicati, usati per fornire le dimensioni nella tabella precedente, sono i valori minimo e massimo del numero di registrazioni che la struttura dei dati della carta dell'officina deve utilizzare per un'applicazione di prima generazione:

		Min.	**Max.**
n_1	NoOfEventsPerType	3	3
n_2	NoOfFaultsPerType	6	6
n_3	NoOfCardVehicleRecords	4	8
n_4	NoOfCardPlaceRecords	6	8
n_5	NoOfCalibrationRecords	88	255
n_6	CardActivityLengthRange	198 byte (1 giorno * 93 cambi di attività)	492 byte (1 giorno * 240 cambi di attività)

4.3.2 *Applicazione della carta dell'officina di seconda generazione*

TCS_160 Dopo la personalizzazione, l'applicazione della carta dell'officina di seconda generazione deve avere la struttura dei file e le regole di accesso permanenti a seguire.

Nota: l'identificativo breve dell'EF SFID è indicato come numero decimale: ad esempio, il valore 30 corrisponde a 11110 in formato binario.

			Regole di accesso		
File	**ID del file**	**SFID**	**Leggi**	**Seleziona**	**Aggiorna**
DF Tachograph_G2			SC1	SC1	
EF Application_Identification	'0501h'	1	SC1	SC1	NEV
EF CardMA_Certificate	'C100h'	2	SC1	SC1	NEV
EF CardSignCertificate	'C101h'	3	SC1	SC1	NEV
EF CA_Certificate	'C108h'	4	SC1	SC1	NEV
EF Link_Certificate	'C109h'	5	SC1	SC1	NEV
EF Identification	'0520h'	6	SC1	SC1	NEV
EF Card_Download	'0509h'	7	SC1	SC1	SC1
EF Calibration	'050Ah'	10	SC1	SC1	SM-MAC-G2
EF Sensor_Installation_Data	'050Bh'	11	**SC5**	SM-MAC-G2	NEV
EF Events_Data	'0502h'	12	SC1	SC1	SM-MAC-G2
EF Faults_Data	'0503h'	13	SC1	SC1	SM-MAC-G2
EF Driver_Activity_Data	'0504h'	14	SC1	SC1	SM-MAC-G2
EF Vehicles_Used	'0505h'	15	SC1	SC1	SM-MAC-G2
EF Places	'0506h'	16	SC1	SC1	SM-MAC-G2
EF Current_Usage	'0507h'	17	SC1	SC1	SM-MAC-G2
EF Control_Activity_Data	'0508h'	18	SC1	SC1	SM-MAC-G2
EF Specific_Conditions	'0522h'	19	SC1	SC1	SM-MAC-G2
EF VehicleUnits_Used	'0523h'	20	SC1	SC1	SM-MAC-G2
EF GNSS_Places	'0524h'	21	SC1	SC1	SM-MAC-G2

▼B

Nella tabella a seguire si usano le seguenti abbreviazioni per le condizioni di sicurezza:

SC1 ALW OR SM-MAC-G2

SC5 Per il comando Read Binary con byte INS pari: SM-C-MAC-G2 AND SM-R-ENC-MAC-G2

Per il comando Read Binary con byte INS dispari (se supportato): NEV

TCS_161 Le strutture di tutti gli EF devono essere trasparenti.

TCS_162 L'applicazione della carta dell'officina di seconda generazione deve avere la seguente struttura dei dati:

File / Elemento di dati	Numero di registrazioni	Dimensioni (byte) Min.	Max.	Valori standard
DF Tachograph_G2		*17837*	*47163*	
EF Application_Identification		*17*	*17*	
WorkshopCardApplicationIdentification		*17*	*17*	
typeOfTachographCardId		1	1	{00}
cardStructureVersion		2	2	{00 00}
noOfEventsPerType		1	1	{00}
noOfFaultsPerType		1	1	{00}
activityStructureLength		2	2	{00 00}
noOfCardVehicleRecords		2	2	{00 00}
noOfCardPlaceRecords		2	2	{00}
noOfCalibrationRecords		2	2	{00}
noOfGNSSCDRecords		2	2	{00..00}
noOfSpecificConditionRecords		2	2	{00..00}
EF CardMA_Certificate		*204*	*341*	
CardMACertificate		204	341	{00..00}
EF CardSignCertificate		*204*	*341*	
CardSignCertificate		204	341	{00..00}
EF CA_Certificate		*204*	*341*	
MemberStateCertificate		204	341	{00..00}
EF Link_Certificate		*204*	*341*	
LinkCertificate		204	341	{00..00}
EF Identification		*211*	*211*	
CardIdentification		*65*	*65*	
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
cardIssuingAuthorityName		36	36	{00, 20..20}
cardIssueDate		4	4	{00..00}
cardValidityBegin		4	4	{00..00}
cardExpiryDate		4	4	{00..00}
WorkshopCardHolderIdentification		*146*	*146*	
workshopName		36	36	{00, 20..20}
workshopAddress		36	36	{00, 20..20}
cardHolderName				
holderSurname		36	36	{00, 20..20}
holderFirstNames		36	36	{00, 20..20}
cardHolderPreferredLanguage		2	2	{20 20}
EF Card_Download		*2*	*2*	
NoOfCalibrationsSinceDownload		2	2	{00 00}
EF Calibration		*14788*	*42844*	
WorkshopCardCalibrationData		*14788*	*42844*	
calibrationTotalNumber		2	2	{00 00}
calibrationPointerNewestRecord		2	2	{00}
calibrationRecords		*14784*	*42840*	
WorkshopCardCalibrationRecord	n_5	*168*	*168*	
calibrationPurpose		1	1	{00}
vehicleIdentificationNumber		17	17	{20..20}
vehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
wVehicleCharacteristicConstant		2	2	{00 00}
kConstantOfRecordingEquipment		2	2	{00 00}
lTyreCircumference		2	2	{00 00}
tyreSize		15	15	{20..20}
authorisedSpeed		1	1	{00}
oldOdometerValue		3	3	{00..00}
newOdometerValue		3	3	{00..00}

▼B

oldTimeValue		4	4	{00..00}
newTimeValue		4	4	{00..00}
nextCalibrationDate		4	4	{00..00}
vuPartNumber		16	16	{20..20}
vuSerialNumber		8	8	{00..00}
sensorSerialNumber		8	8	{00..00}
sensorGNSSSerialNumber		8	8	{00..00}
rcmSerialNumber		8	8	{00..00}
vuAbility		1	1	{00}
sealDataCard		46	46	
noOfSealRecords		1	1	{00}
SealRecords		45	45	
SealRecord	5	9	9	
equipmentType		1	1	{00}
extendedSealIdentifier		8	8	{00..00}
EF Sensor_Installation_Data		*18*	*102*	
SensorInstallationSecData		18	102	{00..00}
EF Events_Data		*792*	*792*	
CardEventData		*792*	*792*	
cardEventRecords	11	*72*	*72*	
CardEventRecord	n_1	*24*	*24*	
eventType		1	1	{00}
eventBeginTime		4	4	{00..00}
eventEndTime		4	4	{00..00}
eventVehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
EF Faults_Data		*288*	*288*	
CardFaultData		*288*	*288*	
cardFaultRecords	2	*144*	*144*	
CardFaultRecord	n_2	*24*	*24*	
faultType		1	1	{00}
faultBeginTime		4	4	{00..00}
faultEndTime		4	4	{00..00}
faultVehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
EF Driver_Activity_Data		*202*	*496*	
CardDriverActivity		*202*	*496*	
activityPointerOldestDayRecord		2	2	{00 00}
activityPointerNewestRecord		2	2	{00 00}
activityDailyRecords	n_6	198	492	{00..00}
EF Vehicles_Used		*194*	*386*	
CardVehiclesUsed		*194*	*386*	
vehiclePointerNewestRecord		2	2	{00 00}
cardVehicleRecords		*192*	*384*	
CardVehicleRecord	n_3	*48*	*48*	
vehicleOdometerBegin		3	3	{00..00}
vehicleOdometerEnd		3	3	{00..00}
vehicleFirstUse		4	4	{00..00}
vehicleLastUse		4	4	{00..00}
vehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
vuDataBlockCounter		2	2	{00 00}
vehicleIdentificationNumber		*17*	17	{20..20}
EF Places		*128*	*170*	

▼B

└CardPlaceDailyWorkPeriod		*128*	*170*	
├placePointerNewestRecord		2	2	{00 00}
└placeRecords		*126*	*168*	
└PlaceRecord	n_4	*21*	*21*	
├entryTime		4	4	{00..00}
├entryTypeDailyWorkPeriod		1	1	{00}
├dailyWorkPeriodCountry		1	1	{00}
├dailyWorkPeriodRegion		1	1	{00}
├vehicleOdometerValue		3	3	{00..00}
└entryGNSSPlaceRecord		11	11	{00..00}
├timeStamp		4	4	{00..00}
├gnssAccuracy		1	1	{00}
└geoCoordinates		6	6	{00..00}
EF Current_Usage		*19*	*19*	
└CardCurrentUse		*19*	*19*	
├sessionOpenTime		4	4	{00..00}
└sessionOpenVehicle				
├vehicleRegistrationNation		1	1	{00}
└vehicleRegistrationNumber		14	14	{00, 20..20}
EF Control_Activity_Data		*46*	*46*	
└CardControlActivityDataRecord		*46*	*46*	
├controlType		1	1	{00}
├controlTime		4	4	{00..00}
├controlCardNumber				
├cardType		1	1	{00}
├cardIssuingMemberState		1	1	{00}
└cardNumber		16	16	{20..20}
├controlVehicleRegistration				
├vehicleRegistrationNation		1	1	{00}
└vehicleRegistrationNumber		14	14	{00, 20..20}
├controlDownloadPeriodBegin		4	4	{00..00}
└controlDownloadPeriodEnd		4	4	{00..00}
EF VehicleUnits_Used		*42*	*42*	
└CardVehicleUnitsUsed		*42*	*82*	
├vehicleUnitPointerNewestRecord		2	2	{00 00}
└cardVehicleUnitRecords		*40*	*80*	
└CardVehicleUnitRecord	n_7	*10*	*10*	
├timeStamp		4	4	{00..00}
├manufacturerCode		1	1	{00..00}
├deviceID		1	1	{00..00}
└vuSoftwareVersion		4	4	{00..00}
EF GNSS_Places		*262*	*362*	
└GNSSContinuousDriving		*262*	*362*	
├gnssCDPointerNewestRecord		2	2	{00 00}
└gnssContinuousDrivingRecords		*260*	*360*	
└GNSSContinuousDrivingRecord	n_8	*15*	*15*	
├timeStamp		4	4	{00..00}
└gnssPlaceRecord		11	11	
├timeStamp		4	4	{00..00}
├gnssAccuracy		1	1	{00}
└geoCoordinates		6	6	{00..00}
EF Specific_Conditions		*12*	*22*	
└SpecificConditions		*12*	*22*	
├conditionPointerNewestRecord		2	2	{00 00}
└specificConditionRecords		10	20	
└SpecificConditionRecord	n_9	*5*	*5*	
├entryTime		4	4	{00..00}
└specificConditionType		1	1	{00}

▼B

TCS_163 I valori sotto indicati, usati per fornire le dimensioni nella tabella precedente, sono i valori minimo e massimo del numero di registrazioni che la struttura dei dati della carta dell'officina deve utilizzare per un'applicazione di seconda generazione:

		Min.	Max.
n_1	NoOfEventsPerType	3	3
n_2	NoOfFaultsPerType	6	6
n_3	NoOfCardVehicleRecords	4	8
n_4	NoOfCardPlaceRecords	6	8
n_5	NoOfCalibrationRecords	88	255
n_6	CardActivityLengthRange	198 byte (1 giorno * 93 cambi di attività)	492 byte (1 giorno * 240 cambi di attività)
n_7	NoOfCardVehicleUnitRecords	4	8
n_8	NoOfGNSSCDRecords	18	24
n_9	NoOfSpecificConditionRecords	2	4

4.4. Applicazioni della carta di controllo

4.4.1 *Applicazione della carta di controllo di prima generazione*

TCS_164 Dopo la personalizzazione, l'applicazione della carta di controllo di prima generazione deve avere la struttura dei file e le regole di accesso permanenti a seguire.

		Regole di accesso		
File	**ID del file**	**Leggi**	**Seleziona**	**Aggiorna**
└─DF Tachograph	'0500h'			
├─EF Application_Identification	'0501h'	SC2	SC1	NEV
├─EF Card_Certificate	'C100h'	SC2	SC1	NEV
├─EF CA_Certificate	'C108h'	SC2	SC1	NEV
├─EF Identification	'0520h'	**SC6**	SC1	NEV
└─EF Controller_Activity_Data	'050Ch'	SC2	SC1	SC3

Nella tabella a seguire si usano le seguenti abbreviazioni per le condizioni di sicurezza:

SC1 ALW OR SM-MAC-G2

SC2 ALW OR SM-MAC-G1 OR SM-MAC-G2

SC3 SM-MAC-G1 OR SM-MAC-G2

SC6 EXT-AUT-G1 OR SM-MAC-G1 OR SM-MAC-G2

TCS_165 Le strutture di tutti gli EF devono essere trasparenti.

TCS_166 L'applicazione della carta di controllo di prima generazione deve avere la seguente struttura dei dati:

▼B

File / Elemento di dati	Numero di registrazioni	Dimensioni (byte) Min.	Max.	
DF Tachograph		*11186*	*24526*	
EF Application_Identification		*5*	*5*	
ControlCardApplicationIdentification		*5*	*5*	
typeOfTachographCardId		1	1	{00}
cardStructureVersion		2	2	{00 00}
noOfControlActivityRecords		2	2	{00 00}
EF Card_Certificate		*194*	*194*	
CardCertificate		194	194	{00..00}
EF CA_Certificate		*194*	*194*	
MemberStateCertificate		194	194	{00..00}
EF Identification		*211*	*211*	
CardIdentification		*65*	*65*	
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
cardIssuingAuthorityName		36	36	{00, 20..20}
cardIssueDate		4	4	{00..00}
cardValidityBegin		4	4	{00..00}
cardExpiryDate		4	4	{00..00}
ControlCardHolderIdentification		*146*	*146*	
controlBodyName		36	36	{00, 20..20}
controlBodyAddress		36	36	{00, 20..20}
cardHolderName				
holderSurname		36	36	{00, 20..20}
holderFirstNames		36	36	{00, 20..20}
cardHolderPreferredLanguage		2	2	{20 20}
EF Controller_Activity_Data		*10582*	*23922*	
ControlCardControlActivityData		*10582*	*23922*	
controlPointerNewestRecord		2	2	{00 00}
controlActivityRecords		*10580*	*23920*	
controlActivityRecord	n_7	*46*	*46*	
controlType		1	1	{00}
controlTime		4	4	{00..00}
controlledCardNumber				
cardType		1	1	{00}
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
controlledVehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
controlDownloadPeriodBegin		4	4	{00..00}
controlDownloadPeriodEnd		4	4	{00..00}

TCS_167 I valori sotto indicati, usati per fornire le dimensioni nella tabella precedente, sono i valori minimo e massimo del numero di registrazioni che la struttura dei dati della carta di controllo deve utilizzare per un'applicazione di prima generazione:

		Min.	Max
n_7	NoOfControlActivityRecords	230	520

4.4.2 *Applicazione della carta di controllo di seconda generazione*

TCS_168 Dopo la personalizzazione, l'applicazione della carta di controllo di seconda generazione deve avere la struttura dei file e le regole di accesso permanenti a seguire.

Nota: l'identificativo breve dell'EF SFID è indicato come numero decimale: ad esempio, il valore 30 corrisponde a 11110 in formato binario.

▼B

File	ID del file	SFID	Regole di accesso	
			Leggi/seleziona	Aggiorna
└─DF Tachograph_G2			SC1	
├─EF Application_Identification	'0501h'	1	SC1	NEV
├─EF CardMA_Certificate	'C100h'	2	SC1	NEV
├─EF CA_Certificate	'C108h'	4	SC1	NEV
├─EF Link_Certificate	'C109h'	5	SC1	NEV
├─EF Identification	'0520h'	6	SC1	NEV
└─EF Controller_Activity_Data	'050Ch'	14	SC1	SM-MAC-G2

Nella tabella a seguire si usa la seguente abbreviazione per le condizioni di sicurezza:

SC1 ALW OR SM-MAC-G2

TCS_169 Le strutture di tutti gli EF devono essere trasparenti.

TCS_170 L'applicazione della carta di controllo di seconda generazione deve avere la seguente struttura dei dati:

File / Elemento di dati	Numero di registrazioni	Dimensioni (byte) Min.	Max.	
└─DF Tachograph_G2		*11410*	*25161*	
├─EF Application_Identification		*5*	*5*	
│ └─ControlCardApplicationIdentification		*5*	*5*	
│ ├─typeOfTachographCardId		1	1	{00}
│ ├─cardStructureVersion		2	2	{00 00}
│ └─noOfControlActivityRecords		2	2	{00 00}
├─EF CardMA_Certificate		*204*	*341*	
│ └─CardMACertificate		204	341	{00..00}
├─EF CA_Certificate		*204*	*341*	
│ └─MemberStateCertificate		204	341	{00..00}
├─EF Link_Certificate		*204*	*341*	
│ └─LinkCertificate		204	341	{00..00}
├─EF Identification		*211*	*211*	
│ ├─CardIdentification		*65*	*65*	
│ │ ├─cardIssuingMemberState		1	1	{00}
│ │ ├─cardNumber		16	16	{20..20}
│ │ ├─cardIssuingAuthorityName		36	36	{00, 20..20}
│ │ ├─cardIssueDate		4	4	{00..00}
│ │ ├─cardValidityBegin		4	4	{00..00}
│ │ └─cardExpiryDate		4	4	{00..00}
│ └─ControlCardHolderIdentification		*146*	*146*	
│ ├─controlBodyName		36	36	{00, 20..20}
│ ├─controlBodyAddress		36	36	{00, 20..20}
│ ├─cardHolderName				
│ │ ├─holderSurname		36	36	{00, 20..20}
│ │ └─holderFirstNames		36	36	{00, 20..20}
│ └─cardHolderPreferredLanguage		2	2	{20 20}
└─EF Controller_Activity_Data		*10582*	*23922*	
└─ControlCardControlActivityData		*10582*	*23922*	
├─controlPointerNewestRecord		2	2	{00 00}
└─controlActivityRecords		*10580*	*23920*	
└─controlActivityRecord	n_7	*46*	*46*	
├─controlType		1	1	{00}
├─controlTime		4	4	{00..00}
├─controlledCardNumber				
│ ├─cardType		1	1	{00}
│ ├─cardIssuingMemberState		1	1	{00}
│ └─cardNumber		16	16	{20..20}
├─controlledVehicleRegistration				
│ ├─vehicleRegistrationNation		1	1	{00}
│ └─vehicleRegistrationNumber		14	14	{00, 20..20}
├─controlDownloadPeriodBegin		4	4	{00..00}
└─controlDownloadPeriodEnd		4	4	{00..00}

TCS_171 I valori sotto indicati, usati per fornire le dimensioni nella tabella precedente, sono i valori minimo e massimo del numero di registrazioni che la struttura dei dati della carta di controllo deve utilizzare per un'applicazione di seconda generazione:

▼B

		Min.	Max.
n_7	NoOfControlActivityRecords	230	520

4.5. **Applicazioni della carta dell'azienda**

4.5.1 *Applicazione della carta dell'azienda di prima generazione*

TCS_172 Dopo la personalizzazione, l'applicazione della carta dell'azienda di prima generazione deve avere la struttura dei file e le regole di accesso permanenti a seguire.

		Regole di accesso		
File	**ID del file**	**Leggi**	**Seleziona**	**Aggiorna**
└DF Tachograph	'0500h'		SC1	
├EF Application_Identification	'0501h'	SC2	SC1	NEV
├EF Card_Certificate	'C100h'	SC2	SC1	NEV
├EF CA_Certificate	'C108h'	SC2	SC1	NEV
├EF Identification	'0520h'	**SC6**	SC1	NEV
└EF Company_Activity_Data	'050Dh'	SC2	SC1	SC3

Nella tabella a seguire si usano le seguenti abbreviazioni per le condizioni di sicurezza:

SC1 ALW OR SM-MAC-G2

SC2 ALW OR SM-MAC-G1 OR SM-MAC-G2

SC3 SM-MAC-G1 OR SM-MAC-G2

SC6 EXT-AUT-G1 OR SM-MAC-G1 OR SM-MAC-G2

TCS_173 Le strutture di tutti gli EF devono essere trasparenti.

TCS_174 L'applicazione della carta dell'azienda di prima generazione deve avere la seguente struttura dei dati:

File / Elemento di dati	**Numero di registrazioni**	**Dimensioni (in byte) Min.**	**Max.**	**Valori standard**
└DF Tachograph		*11114*	*24454*	
├EF Application_Identification		*5*	*5*	
└CompanyCardApplicationIdentification		*5*	*5*	
├typeOfTachographCardId		1	1	{00}
├cardStructureVersion		2	2	{00 00}
└noOfCompanyActivityRecords		2	2	{00 00}
├EF Card_Certificate		*194*	*194*	
└CardCertificate		194	194	{00..00}
├EF CA_Certificate		*194*	*194*	
└MemberStateCertificate		194	194	{00..00}
├EF Identification		*139*	*139*	
├CardIdentification		*65*	*65*	
├cardIssuingMemberState		1	1	{00}
├cardNumber		16	16	{20..20}
├cardIssuingAuthorityName		36	36	{00, 20..20}
├cardIssueDate		4	4	{00..00}
├cardValidityBegin		4	4	{00..00}
└cardExpiryDate		4	4	{00..00}
└CompanyCardHolderIdentification		*74*	*74*	
├companyName		36	36	{00, 20..20}
├companyAddress		36	36	{00, 20..20}
└cardHolderPreferredLanguage		2	2	{20 20}
└EF Company_Activity_Data		*10582*	*23922*	
└CompanyActivityData		*10582*	*23922*	
├companyPointerNewestRecord		2	2	{00 00}
└companyActivityRecords		*10580*	*23920*	
└companyActivityRecord	n_8	*46*	*46*	
├companyActivityType		1	1	{00}
├companyActivityTime		4	4	{00..00}
├cardNumberInformation				
├cardType		1	1	{00}
├cardIssuingMemberState		1	1	{00}
└cardNumber		16	16	{20..20}
├vehicleRegistrationInformation				
├vehicleRegistrationNation		1	1	{00}
└vehicleRegistrationNumber		14	14	{00, 20..20}
├downloadPeriodBegin		4	4	{00..00}
└downloadPeriodEnd		4	4	{00..00}

▼B

TCS_175 I valori sotto indicati, usati per fornire le dimensioni nella tabella precedente, sono i valori minimo e massimo del numero di registrazioni che la struttura dei dati della carta dell'azienda deve utilizzare per un'applicazione di prima generazione:

		Min.	Max.
n_8	NoOfCompanyActivityRecords	230	520

4.5.2 *Applicazione della carta dell'azienda di seconda generazione*

TCS_176 Dopo la personalizzazione, l'applicazione della carta dell'azienda di seconda generazione deve avere la struttura dei file e le regole di accesso permanenti a seguire.

Nota: l'identificativo breve dell'EF SFID è indicato come numero decimale: ad esempio, il valore 30 corrisponde a 11110 in formato binario.

			Regole di accesso	
File	**ID del file**	**SFID**	**Leggi/seleziona**	**Aggiorna**
└DF Tachograph_G2			SC1	
├EF Application_Identification	'0501h'	1	SC1	NEV
├EF CardMA_Certificate	'C100h'	2	SC1	NEV
├EF CA_Certificate	'C108h'	4	SC1	NEV
├EF Link_Certificate	'C109h'	5	SC1	NEV
├EF Identification	'0520h'	6	SC1	NEV
└EF Company_Activity_Data	'050Dh'	14	SC1	SM-MAC-G2

Nella tabella a seguire si usa la seguente abbreviazione per le condizioni di sicurezza:

SC1 ALW OR SM-MAC-G2

TCS_177 Le strutture di tutti gli EF devono essere trasparenti.

TCS_178 L'applicazione della carta dell'azienda di seconda generazione deve avere la seguente struttura dei dati:

File / Elemento di dati	**Numero di registrazioni**	**Dimensioni (in byte) Min.**	**Max.**	**Valori standard**
└DF Tachograph_G2		*11338*	*25089*	
├EF Application_Identification		*5*	*5*	
└CompanyCardApplicationIdentification		*5*	*5*	
├typeOfTachographCardId		1	1	{00}
├cardStructureVersion		2	2	{00 00}
└noOfCompanyActivityRecords		2	2	{00 00}
├EF CardMA_Certificate		*204*	*341*	
└CardMACertificate		204	341	{00..00}
├EF CA_Certificate		*204*	*341*	
└MemberStateCertificate		204	341	{00..00}
├EF Link_Certificate		*204*	*341*	
└LinkCertificate		204	341	{00..00}
├EF Identification		*139*	*139*	
├CardIdentification		*65*	*65*	
├cardIssuingMemberState		1	1	{00}
├cardNumber		16	16	{20..20}
├cardIssuingAuthorityName		36	36	{00, 20..20}
├cardIssueDate		4	4	{00..00}
├cardValidityBegin		4	4	{00..00}
└cardExpiryDate		4	4	{00..00}
└CompanyCardHolderIdentification		*74*	*74*	
├companyName		36	36	{00, 20..20}
├companyAddress		36	36	{00, 20..20}
└cardHolderPreferredLanguage		2	2	{20 20}
├EF Company_Activity_Data		*10582*	*23922*	
└CompanyActivityData		*10582*	*23922*	
├companyPointerNewestRecord		2	2	{00 00}
└companyActivityRecords		*10580*	*23920*	
└companyActivityRecord	n_8	*46*	*46*	
├companyActivityType		1	1	{00}
├companyActivityTime		4	4	{00..00}
├cardNumberInformation				
├cardType		1	1	{00}
├cardIssuingMemberState		1	1	{00}
└cardNumber		16	16	{20..20}
├vehicleRegistrationInformation				
├vehicleRegistrationNation		1	1	{00}
└vehicleRegistrationNumber		14	14	{00, 20..20}
├downloadPeriodBegin		4	4	{00..00}
└downloadPeriodEnd		4	4	{00..00}

▼B

TCS_179 I valori sotto indicati, usati per fornire le dimensioni nella tabella precedente, sono i valori minimo e massimo del numero di registrazioni che la struttura dei dati della carta dell'azienda deve utilizzare per un'applicazione di seconda generazione:

		Min.	Max.
n_8	NoOfCompanyActivityRecords	230	520

▼B

Appendice 3

PITTOGRAMMI

PIC_001 Il tachigrafo può usare facoltativamente i pittogrammi e le combinazioni di pittogrammi seguenti (o pittogrammi e combinazioni di pittogrammi sufficientemente simili da essere identificati senza ambiguità con essi):

1. PITTOGRAMMI DI BASE

	Persone	**Azioni**	**Modalità di funzionamento**
	Azienda		Modalità azienda
	Controllore	Controllo	Modalità controllo
	Conducente	Guida	Modalità funzionamento
	Officina/centro di prova	Controllo/taratura	Modalità taratura
	Fabbricante		

	Attività	**Durata**
	Disponibile	Periodo di disponibilità in corso
	Guida	Periodo di guida continuo
	Riposo	Periodo di riposo in corso
	Altra attività	Periodo di lavoro in corso
	Interruzione	Periodo cumulato di interruzione
	Sconosciuto	

	Apparecchio	**Funzioni**
	Sede (slot) del conducente	
	Sede (slot) del secondo conducente	
	Carta	
	Orologio	
	Dispositivo di visualizzazione	Visualizzazione
	Memoria esterna	Trasferimento dati
	Alimentazione	
	Stampante/stampa	Stampa
	Sensore	
	Dimensioni pneumatici	
	Veicolo/unità elettronica di bordo	
	Dispositivo GNSS	
	Dispositivo di diagnosi remota	
	Interfaccia ITS	

▼B

Condizioni particolari

OUT	Escluso dal campo di applicazione
	Attraversamento mediante traghetto/treno

Varie

	Anomalie		Guasti
	Inizio del periodo di lavoro giornaliero		Termine del periodo di lavoro giornaliero
	Posizione		
M	Immissione manuale delle attività del conducente		
	Sicurezza		
	Velocità		
	Ora		
Σ	Totale/riepilogo		

Indicatori

24h	Giornaliero
I	Settimanale
II	Quindicinale
+	Da/a

2. COMBINAZIONI DI PITTOGRAMMI

Varie

+	Luogo di controllo		
+	Luogo in cui inizia il periodo di lavoro giornaliero	+	Luogo in cui termina il periodo di lavoro giornaliero
+	Dalle ore	+	Alle ore
+	Dal veicolo		
OUT+	Escluso dal campo di applicazione — Inizio	+OUT	Escluso dal campo di applicazione — Fine

Carte

	Carta del conducente
	Carta dell'azienda
	Carta di controllo
	Carta dell'officina
– – –	Carta assente

Guida

	Guida con equipaggio
I	Periodo di guida di una settimana
II	Periodo di guida di due settimane

▼B

	Stampe
24h	Stampa giornaliera delle attività del conducente contenute nella carta
24h	Stampa giornaliera delle attività del conducente contenute nella VU
	Stampa di anomalie e guasti contenuti nella carta
	Stampa di anomalie e guasti contenuti nella VU
	Stampa dei dati tecnici
	Stampa dei superamenti di velocità
	Anomalie
	Inserimento di una carta non valida
	Conflitto di carte
	Sovrapposizione di orari
	Guida in assenza di una carta adeguata
	Inserimento carta durante la guida
	Chiusura errata ultima sessione carta
	Superamento di velocità
	Interruzione dell'alimentazione di energia
	Errore dei dati di movimento
	Dati contrastanti sul movimento del veicolo
	Violazione della sicurezza
	Regolazione dell'ora (in officina)
	Controllo superamento di velocità
	Guasti
1	Guasto della carta (slot del conducente)
2	Guasto della carta (slot del secondo conducente)
	Guasto del dispositivo di visualizzazione
	Guasto nel trasferimento di dati
	Guasto della stampante
	Guasto del sensore
	Guasto interno della VU
	Guasto del GNSS
	Guasto del dispositivo di diagnosi remota
	Procedura di immissione manuale
?	Stesso periodo di lavoro giornaliero?
?	Termine del periodo di lavoro precedente?
?	Conferma o immissione del luogo in cui termina il periodo di lavoro
?	Immissione ora di inizio
?	Immissione del luogo in cui inizia il periodo di lavoro

Nota: nell'appendice 4 sono definite alcune combinazioni di pittogrammi supplementari per creare blocchi di stampa o identificazioni delle registrazioni.

▼B

Appendice 4

STAMPE

INDICE

1. DATI GENERALI

2. SPECIFICHE DEI BLOCCHI DI DATI

3. SPECIFICHE DELLE STAMPE

3.1. Stampa giornaliera delle attività del conducente contenute nella carta

3.2. Stampa giornaliera delle attività del conducente contenute nella VU

3.3. Stampa di anomalie e guasti contenuti nella carta

3.4. Stampa di anomalie e guasti contenuti nella VU

3.5. Stampa dei dati tecnici

3.6. Stampa dei superamenti di velocità

3.7. Cronologia delle carte inserite

1. DATI GENERALI

Ogni stampa è realizzata mediante il concatenamento di diversi blocchi di dati, possibilmente identificati da un identificativo di blocco.

Un blocco di dati contiene una o più registrazioni, possibilmente identificate da un identificativo di registrazione.

PRT_001 Se un identificativo di blocco precede direttamente un identificativo di registrazione, quest'ultima non viene stampata.

PRT_002 Nel caso in cui un elemento di dati non sia noto, o non debba essere stampato per motivi riguardanti i diritti di accesso ai dati, al suo posto vengono stampati degli spazi.

PRT_003 Se il contenuto di un'intera riga non è noto, o non deve essere stampato, la riga viene omessa.

PRT_004 I campi contenenti dati numerici sono stampati con l'allineamento a destra, con le migliaia e i milioni separati da uno spazio e senza zeri iniziali.

PRT_005 I campi contenenti stringhe di dati sono stampati con l'allineamento a sinistra e riempiti da spazi fino a coprire l'intera lunghezza dell'elemento di dati o, se necessario, troncati in corrispondenza di tale lunghezza (nomi e indirizzi).

PRT_006 Nel caso in cui sia necessaria una interruzione di riga poiché il testo è troppo lungo, è necessario stampare un carattere speciale (punto mediano, «•») come primo carattere della nuova riga.

2. SPECIFICHE DEI BLOCCHI DI DATI

Nel presente capitolo sono state usate le seguenti convenzioni tipografiche:

— i caratteri in **grassetto** indicano il testo normale da stampare (nella stampa non saranno in grassetto),

▼B

— i caratteri normali indicano le variabili (pittogrammi o dati), che nella stampa saranno sostituiti con i rispettivi valori,

— i nomi delle variabili sono integrati da una sequenza di trattini bassi che indicano la lunghezza dell'elemento di dati disponibile per la variabile,

— le date sono indicate nel formato «dd/mm/yyyy» (giorno, mese, anno); si può anche usare il formato «dd.mm.yyyy»,

— l'espressione «identificazione della carta» («card identification») indica un elemento composto da: una combinazione di pittogrammi della carta che indicano il tipo di carta, il codice dello Stato membro che ha rilasciato la carta, una barra e il numero della carta con i codici di sostituzione e di rinnovo separati da uno spazio:

P	■	x	x	x	/	x	x	x	x	x	x	x	x	x	x	x	x	x		x		x
Combinazione di pittogrammi della carta		Codice dello Stato membro di rilascio				Primi 14 caratteri del numero della carta (possibilmente comprendente un codice di serie)														Codice di sostituzione		Codice di rinnovo

▼B

PRT_007 Le stampe usano i blocchi e/o le registrazioni di dati sotto riportati, in base ai significati e formati seguenti:

Numero di blocco o di registrazione Significato	Data Format
1 ***Data e ora di stampa documento***	▼ dd/mm/yyyy hh:mm **(UTC)**
2 ***Tipo di stampa*** Identificativo di blocco Combinazione di pittogrammi stampati (cfr. app. 3), regolazione del limitatore di velocità (solo per la stampa dei superamenti di velocità)	----------▼---------- Picto xxx **km/h**
3 ***Identificazione del titolare della carta*** Identificativo di blocco P = pittogramma di persone Cognome del titolare della carta Eventuale nome o nomi del titolare della carta Identificazione della carta Eventuale data di termine di validità della carta e numero di generazione (GEN 1 o GEN 2) (*)	----------P---------- P Last_Name_____ First_Name_____ Card_Identification_____ dd/mm/yyyy - GEN 2

Una carta di tipo non personale su cui non figuri il cognome del titolare deve riportare il nome dell'impresa o dell'officina o dell'organismo di controllo.

(*) Il numero di generazione della carta può essere stampato soltanto dai tachigrafi intelligenti.

4 ***Identificazione del veicolo*** Identificativo di blocco VIN Stato membro di immatricolazione e VRN	----------▲---------- ▲ VIN_____ Nat/VRN_____
5 ***Identificazione della VU*** Identificativo di blocco Nome del fabbricante della VU Codice componente della VU Numero di generazione della VU (*)	----------▣---------- ▣ VU_Manufacturer_____ VU_Part_Number__ GEN 2

(*) Il numero di generazione della carta può essere stampato soltanto dai tachigrafi intelligenti.

6 ***Ultima taratura del tachigrafo*** Identificativo di blocco Nome dell'officina Identificazione della carta dell'officina Data della taratura	----------T---------- T Last_Name_____ Card_Identification_____ T dd/mm/yyyy

▼B

7 ***Ultimo controllo (da parte di un agente incaricato)***

Identificativo di blocco

Identificazione della carta dell'agente

Data, ora e tipo di controllo

```
----------▫----------
Card_Identification_____
▫ dd/mm/yyyy hh:mm ppppp
```

Tipo di controllo: fino a cinque pittogrammi. Il tipo di controllo può corrispondere a uno dei pittogrammi seguenti o a una combinazione degli stessi:

▪: trasferimento dei dati della carta, ↧: trasferimento dei dati della VU, ▼: stampa, ▫: visualizzazione, ↑: verifica della taratura su strada.

8 ***Attività del conducente registrate sulla carta in ordine cronologico***

Identificativo di blocco

Data di consultazione (giorno di calendario oggetto della stampa) + contatore di presenza giornaliera della carta

```
----------⊙----------
    dd/mm/yyyy  xxx
```

8a *Condizione "escluso dal campo di applicazione all'inizio del giorno in questione"* (lasciare in bianco se tale condizione non è attiva)

```
----------OUT----------
```

8.1 *Periodo in cui la carta non è stata inserita*

8.1a Identificativo di registrazione (inizio del periodo)

8.1b *Periodo sconosciuto* Ora di inizio, durata

8.1c *Attività inserita manualmente.*

Pittogramma di attività, ora di inizio, durata

```
  --------------------
?       hh:mm hhhmm
A       hh:mm hhhmm
```

8.2 *Inserimento della carta nella sede (slot) S*

Identificativo di registrazione; S = pittogramma della sede (slot)

Stato membro di immatricolazione del veicolo e VRN

Odometro del veicolo all'atto dell'inserimento della carta

```
  ---------S---------
▲ Nat/VRN___________
  x xxx xxx km
```

8.3 *Attività (quando la carta era inserita)*

Pittogramma di attività, ora di inizio, durata, situazione dell'equipaggio (pittogramma dell'equipaggio se EQUIPAGGIO, spazio bianco se SINGOLO).

```
A       hh:mm hhhmm ⊙⊙
```

8.3a Condizioni particolari. Ora di immissione, pittogramma della condizione particolare (o combinazione di pittogrammi)

```
        hh:mm ---pppp---
```

8.4 *Estrazione della carta*

Odometro del veicolo e distanza percorsa dall'ultimo inserimento della carta per il quale è noto l'odometro

```
  x xxx xxx km; x xxx km
```

9 ***Attività del conducente registrate nella VU per sede (slot) in ordine cronologico***

Identificativo di blocco

Data di consultazione (giorno di calendario oggetto della stampa)

Odometro del veicolo alle ore 00:00 e 24:00

```
----------⊙----------
       dd/mm/yyyy
x xxx xxx - x xxx xxx km
```

10 ***Attività registrate nella sede (slot) S***

Identificativo di blocco

```
----------S----------
```

10a *Condizione "escluso dal campo di applicazione all'inizio del giorno in questione"* (lasciare in bianco se tale condizione non è attiva)

```
----------OUT----------
```

10.1 *Periodo in cui nessuna carta è inserita nella sede (slot) S*

Identificativo di registrazione.

Nessuna carta inserita

Odometro del veicolo all'inizio del periodo

```
  --------------------
⊙▪---
  x xxx xxx km
```

10.2 *Inserimento della carta*

Identificativo di registrazione dell'inserimento carta

Cognome del conducente

```
  --------------------
⊙ Last_Name_____________
```

▼B

	Nome del conducente	First_Name_____
	Identificazione della carta del conducente	Card_Identification_____
	Eventuale data di termine di validità della carta e numero di generazione (GEN 1 o GEN 2) (*)	dd/mm/yyyy - GEN 2
	Stato membro di immatricolazione e numero di immatricolazione (VRN) del veicolo precedentemente usato	Nat/VRN_____
	Data e ora di estrazione della carta dal veicolo precedente	dd/mm/yyyy hh:mm
	Riga vuota	
	Odometro del veicolo all'atto dell'inserimento della carta, flag dell'immissione manuale delle attività del conducente (M = sì, spazio vuoto = no)	x xxx xxx km M
	Se la carta del conducente non è stata inserita il giorno per il quale è stata effettuata la stampa del documento, per il blocco 10.2 vengono usati i dati dell'odometro rilevati al momento dell'ultimo inserimento della carta disponibile prima del giorno i	
10.3	*Attività*	
	Pittogramma di attività, ora di inizio, durata, situazione dell'equipaggio (pittogramma dell'equipaggio se EQUIPAGGIO, spazio bianco se SINGOLO).	A hh:mm hhhmm ⊙⊙
10.3a	*Condizioni particolari*. Ora di immissione, pittogramma della condizione particolare (o combinazione di pittogrammi)	hh:mm ---pppp---
10.4	*Estrazione della carta o termine del periodo "carta non inserita"*	
	Odometro del veicolo all'atto dell'estrazione della carta o al termine del periodo "carta non inserita" e distanza percorsa a partire dall'inserimento o dall'inizio del periodo "carta non inserita".	x xxx xxx km; x xxx km

(*) Il numero di generazione della carta può essere stampato soltanto dai tachigrafi intelligenti.

11	***Riepilogo giornaliero***	
	Identificativo di blocco	----------Σ----------
11.1	***Riepilogo della VU dei periodi senza carta nella sede (slot) del conducente***	
	Identificativo di blocco	1⊙----
11.2	***Riepilogo della VU dei periodi senza carta nella sede (slot) del secondo conducente***	
	Identificativo di blocco	2⊙----
11.3	***Riepilogo giornaliero della VU per conducente***	
	Identificativo di registrazione	----------
	Cognome del conducente	⊙ Last_Name_____
	Nome del conducente	First_Name_____
	Identificazione della carta del conducente	Card_Identification_____
11.4	*Immissione del luogo in cui inizia e/o termina un periodo di lavoro giornaliero*	
	pi = pittogramma luogo di inizio / termine, ora, Stato, regione	pihh:mm Cou Reg
	Odometro	x xxx xxx km
11.5	*Immissione del luogo in cui inizia e/o termina un periodo di lavoro giornaliero*	
	e dopo 3 ore di periodo di guida continuo	hh:mm
	Odometro	x xxx xxx km
11.6	*Totali delle attività (registrate in una carta)*	
	Durata totale di guida, distanza percorsa	⊙ hhhmm x xxx km
	Durata totale lavoro e disponibilità	✻ hhhmm ⧈ hhhmm
	Durata totale riposo e periodi non noti	⊢ hhhmm ? hhhmm
	Durata totale delle attività dell'equipaggio	⊙⊙ hhhmm
11.7	*Totali delle attività [periodi senza carta nella sede (slot) del conducente]*	
	Durata totale di guida, distanza percorsa	⊙ hhhmm x xxx km
	Durata totale lavoro e disponibilità	✻ hhhmm ⧈ hhhmm
	Durata totale riposo	⊢ hhhmm

▼B

11.8	*Totali delle attività [periodi senza carta nella sede (slot) del secondo conducente]*	
	Durata totale lavoro e disponibilità	* hhhmm ⧈ hhhmm
	Durata totale riposo	⊢ hhhmm
11.9	*Totali delle attività [per conducente, comprese entrambe le sedi (slot)]*	
	Durata totale di guida, distanza percorsa	⊙ hhhmm x xxx km
	Durata totale lavoro e disponibilità	* hhhmm ⧈ hhhmm
	Durata totale riposo	⊢ hhhmm
	Durata totale delle attività dell'equipaggio	⊙⊙ hhhmm

Se si richiede una stampa giornaliera per il giorno in corso, le informazioni sul riepilogo giornaliero sono calcolate in base ai dati disponibili al momento della stampa.

12	***Anomalie e/o guasti memorizzati in una carta***	
12.1	Identificativo di blocco degli ultimi cinque "Anomalie e guasti" registrati sulla carta	----------!×▬----------
12.2	Identificativo di blocco di tutte le "Anomalie" registrate sulla carta	----------!▬----------
12.3	Identificativo di blocco di tutti i "Guasti" registrati sulla carta	----------×▬----------
12.4	*Registrazione di anomalie e/o guasti*	
	Identificativo di registrazione	----------
	Pittogramma anomalia/guasto, scopo della registrazione, data e ora di inizio	Pic (p) dd/mm/yyyy hh:mm
	Eventuale codice aggiuntivo anomalia/guasto, durata	!xx hhhmm
	Stato membro di immatricolazione e VRN del veicolo in cui si è verificata l'anomalia o il guasto	Nat/VRN_____

13	***Anomalie e/o guasti memorizzati o in corso nella VU***	
13.1	Identificativo di blocco degli ultimi cinque "Anomalie e guasti" registrati nella VU	----------!×▲----------
13.2	Identificativo di blocco di tutte le "Anomalie" registrate o in corso nella VU	----------!▲----------
13.3	Identificativo di blocco di tutti i "Guasti" memorizzati o in corso nella VU	----------×▲----------
13.4	*Registrazione di anomalie e/o guasti*	
	Identificativo di registrazione	----------
	Pittogramma anomalia/guasto, scopo della registrazione, data e ora di inizio	Pic (p) dd/mm/yyyy hh:mm
	Eventuale codice aggiuntivo anomalia/guasto, numero di anomalie analoghe nel giorno in questione, durata	!xx (xxx) hhhmm
	Identificazione delle carte inserite all'inizio o al termine dell'anomalia o guasto (massimo 4 righe senza ripetere gli stessi numeri di carta)	Card_Identification_____ Card_Identification_____ Card_Identification_____ Card_Identification_____
	Caso in cui non era inserita alcuna carta	▬---
	Dati specifici per ciascun fabbricante	< Literal><ErrorCode>

Lo scopo della registrazione (p) è un codice numerico che spiega il motivo della registrazione dell'anomalia o del guasto, codificato in base all'elemento di dati `EventFaultRecordPurpose`.

`Literal` è specifico del fabbricante di tachigrafi e comprende un massimo di 12 caratteri.

`ErrorCode` è un codice di errore specifico del fabbricante di tachigrafi e comprende un massimo di 12 caratteri.

▼B

14	***Identificazione della VU***	
	Identificativo di blocco	`----------B----------`
	Nome del fabbricante della VU	`B Name_____`
	Indirizzo del fabbricante della VU	`Address_____`
	Codice componente della VU	`PartNumber_____`
	Numero di omologazione della VU	`Apprv_____`
	Numero di serie della VU	`S/N_____`
	Anno di fabbricazione della VU	`yyyy`
	Versione software della VU e data di installazione	`V xxxx dd/mm/yyyy`
15	***Identificazione del sensore***	
	Identificativo di blocco	`----------Л----------`
15.1	*Registro degli accoppiamenti*	
	Numero di serie del sensore	`Л S/N_____`
	Numero di omologazione del sensore	`Apprv_____`
	Data di accoppiamento del sensore	`dd/mm/yyyy hh:mm`
16	*Identificazione del GNSS*	
	Identificativo di blocco	`----------▚----------`
16.1	*Registro degli accoppiamenti*	
	Numero di serie del dispositivo GNSS esterno	`▚ S/N_____`
	Numero di omologazione del dispositivo GNSS esterno	`Apprv_____`
	Data di accoppiamento del dispositivo GNSS esterno	`dd/mm/yyyy hh:mm`
17	***Dati di taratura***	
	Identificativo di blocco	`----------T----------`
17.1	*Registrazione della taratura*	
	Identificativo di registrazione	`--------------------`
	Officina che ha effettuato la taratura	`T Workshop_name_____`
	Indirizzo dell'officina	`Workshop_address_____`
	Identificazione della carta dell'officina	`Card_Identification_____`
	Data di scadenza della carta dell'officina	`dd/mm/yyyy`
	Riga vuota	
	Data della taratura + scopo della taratura	`T dd/mm/yyyy (p)`
	VIN	`A VIN_____`
	Stato membro di immatricolazione e VRN	`Nat/VRN_____`
	Coefficiente caratteristico del veicolo	`w xx xxx Imp/km`
	Costante dell'apparecchio di controllo	`k xx xxx Imp/km`
	Effective circumference of wheel tyres	`l xx xxx mm`
	Dimensione degli pneumatici montati	`e TyreSize_____`
	Regolazione del limitatore di velocità	`> xxx km/h`
	Valori dell'odometro vecchi e nuovi	`x xxx xxx - x xxx xxx km`

Lo scopo della taratura (p) è un codice numerico che spiega il motivo della registrazione di questi parametri di taratura, codificato in base all'elemento di dati `CalibrationPurpose`.

▼B

18	***Regolazione dell'ora***	
	Identificativo di blocco	`----------◷----------`
18.1	*Registrazione della regolazione dell'ora*	
	Identificativo di registrazione	`--------------------`
	Data e ora vecchie	`!◷ dd/mm/yyyy hh:mm`
	Data e ora nuove	`◷ dd/mm/yyyy hh:mm`
	Officina che ha effettuato la regolazione dell'ora	`T Workshop_name_____`
	Indirizzo dell'officina	`Workshop_address_____`
	Identificazione della carta dell'officina	`Card_Identification_____`
	Data di scadenza della carta dell'officina	`dd/mm/yyyy`
19	***Anomalia e guasto più recenti registrati nella VU***	
	Identificativo di blocco	`----------!×🕮----------`
	Data e ora dell'anomalia più recente	`! dd/mm/yyyy hh:mm`
	Data e ora del guasto più recente	`× dd/mm/yyyy hh:mm`
20	***Informazioni relative al controllo dei superamenti di velocità***	
	Identificativo di blocco	`----------»»----------`
	Data e ora dell'ultimo CONTROLLO SUPERAMENTO DI VELOCITÀ	`»▫dd/mm/yyyy hh:mm`
	Data/ora del primo superamento di velocità e numero di superamenti di velocità a partire da tale momento	`»»dd/mm/yyyy hh:mm (nnn)`
21	***Registrazione superamento di velocità***	
21.1	Identificativo di blocco "Primo superamento di velocità dopo l'ultima taratura"	`--------»»T---------`
21.2	Identificativo di blocco "Cinque superamenti più gravi nel corso degli ultimi 365 giorni"	`-------»»(365)------`
21.3	Identificativo di blocco "Superamento più grave per ciascuno degli ultimi 10 giorni in cui si è verificato un superamento"	`-------»»(10)-------`
21.4	Identificativo di registrazione	`--------------------`
	Data, ora e durata	`»»dd/mm/yyyy hh:mm hhhmm`
	Velocità massima e media, numero di anomalie analoghe nel giorno in questione	`xxx km/h xxx km/h(xxx)`
	Cognome del conducente	`◙ Last_Name_____`
	Nome del conducente	`First_Name_____`
	Identificazione della carta del conducente	`Card_Identification_____`
21.5	Se in un blocco non sono stati registrati superamenti di velocità	`»»---`
22	***Informazioni da inserire manualmente***	
	Identificativo di blocco	`------------------------`
22.1	Luogo del controllo	`▫• ..................`
22.2	Firma dell'agente incaricato del controllo	`▫ ..................`
22.3	Dalle ore	`◷→ ..................`
22.4	Alle ore	`→◷ ..................`
22.5	Firma del conducente	`◙ ..................`

"Informazioni da inserire manualmente": inserire un numero sufficiente di righe vuote sopra una voce da compilare a mano, per consentire la trascrizione effettiva delle informazioni richieste o per apporre una firma.

▼B

23 ***Carte più recenti inserite nella VU***

Identificativo di blocco

23.1 Carta inserita

Identificativo di registrazione

Tipo di carta, Generazione, Versione, Fabbricante (*)

Identificazione della carta

Numero di serie della carta

Data e ora dell'ultimo inserimento della carta

```
-------- ▯▮◔ --------


----
↑ <gen> <version> <MC>
Card Identification
Card Serial Number
dd/mm/yyyy hh:mm
```

(*) (tutto in una riga)

con

tipo di carta: pittogramma, un carattere + spazio

gen: GEN1 o GEN2, 4 caratteri + spazio

versione: fino a 10 caratteri

MC: codice del fabbricante, 3 caratteri

3. SPECIFICHE DELLE STAMPE

Nel presente capitolo sono state usate le seguenti convenzioni tipografiche:

N	Blocco di stampa o numero di registrazione N
N	Blocco di stampa o numero di registrazione N ripetuto tante volte quante necessario
X/Y	Blocchi di stampa o registrazioni X e/o Y, a seconda della necessità, ripetuti tante volte quante necessario

3.1. **Stampa giornaliera delle attività del conducente contenute nella carta**

PRT_008 La stampa giornaliera delle attività del conducente contenute nella carta deve rispettare il formato seguente:

1	Data e ora di stampa del documento
2	Tipo di stampa
3	Identificazione dell'agente incaricato del controllo (se nella VU è inserita una carta di controllo)
3	Identificazione del conducente (dalla carta cui si riferisce la stampa + GEN)
4	Identificazione del veicolo (veicolo da cui si ottiene la stampa)
5	Identificazione della VU (VU da cui si ottiene la stampa + GEN)
6	Ultima taratura di questa VU
7	Ultimo controllo cui è stato sottoposto il conducente
8	Delimitatore delle attività del conducente
8a	Condizione «escluso dal campo di applicazione» all'inizio del giorno in questione
8.1a / 8.1b / 8.1c / 8.2 / 8.3 / 8.3a / 8.4	Attività del conducente in ordine cronologico
11	Delimitatore del riepilogo giornaliero

▼B

11.4	Luoghi immessi in ordine cronologico
11.5	Dati GNSS
11.6	Totali delle attività
12.1	Anomalie o guasti dal delimitatore della carta
12.4	Registrazione di anomalie/guasti (ultimi 5 anomalie/guasti memorizzati sulla carta)
13.1	Anomalie o guasti dal delimitatore della VU
13.4	Registrazione di anomalie/guasti (ultimi 5 anomalie/guasti memorizzati o in corso nella VU)
22.1	Luogo del controllo
22.2	Firma dell'agente incaricato del controllo
22.5	Firma del conducente

3.2. **Stampa giornaliera delle attività del conducente contenute nella VU**

PRT_009 La stampa giornaliera delle attività del conducente contenute nella VU deve rispettare il formato seguente:

1	Data e ora di stampa del documento
2	Tipo di stampa
3	Identificazione del titolare della carta (per tutte le carte inserite nella VU + GEN)
4	Identificazione del veicolo (veicolo da cui si ottiene la stampa)
5	Identificazione della VU (VU da cui si ottiene la stampa + GEN)
6	Ultima taratura di questa VU
7	Ultimo controllo di questo tachigrafo
9	Delimitatore delle attività del conducente
10	Delimitatore della sede (slot) del conducente (slot 1)
10a	Condizione «escluso dal campo di applicazione» all'inizio del giorno in questione
10.1 / 10.2 / 10.3 /10.3a / 10.4	Attività in ordine cronologico [sede (slot) conducente]
10	Delimitatore della sede (slot) del secondo conducente (slot 2)
10a	Condizione «escluso dal campo di applicazione» all'inizio del giorno in questione
10.1 / 10.2 / 10.3 /10.3a / 10.4	Attività in ordine cronologico [sede (slot) secondo conducente]
11	Delimitatore del riepilogo giornaliero
11.1	Riepilogo dei periodi senza carta nella sede (slot) del conducente
11.4	Luoghi immessi in ordine cronologico
11.5	Dati GNSS

▼B

11.6	Totali delle attività
11.2	Riepilogo dei periodi senza carta nella sede (slot) del secondo conducente
11.4	Luoghi immessi in ordine cronologico
11.5	Dati GNSS
11.7	Totali delle attività
11.3	Riepilogo delle attività per un conducente, comprese entrambe le sedi (slot)
11.4	Luoghi immessi da tale conducente in ordine cronologico
11.5	Dati GNSS
11.8	Totali delle attività per questo conducente
13.1	Delimitatore di anomalie e guasti
12.4	Registrazione di anomalie/guasti (ultimi 5 anomalie/guasti memorizzati o in corso nella VU)
13.1	Luogo del controllo
22.2	Firma dell'agente incaricato del controllo
22.3	Dalle ore (spazio disponibile per consentire a un conducente senza carta di indicare quali periodi sono pertinenti per lui)
22.4	Alle ore
22.5	Firma del conducente

3.3. **Stampa di anomalie e guasti contenuti nella carta**

PRT_010 La stampa di anomalie e guasti contenuti nella carta deve rispettare il formato seguente:

1	Data e ora di stampa del documento
2	Tipo di stampa
3	Identificazione dell'agente incaricato del controllo (se una carta di controllo è inserita nella VU + GEN)
3	Identificazione del conducente (dalla carta cui si riferisce la stampa)
4	Identificazione del veicolo (veicolo da cui si ottiene la stampa)
12.2	Delimitatore delle anomalie
12.4	Registrazioni delle anomalie (tutte le anomalie memorizzate nella carta)
12.3	Delimitatore dei guasti
12.4	Registrazioni dei guasti (tutti i guasti memorizzati nella carta)
22.1	Luogo del controllo
22.2	Firma dell'agente incaricato del controllo
22.5	Firma del conducente

▼B

3.4. **Stampa di anomalie e guasti contenuti nella VU**

PRT_011 La stampa di anomalie e guasti contenuti nella VU deve rispettare il formato seguente:

1	Data e ora di stampa del documento
2	Tipo di stampa
3	Identificazione del titolare della carta (per tutte le carte inserite nella VU + GEN)
4	Identificazione del veicolo (veicolo da cui si ottiene la stampa)
13.2	Delimitatore delle anomalie
13.4	Registrazioni delle anomalie (tutte le anomalie memorizzate o in corso nella VU)
13.3	Delimitatore dei guasti
13.4	Registrazioni dei guasti (tutti i guasti memorizzati o in corso nella VU)
22.1	Luogo del controllo
22.2	Firma dell'agente incaricato del controllo
22.5	Firma del conducente

3.5. **Stampa dei dati tecnici**

PRT_012 La stampa dei dati tecnici deve rispettare il formato seguente:

1	Data e ora di stampa del documento
2	Tipo di stampa
3	Identificazione del titolare della carta (per tutte le carte inserite nella VU + GEN)
4	Identificazione del veicolo (veicolo da cui si ottiene la stampa)
14	Identificazione della VU
15	Identificazione del sensore
15.1	Dati di accoppiamento del sensore (tutti i dati disponibili in ordine cronologico)
16	Identificazione del GNSS
16.1	Dati di accoppiamento del dispositivo GNSS esterno (tutti i dati disponibili in ordine cronologico)
17	Delimitatore dei dati di taratura
17.1	Registrazioni delle tarature (tutte le registrazioni disponibili in ordine cronologico)
18	Delimitatore delle regolazioni dell'ora
18.1	Registrazioni delle regolazioni dell'ora (tutte le registrazioni disponibili per le regolazioni dell'ora e i dati di taratura)
19	Anomalia e guasto più recenti registrati nella VU

▼B

3.6. **Stampa dei superamenti di velocità**

PRT_013 La stampa dei superamenti di velocità deve rispettare il formato seguente:

1	Data e ora di stampa del documento
2	Tipo di stampa
3	Identificazione del titolare della carta (per tutte le carte inserite nella VU + GEN)
4	Identificazione del veicolo (veicolo da cui si ottiene la stampa)
20	Informazioni relative al controllo dei superamenti di velocità
21.1	Identificativo dei dati relativi ai superamenti di velocità
21.4 / 21.5	Primo superamento di velocità successivo all'ultima taratura
21.2	Identificativo dei dati relativi ai superamenti di velocità
21.4 / 21.5	I 5 superamenti di velocità più gravi nel corso degli ultimi 365 giorni
21.3	Identificativo dei dati relativi ai superamenti di velocità
21.4 / 21.5	Il superamento di velocità più grave per ciascuno degli ultimi 10 giorni in cui si è verificato
22.1	Luogo del controllo
22.2	Firma dell'agente incaricato del controllo
22.5	Firma del conducente

3.7. **Cronologia delle carte inserite**

PRT_014 La stampa della cronologia delle carte inserite deve rispettare il formato seguente:

1	Data e ora di stampa del documento
2	Tipo di stampa
3	Identificazione del titolare della carta (per tutte le carte inserite nella VU)
23	Carta più recente inserita nella VU
23.1	Carte inserite (fino a 88 registrazioni)
12.3	Delimitatore dei guasti

▼B

Appendice 5

DISPOSITIVO DI VISUALIZZAZIONE

Nella presente appendice sono state usate le seguenti convenzioni tipografiche:

— i caratteri in **grassetto** indicano il testo normale da visualizzare (nella visualizzazione non saranno in grassetto),

— i caratteri normali indicano le variabili (pittogrammi o dati) che nella visualizzazione saranno sostituiti con i rispettivi valori:

  — dd mm yyyy: giorno, mese, anno,

  — hh: ore,

  — mm: minuti,

  — D: pittogramma della durata,

  — EF: combinazione di pittogrammi relativi ad anomalie o guasti,

  — O: pittogramma della modalità di funzionamento.

DIS_001 Il tachigrafo deve visualizzare i dati nei formati seguenti:

Dati	Formato
Visualizzazione predefinita	
Ora locale	hh:mm
Modalità di funzionamento	O
Informazioni relative al conducente	1 Dhh**h**mm ▮▮hh**h**mm
Informazioni relative al secondo conducente	2 Dhh**h**mm
Condizione «Escluso dal campo di applicazione» attiva	OUT
Visualizzazione degli avvisi	
Superamento del periodo di guida continuo	1 ⊙ hh**h**mm ▮▮hh**h**mm
Anomalia o guasto	EF
Visualizzazione di altre informazioni	
Data UTC Ora	UTC ⊙ dd/mm/yyyy o UTC ⊙ dd.mm.yyyy hh:mm
Periodo di guida continuo e periodo cumulato di interruzione del conducente	1 ⊙ hh**h**mm ▮▮hh**h**mm
Periodo di guida continuo e periodo cumulato di interruzione del secondo conducente	2 ⊙ hh**h**mm ▮▮hh**h**mm
Periodo cumulato di guida del conducente per la settimana in corso e quella precedente	1 ⊙ ▮▮ hhh**h**mm
Periodo cumulato di guida del secondo conducente per la settimana in corso e quella precedente	2 ⊙ ▮▮ hhh**h**mm

▼B

Appendice 6

CONNETTORE ANTERIORE PER LA TARATURA E IL TRASFERIMENTO DEI DATI

INDICE

1. HARDWARE

1.1. Connettore

1.2. Distribuzione dei contatti

1.3. Schema elettrico

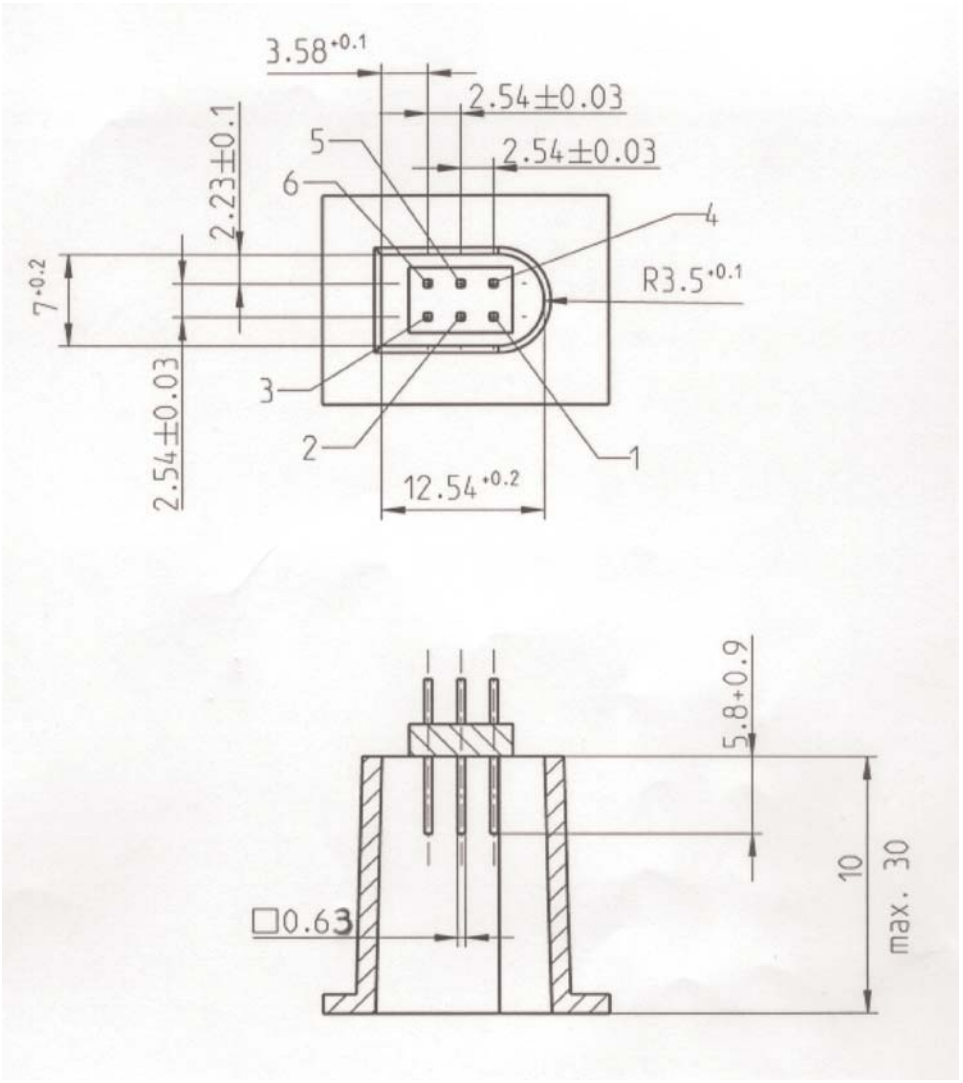
2. INTERFACCIA DI TRASFERIMENTO DATI

3. INTERFACCIA DI TARATURA

1. HARDWARE

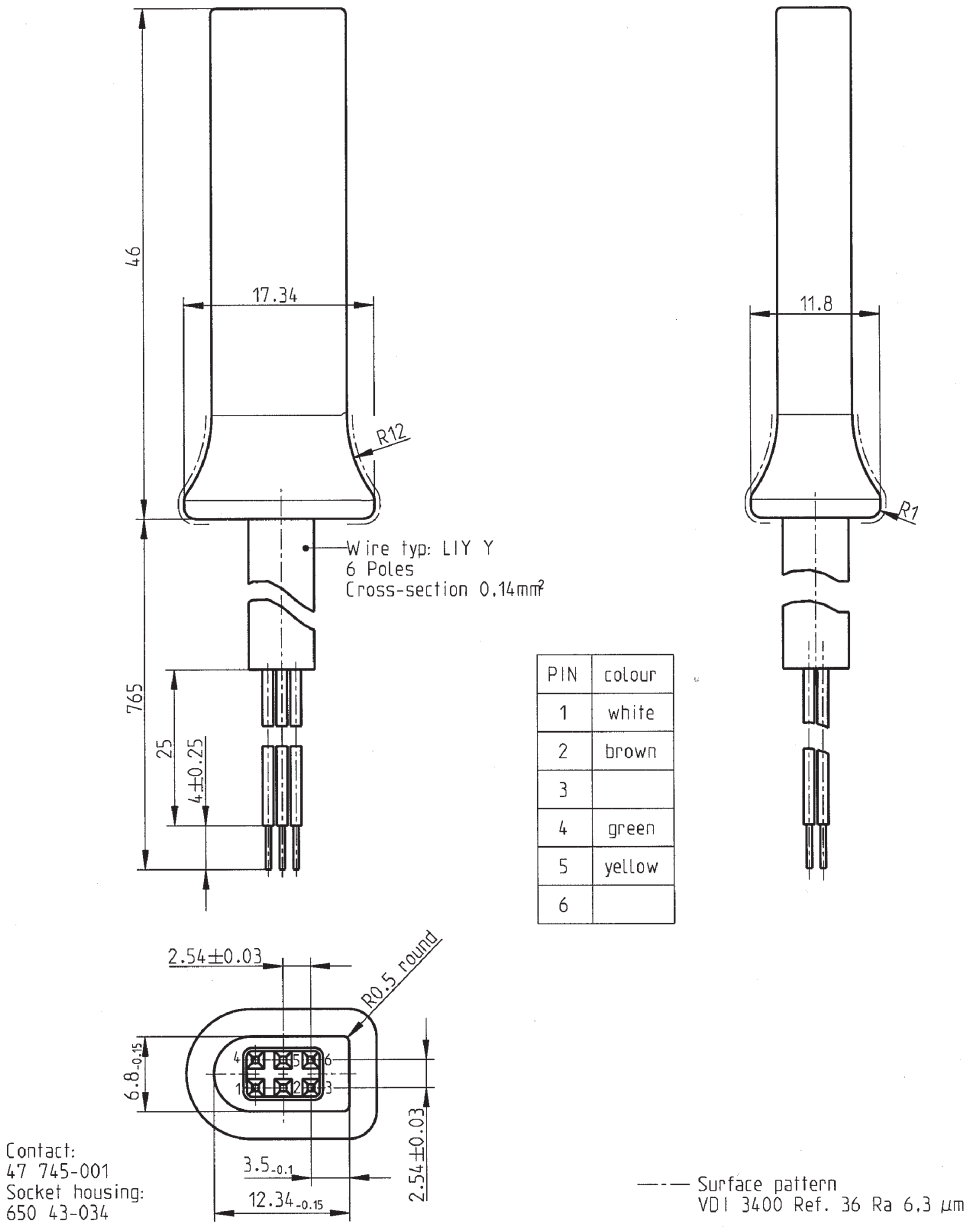
1.1. **Connettore**

INT_001 Il connettore per la taratura e il trasferimento dei dati deve essere un connettore a 6 pin, accessibile sul pannello anteriore senza necessità di smontare alcun elemento del tachigrafo e deve essere conforme al disegno seguente (tutte le dimensioni sono indicate in millimetri):



▼B

Il disegno seguente illustra un tipico connettore volante a 6 pin:



1.2. **Distribuzione dei contatti**

INT_002 I contatti devono essere distribuiti secondo la tabella seguente:

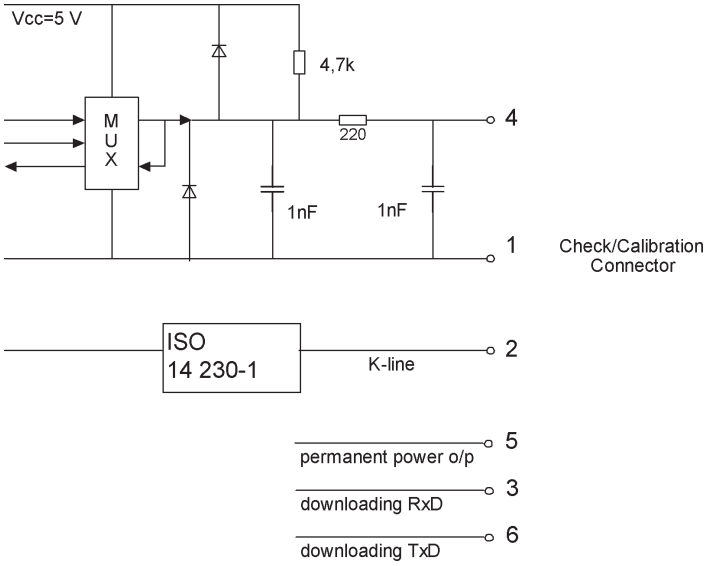
Pin	Descrizione	Osservazioni
1	Polo negativo batteria	Collegato al polo negativo della batteria del veicolo
2	Comunicazione di dati	Linea K (ISO 14230-1)
3	RxD — Trasferimento di dati	Ingresso dati del tachigrafo
4	Segnale di ingresso/uscita	Taratura

▼B

Pin	Descrizione	Osservazioni
5	Uscita di alimentazione permanente	Il campo di tensione deve essere quello dell'alimentazione elettrica del veicolo meno 3V per tenere conto della caduta di tensione nel circuito di protezione Uscita 40 mA
6	TxD — Trasferimento di dati	Uscita dati del tachigrafo

1.3. **Schema elettrico**

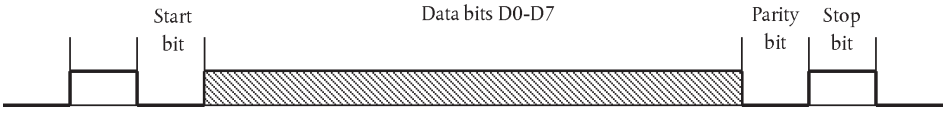
INT_003 Lo schema elettrico deve essere conforme a quello sotto riportato:



2. INTERFACCIA DI TRASFERIMENTO DATI

INT_004 L'interfaccia di trasferimento dati deve essere conforme alle specifiche RS232.

INT_005 L'interfaccia di trasferimento dati deve utilizzare un bit di avvio, 8 bit di dati con il bit meno significativo (LSB) per primo, un bit di parità pari e 1 bit di arresto.



Organizzazione dei byte di dati

Bit di avvio (start bit): un bit con livello logico 0;

Bit di dati (data bits): trasmessi con LSB per primo;

Bit di parità (parity bit): parità pari;

Bit di arresto (stop bit): un bit con livello logico 1.

In caso di trasmissione di dati numerici costituiti da più di un byte, il byte più significativo viene trasmesso per primo ed il byte meno significativo viene trasmesso per ultimo.

INT_006 La velocità di trasmissione deve avere un campo di regolazione compreso tra 9 600 bps e 115 200 bps. La trasmissione deve avvenire alla velocità di trasmissione più elevata possibile, con la velocità iniziale impostata su 9 600 bps dopo l'avvio della comunicazione.

▼B

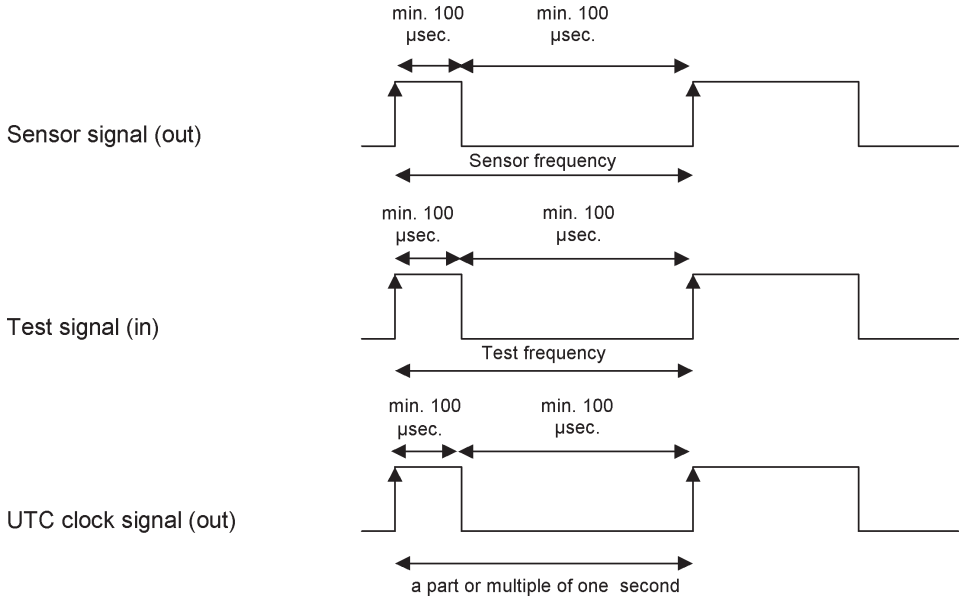
3. INTERFACCIA DI TARATURA

INT_007 La comunicazione di dati deve essere conforme alla norma ISO 14230-1, Road vehicles — Diagnostic systems — Keyword protocol 2000 — Part 1: Physical layer, First edition: 1999.

INT_008 Il segnale in ingresso (in)/uscita (out) deve essere conforme alle seguenti specifiche elettriche:

Parametro	Minimo	Tipico	Massimo	Osservazioni
U_{low} (in)			1,0 V	I = 750 µA
U_{high} (in)	4 V			I = 200 µA
Frequenza			4 kHz	
U_{low} (out)			1,0 V	I = 1 mA
U_{high} (out)	4 V			I = 1 mA

INT_009 Il segnale in ingresso (in)/uscita (out) deve essere conforme alle seguenti temporizzazioni:



▼B

Appendice 7

PROTOCOLLI DI TRASFERIMENTO DEI DATI

INDICE

1. INTRODUZIONE

1.1. Campo di applicazione

1.2. Acronimi e simboli

2. TRASFERIMENTO DEI DATI DA UNA VU

2.1. Procedura di trasferimento dei dati

2.2. Protocolli di trasferimento dei dati

2.2.1 Struttura dei messaggi

2.2.2 Tipi di messaggio

2.2.2.1 Richiesta di inizio comunicazione (SID 81)

2.2.2.2 Risposta positiva di inizio comunicazione (SID C1)

2.2.2.3 Richiesta di inizio sessione diagnostica (SID 10)

2.2.2.4 Risposta positiva di inizio sessione diagnostica (SID 50)

2.2.2.5 Servizio di controllo del collegamento (SID 87)

2.2.2.6 Risposta positiva di controllo del collegamento (SID C7)

2.2.2.7 Richiesta di invio dati (upload) (SID 35)

2.2.2.8 Risposta positiva di invio dati (upload) (SID 75)

2.2.2.9 Richiesta di trasferimento dati (SID 36)

2.2.2.10 Risposta positiva di trasferimento dati (SID 76)

2.2.2.11 Richiesta di chiusura trasferimento (SID 37)

2.2.2.12 Risposta positiva di richiesta chiusura trasferimento (SID 77)

2.2.2.13 Richiesta di termine comunicazione (SID 82)

2.2.2.14 Richiesta di risposta positiva di termine comunicazione (SID C2)

2.2.2.15 Riconoscimento sottomessaggio (SID 83)

2.2.2.16 Risposta negativa (SID 7F)

2.2.3 Flusso di messaggi

2.2.4 Temporizzazione

▼B

2.2.5 Gestione degli errori

2.2.5.1 Fase di inizio della comunicazione

2.2.5.2 Fase di comunicazione

2.2.6 Contenuto del messaggio di risposta

2.2.6.1 Risposta positiva di trasferimento dati ispezione

2.2.6.2 Risposta positiva di trasferimento dati relativi alle attività

2.2.6.3 Risposta positiva di trasferimento dati relativi alle anomalie e ai guasti

2.2.6.4 Risposta positiva di trasferimento dati dettagliati relativi alla velocità

2.2.6.5 Risposta positiva di trasferimento dati tecnici

2.3. Memorizzazione dei file ESM

3. PROTOCOLLO DI TRASFERIMENTO DEI DATI DELLE CARTE TACHIGRAFICHE

3.1. Campo di applicazione

3.2. Definizioni

3.3. Trasferimento dati carta

3.3.1 Sequenza di inizializzazione

3.3.2 Sequenza dei file di dati non firmati

3.3.3 Sequenza dei file di dati firmati

3.3.4 Sequenza di azzeramento del contatore di taratura

3.4. Formato di memorizzazione dei dati

3.4.1 Introduzione

3.4.2 Formato dei file

4. TRASFERIMENTO DEI DATI DI UNA CARTA TACHIGRAFICA MEDIANTE UN'UNITÀ ELETTRONICA DI BORDO

1. INTRODUZIONE

La presente appendice stabilisce le procedure per l'esecuzione delle differenti modalità di trasferimento dei dati ad un dispositivo di memorizzazione esterno (ESM), insieme ai protocolli da attuare per garantire il corretto trasferimento dei dati e la piena compatibilità del formato dei dati trasferiti, in modo da consentire a qualsiasi agente di controllo di ispezionare i dati in questione e verificarne l'autenticità e integrità prima di procedere alla loro analisi.

1.1. **Campo di applicazione**

Il trasferimento di dati ad un ESM può avvenire:

— da un'unità elettronica di bordo mediante un apparecchio intelligente dedicato (Intelligent dedicated equipment — IDE) collegato alla VU,

— da una carta tachigrafica mediante un IDE dotato di interfaccia della carta (IFD),

▼B

— da una carta tachigrafica e attraverso l'unità elettronica di bordo mediante un IDE collegato alla VU.

Per consentire la verifica dell'autenticità e dell'integrità dei dati trasferiti e memorizzati in un ESM, i dati vengono trasferiti allegando una firma digitale conformemente all'appendice 11 (Meccanismi comuni di sicurezza). Vengono inoltre trasferiti i dati relativi all'identificazione dell'apparecchio di provenienza (VU o carta tachigrafica) e i relativi certificati di sicurezza (Stato membro e apparecchio). Chi è preposto alla verifica dei dati deve essere in possesso di una chiave pubblica europea fidata.

DDP_001 I dati trasferiti nel corso di un'unica sessione devono essere memorizzati all'interno dell'ESM in un unico file.

1.2. **Acronimi e simboli**

Nella presente appendice sono utilizzati i seguenti acronimi:

AID Identificativo dell'applicazione (Application Identifier)

ATR Risposta al reset (Answer To Reset)

CS Byte di totale di controllo (Checksum byte)

DF File dedicato

DS_ Sessione di diagnostica

EF File elementare

ESM Dispositivo di memorizzazione esterno (External Storage Medium)

FID Identificatore file (file ID) (File identifier)

FMT Format byte (primo byte dell'intestazione del messaggio)

ICC Carta a circuito integrato (Integrated Circuit Card)

IDE Apparecchio intelligente dedicato (Intelligent dedicated equipment): apparecchio utilizzato per effettuare il trasferimento di dati all'ESM (ad esempio: un personal computer)

IFD Dispositivo interfaccia (Interface device)

KWP Keyword Protocol 2000

LEN Byte di lunghezza (Length Byte) (ultimo byte nell'intestazione del messaggio)

PPS Selezione del parametro di protocollo (Protocol Parameter Selection)

PSO Esecuzione operazione di sicurezza (Perform Security Operation)

SID Identificativo del servizio

SRC Source byte

TGT Target byte

TLV Valore lunghezza tag (Tag Length Value)

TREP Parametro di risposta di trasferimento (Transfer Response Parameter)

TRTP Parametro di richiesta di trasferimento (Transfer Request Parameter)

VU Unità elettronica di bordo (Vehicle Unit)

▼B

2. TRASFERIMENTO DEI DATI DA UNA VU

2.1. **Procedura di trasferimento dei dati**

Per effettuare un trasferimento di dati da una VU l'operatore deve eseguire le seguenti operazioni:

— inserire la propria carta tachigrafica in una sede (slot) della VU (*);

— collegare l'IDE al connettore di trasferimento dati della VU;

— stabilire il collegamento tra l'IDE e la VU;

— selezionare sull'IDE i dati da trasferire e inviare la richiesta alla VU;

— terminare la sessione di trasferimento dati.

2.2. **Protocollo di trasferimento dei dati**

Il protocollo è strutturato sulla base di una configurazione di tipo «master-slave», in cui all'IDE è assegnato il ruolo master e alla VU quello slave.

La struttura, i tipi e il flusso dei messaggi si basano principalmente sul Keyword Protocol 2000 (KWP) (ISO 14230-2 Road vehicles — Diagnostic systems — Keyword protocol 2000 — Part 2: Data link layer).

Il livello dell'applicazione è basato in gran parte sull'attuale versione della norma ISO 14229-1 (Road vehicles — Diagnostic systems — Part 1: Diagnostic services, versione 6 del 22 febbraio 2001).

2.2.1 *Struttura dei messaggi*

DDP_002 Tutti i messaggi scambiati tra l'IDE e la VU sono formattati secondo una struttura composta da tre parti:

— intestazione, costituita da un format byte di formato (FMT), un target byte (TGT), un source byte (SRC) ed, eventualmente, un byte di lunghezza (LEN);

— campo dati, costituito da un byte identificatore del servizio (SID), che può comprendere un byte facoltativo relativo alla sessione di diagnostica (DS_) o un byte facoltativo relativo al parametro di trasferimento (TRIP o TREP);

— totale di controllo, costituito da un byte di totale di controllo (CS).

Intestazione				Campo dati					Totale di controllo
FMT	TGT	SRC	LEN	SID	DATI	…	…	…	CS
4 byte				Max 255 byte					1 byte

I byte TGT e SRC rappresentano l'indirizzo fisico del destinatario e del mittente del messaggio. I valori esadecimali sono rispettivamente F0 per l'IDE ed EE per la VU.

Il byte LEN è la lunghezza della parte riservata al campo dati.

Il byte del totale di controllo è dato dalla somma su 8 bit, modulo 256, di tutti i byte del messaggio escluso lo stesso CS.

I byte relativi a FMT, SID, DS_, TRTP e TREP sono definiti più avanti nel presente documento.

(*) L'inserimento della carta determina l'abilitazione degli opportuni diritti di accesso alla funzione di trasferimento e ai dati in questione. Deve essere possibile tuttavia trasferire dati da una carta del conducente inserita in uno degli slot della VU se nessun'altra carta è inserita nell'altro slot.

▼B

DDP_003 Nel caso in cui i dati da inviare nel messaggio eccedano lo spazio disponibile nella sezione riservata al campo di dati, il messaggio viene suddiviso in diversi sottomessaggi. Ciascun sottomessaggio ha un'intestazione, gli stessi SID, TREP e un contatore a 2 byte che indica il numero del sottomessaggio all'interno del messaggio totale. Per abilitare la verifica degli errori e interrompere la trasmissione di dati, l'IDE conferma tutti i sottomessaggi. L'IDE può accettare un sottomessaggio, chiedere che sia ritrasmesso, richiedere alla VU di ricominciare o interrompere la trasmissione.

DDP_004 Se l'ultimo sottomessaggio contiene esattamente 255 byte nel campo dati, è necessario allegare un sottomessaggio finale con un campo dati vuoto (salvo SID, TREP e il contatore sottomessaggi) per indicare la fine del messaggio.

Esempio:

Intestazione	SID	TREP	Messaggio	CS
4 byte	Lunghezza superiore a 255 byte			

è trasmesso nella seguente forma:

Intestazione	SID	TREP	00	01	Sottomessaggio 1	CS
4 byte	255 byte					

Intestazione	SID	TREP	00	02	Sottomessaggio 2	CS
4 byte	255 byte					

…

Intestazione	SID	TREP	xx	yy	Sottomessaggio n	CS
4 byte	Lunghezza inferiore a 255 byte					

o nella forma:

Intestazione	SID	TREP	00	01	Sottomessaggio 1	CS
4 byte	255 byte					

Intestazione	SID	TREP	00	02	Sottomessaggio 2	CS
4 byte	255 byte					

…

Intestazione	SID	TREP	xx	yy	Sottomessaggio n	CS
4 byte	255 byte					

Intestazione	SID	TREP	xx	yy + 1	CS
4 byte	4 byte				

▼B

2.2.2 *Tipi di messaggio*

Il protocollo di comunicazione per il trasferimento di dati tra la VU e l'IDE richiede lo scambio di 8 tipi diversi di messaggi.

La tabella che segue riepiloga questi messaggi.

Struttura del messaggio	Max 4 Byte Intestazione				Max 255 Byte Dati			1 Byte Totale
IDE -> <- VU	FMT	TGT	SRC	LEN	SID	DS_/TRTP	DATA	CS
Richiesta di inizio comunicazione	81	EE	F0		81			E0
Risposta positiva di inizio comunicazione	80	F0	EE	03	C1		EA, 8F	9B
Richiesta di inizio sessione diagnostica	80	EE	F0	02	10	81		F1
Risposta positiva di inizio sessione diagnostica	80	F0	EE	02	50	81		31
Servizi di controllo del collegamento								
Verifica della frequenza di baud (fase 1)								
9 600 Bd	80	EE	F0	04	87		01,01,01	EC
19 200 Bd	80	EE	F0	04	87		01,01,02	ED
38 400 Bd	80	EE	F0	04	87		01,01,03	EE
57 600 Bd	80	EE	F0	04	87		01,01,04	EF
115 200 Bd	80	EE	F0	04	87		01,01,05	F0
Risposta positiva verifica della frequenza di baud	80	F0	EE	02	C7		01	28
Frequenza di baud di transizione (fase 2)	80	EE	F0	03	87		02,03	ED
Richiesta di invio dati	80	EE	F0	0A	35		00,00,00,00, 00,FF,FF,FF, FF	99
Risposta positiva di invio dati	80	F0	EE	03	75		00,FF	D5
Richiesta di trasferimento dati								
Riepilogo	80	EE	F0	02	36	01		97
Attività	80	EE	F0	06	36	02	Data	CS
Anomalie e guasti	80	EE	F0	02	36	03		99
Dati dettagliati relativi alla velocità	80	EE	F0	02	36	04		9A
Dati tecnici	80	EE	F0	02	36	05		9B
Trasferimento dei dati della carta	80	EE	F0	02	36	06	Slot	CS
Risposta positiva di trasferimento dati	80	F0	EE	Len	76	TREP	Dati	CS
Richiesta di chiusura trasferimento	80	EE	F0	01	37			96
Risposta positiva richiesta di chiusura trasferimento	80	F0	EE	01	77			D6

▼B

Struttura del messaggio	Max 4 Byte Intestazione				Max 255 Byte Dati			1 Byte Totale
IDE -> <- VU	FMT	TGT	SRC	LEN	SID	DS_/TRTP	DATA	CS
Richiesta di termine comunicazione	80	EE	F0	01	82			E1
Risposta positiva di termine comunicazione	80	F0	EE	01	C2			21
Riconoscimento sottomessaggio	80	EE	F0	Len	83		Dati	CS
Risposte negative								
Rifiuto generico	80	F0	EE	03	7F	Sid Req	10	CS
Servizio non supportato	80	F0	EE	03	7F	Sid Req	11	CS
Sottofunzione non supportata	80	F0	EE	03	7F	Sid Req	12	CS
Lunghezza del messaggio non corretta	80	F0	EE	03	7F	Sid Req	13	CS
Condizioni non soddisfatte o errore nella sequenza di richiesta	80	F0	EE	03	7F	Sid Req	22	CS
Richiesta fuori valori limite	80	F0	EE	03	7F	Sid Req	31	CS
Invio dati rifiutato	80	F0	EE	03	7F	Sid Req	50	CS
Risposta pendente	80	F0	EE	03	7F	Sid Req	78	CS
Dati non disponibili	80	F0	EE	03	7F	Sid Req	FA	CS

Note:

— Sid Req = il Sid della richiesta corrispondente.

— TREP = il TRTP della richiesta corrispondente.

— Le celle scure indicano l'assenza di trasmissione.

— Il termine invio (upload) (riferito all'IDE) è utilizzato per compatibilità con la norma ISO 14229. Esso ha lo stesso significato di trasferimentoc (download) (riferito alla VU).

— La tabella non riporta i potenziali contatori a 2 byte di sottomessaggi.

— “Slot” è il numero dello slot, “1” (carta nello slot conducente) o “2” (carta nello slot «secondo conducente»)

— Qualora non sia specificato lo slot, la VU deve selezionare lo slot 1 se la carta è inserita in questo slot e lo slot 2 solo qualora sia scelto espressamente dall'utente.

2.2.2.1 Richiesta di inizio comunicazione (SID 81)

DDP_005 Tale messaggio è inviato dall'IDE per stabilire il collegamento nelle comunicazioni con la VU. Le comunicazioni iniziali sono sempre eseguite a 9 600 baud (finché la velocità non è cambiata usando gli opportuni servizi di controllo del collegamento).

▼B

2.2.2.2 Risposta positiva di inizio comunicazione (SID C1)

DDP_006 Questo messaggio è inviato dalla VU per rispondere positivamente alla richiesta di inizio comunicazione e comprende i 2 byte chiave “EA” e “8F” che indicano che l'unità supporta il protocollo con intestazione, comprendente le informazioni su target, source e lunghezza.

2.2.2.3 Richiesta di inizio sessione diagnostica (SID 10)

DDP_007 Il messaggio “Richiesta di inizio sessione diagnostica” è inviato dall'IDE allo scopo di chiedere una nuova sessione di diagnostica della VU. La sottofunzione «sessione predefinita» (81 esadecimale) indica che deve essere avviata una sessione di diagnostica standard.

2.2.2.4 Risposta positiva di inizio sessione diagnostica (SID 50)

DDP_008 Il messaggio «Risposta positiva di inizio sessione diagnostica» è inviato dalla VU per rispondere positivamente a Richiesta di inizio sessione diagnostica.

2.2.2.5 Servizio di controllo del collegamento (SID 87)

DDP_052 Il «Servizio di controllo del collegamento» è utilizzato dall'IDE per iniziare il cambiamento della velocità in baud. Il cambiamento avviene in due fasi. Nella prima fase l'IDE propone il cambiamento, indicando la nuova velocità. Ricevuta la risposta positiva della VU, l'IDE conferma il cambiamento di velocità in baud alla VU (seconda fase). L'IDE passa quindi alla nuova velocità in baud. Ricevuta la conferma, anche la VU passa alla nuova velocità.

2.2.2.6 Risposta positiva di controllo del collegamento (SID C7)

DDP_053 La «Risposta positiva di controllo del collegamento» è inviata dalla VU per rispondere positivamente alla richiesta di Link Control Service (prima fase). Nessuna risposta è invece inviata alla richiesta di conferma (seconda fase).

2.2.2.7 Richiesta di invio dati (upload) (SID 35)

DDP_009 Il messaggio «Richiesta di invio dati (upload)» è inviato dall'IDE per specificare alla VU che si richiede un'operazione di trasferimento dati. Per soddisfare i requisiti della norma ISO 14229 vengono anche inviati dati relativi all'indirizzo, alla dimensione ed al formato dei dati richiesti. Poiché tali informazioni non sono note all'IDE prima del trasferimento, l'indirizzo di memoria è impostato su 0, il formato non è né criptato né compresso e la dimensione della memoria è impostata sul valore massimo.

2.2.2.8 Risposta positiva di invio dati (upload) (SID 75)

DDP_010 Il messaggio «Risposta positiva di invio dati (upload)» è inviato dalla VU per segnalare all'IDE che la VU è pronta ad eseguire il trasferimento dei dati. Per soddisfare i requisiti della norma ISO 14229 nel messaggio di risposta positiva sono contenuti anche dati che indicano all'IDE che i successivi messaggi di Risposta positiva alla richiesta di trasferimento dati comprenderanno al massimo 00FF bytes esadecimali.

▼B

2.2.2.9 Richiesta di trasferimento dati (SID 36)

DDP_011 La «Richiesta di trasferimento dati» è inviata dall'IDE per specificare alla VU il tipo di dati da trasferire. Un Parametro di richiesta di trasferimento (TRTP) di un byte indica il tipo di trasferimento.

Vi sono sei tipi di trasferimento dati:

— Ispezione (TRTP 01),

— Attività relative ad una data specifica (TRTP 02),

— Anomalie e guasti (TRTP 03),

— Dati dettagliati relativi alla velocità (TRTP 04),

— Dati tecnici (TRTP 05),

— Trasferimento dati carta (TRTP 06).

DDP_054 L'IDE deve obbligatoriamente richiedere il trasferimento dati in modalità ispezione (TRTP 01) durante una sessione di trasferimento, poiché solo in tal modo i certificati della VU vengono registrati nei file trasferiti (e permettono così la verifica della firma digitale).

Nel secondo caso (TRTP 02) il messaggio Richiesta di trasferimento dati comprende l'indicazione del giorno di calendario (formato `TimeReal`) da trasferire.

2.2.2.10 Risposta positiva di trasferimento dati (SID 76)

DDP_012 Il messaggio «Risposta positiva di trasferimento dati» è inviato dalla VU in risposta alla Richiesta di trasferimento dati e contiene i dati richiesti con il Parametro di risposta di trasferimento (TREP) corrispondente al TRTP della richiesta.

DDP055 Nel primo caso (TREP 01) la VU invia i dati utili all'operatore dell'IDE per individuare i dati che intende trasferire. Le informazioni contenute all'interno del messaggio in questione riguardano:

— certificati di sicurezza,

— identificazione del veicolo

— data e ora correnti della VU,

— estremi temporali minimo e massimo dei dati disponibili per il trasferimento (dati VU),

— indicazione della presenza di carte nella VU,

— precedente trasferimento dati ad un'impresa,

— blocchi di un'impresa,

— controlli precedenti.

▼B

2.2.2.11 Richiesta di chiusura trasferimento (SID 37)

DDP_013 Il messaggio «Richiesta di chiusura trasferimento» è inviato dall'IDE per informare la VU che la sessione di trasferimento è terminata.

2.2.2.12 Risposta positiva di richiesta chiusura trasferimento (SID 77)

DDP_014 Il messaggio «Risposta positiva di richiesta chiusura trasferimento» è inviato dalla VU per confermare la ricezione della Richiesta di chiusura trasferimento.

2.2.2.13 Richiesta di termine comunicazione (SID 82)

DDP_015 Il messaggio «Richiesta di termine comunicazione» è inviato dall'IDE per disattivare il collegamento di comunicazione con la VU.

2.2.2.14 Richiesta di risposta positiva di termine comunicazione (SID C2)

DDP_016 Il messaggio «Richiesta di risposta positiva di termine comunicazione» è inviato dalla VU per confermare la ricezione della Richiesta di termine comunicazione.

2.2.2.15 Riconoscimento sottomessaggio (SID 83)

DDP_017 Il messaggio «Riconoscimento sottomessaggio» è inviato dall'IDE per confermare l'avvenuta ricezione di ciascuna parte di un messaggio trasmesso sotto forma di più sottomessaggi. Il campo dati contiene il SID ricevuto dalla VU e un codice a 2 byte, come descritto qui di seguito:

— MsgC + 1 conferma la corretta ricezione del sottomessaggio MsgC.

Richiesta da parte dell'IDE alla VU di inviare il sottomessaggio successivo.

— MsgC indica un problema nella ricezione del sottomessaggio MsgC.

Richiesta da parte dell'IDE alla VU di inviare di nuovo il sottomessaggio.

— FFFF richiede la conclusione del messaggio.

Può essere utilizzato dall'IDE per terminare la trasmissione del messaggio della VU per qualsiasi ragione.

L'ultimo sottomessaggio di un messaggio (byte LEN < 255) può essere confermato utilizzando uno qualsiasi di questi codici oppure non essere confermato.

Le risposte della VU, composte da diversi sottomessaggi, sono:

— Risposta positiva di trasferimento dati (SID 76)

▼B

2.2.2.16 Risposta negativa (SID 7F)

DDP_018 La «Risposta negativa» è inviata dalla VU in risposta alle richieste sopra menzionate nel caso in cui la VU non sia in grado di soddisfare la richiesta in questione. I campi dati del messaggio comprendono il SID della risposta (7F), il SID della richiesta e un codice che specifica la ragione della risposta negativa. Sono disponibili i seguenti codici:

— 10 rifiuto generico

L'azione non può essere eseguita per una ragione diversa da quelle sotto esposte.

— 11 servizio non supportato

Mancata comprensione del SID relativo alla richiesta.

— 12 sottofunzione non supportata

Mancata comprensione del DS_ o TRTP relativo alla richiesta, o assenza di ulteriori sottomessaggi da trasmettere.

— 13 lunghezza del messaggio non corretta

Il messaggio ricevuto non ha la giusta lunghezza.

— 22 condizioni non soddisfatte o errore nella sequenza di richiesta

Il servizio richiesto non è attivo o la sequenza dei messaggi di richiesta non è corretta.

— 31 richiesta fuori valori limite

Il parametro indicato (campo dei dati) non è valido.

— 50 invio dati (upload) rifiutato

La richiesta non può essere eseguita (errata modalità di funzionamento della VU o guasto interno della VU).

— 78 risposta pendente

L'azione richiesta non può essere completata nel tempo previsto e la VU non è pronta per accettare un'altra richiesta.

— FA dati non disponibili

I dati oggetto di una richiesta di trasferimento non sono disponibili nella VU (ad esempio, non vi è alcuna carta inserita, ecc.).

2.2.3 *Flusso di messaggi*

Qui di seguito è illustrato un tipico flusso di messaggi nel corso di una normale procedura di trasferimento dati:

IDE		VU
Richiesta di inizio comunicazione	⇨	
	⇦	Risposta positiva
Richiesta di inizio sessione diagnostica	⇨	
	⇦	Risposta positiva
Richiesta di invio dati	⇨	
	⇦	Risposta positiva

▼B

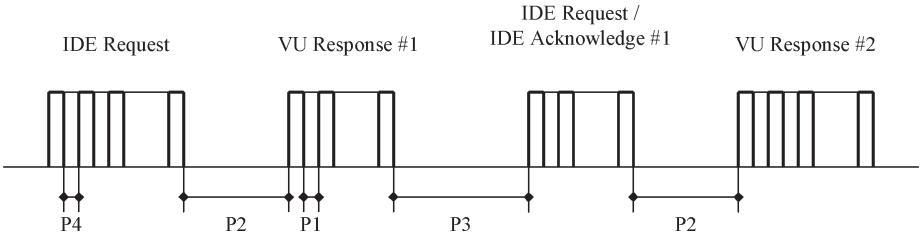
IDE		VU
Riepilogo della richiesta di trasferimento dati	⇨	
	⇦	Risposta positiva
Richiesta di trasferimento dati #2	⇨	
	⇦	Risposta positiva #1
Riconoscimento sottomessaggio #1	⇨	
	⇦	Risposta positiva #2
Riconoscimento sottomessaggio #2	⇨	
	⇦	Risposta positiva #m
Riconoscimento sottomessaggio #m	⇨	
	⇦	Risposta positiva (campo dati<255 byte)
Riconoscimento sottomessaggio (facoltativo)	⇨	
…		
Richiesta di trasferimento dati #n	⇨	
	⇦	Risposta positiva
Richiesta di chiusura trasferimento	⇨	
	⇦	Risposta positiva
Richiesta di termine comunicazione	⇨	
	⇦	Risposta positiva

2.2.4 *Temporizzazione*

DDP_019 La figura di seguito riportata illustra i parametri di temporizzazione importanti durante il normale funzionamento:

Figura 1

Flusso messaggi, temporizzazione



dove:

P1 = Intervallo di tempo tra byte per la risposta della VU.

P2 = Intervallo di tempo tra la fine della richiesta dell'IDE e l'inizio della risposta della VU o tra la fine della conferma di ricezione da parte dell'IDE e l'inizio della successiva risposta della VU.

P3 = Intervallo di tempo tra la fine della risposta della VU e l'inizio della nuova richiesta dell'IDE, o tra la fine della risposta della VU e l'inizio della conferma di ricezione da parte dell'IDE, o tra la fine della richiesta dell'IDE e l'inizio della nuova richiesta dell'IDE in caso di mancata risposta da parte della VU.

P4 = Intervallo di tempo tra byte per la richiesta da parte dell'IDE.

P5 = Valore ampliato di P3 per il trasferimento dei dati dalla carta.

▼B

I valori consentiti per i parametri di temporizzazione sono illustrati nella tabella successiva (impostazione dei parametri di temporizzazione supplementari relativi al KWP, utilizzata in caso di indirizzamento fisico per una comunicazione più veloce).

Parametro di temporizzazione	Valore minimo (ms)	Valore massimo (ms)
P1	0	20
P2	20	1 000 (*)
P3	10	5 000
P4	5	20
P5	10	20 minuti

(*) Se la VU risponde con una Risposta negativa contenente un codice che significa «richiesta correttamente ricevuta, risposta pendente», questo valore è esteso allo stesso valore limite superiore di P3.

2.2.5 *Gestione degli errori*

In caso di errore durante lo scambio di messaggi, lo schema del flusso dei messaggi è modificato a seconda di quale apparecchio abbia rilevato l'errore e del messaggio che l'ha generato.

Le figure 2 e 3 indicano le procedure di gestione degli errori rispettivamente per la VU e per l'IDE.

2.2.5.1 Fase di inizio della comunicazione

DDP_020 Se durante la fase di avvio delle comunicazioni l'IDE rileva un errore, nella temporizzazione o nel flusso di bit, esso attende per un intervallo di tempo pari a P3min prima di riproporre la richiesta.

DDP_021 Se la VU rileva un errore nella sequenza inviata dall'IDE, essa non invia risposta e attende una nuova Richiesta di inizio comunicazione, che deve pervenire entro un limite di tempo pari a P3 max.

2.2.5.2 Fase di comunicazione

Si possono individuare due distinti ambiti di gestione degli errori:

1. **Rilevamento da parte della VU di un errore di trasmissione dell'IDE**

DDP_022 Per ogni messaggio ricevuto la VU deve rilevare l'eventuale presenza di errori di temporizzazione, di formato dei byte (ad esempio: violazione dei bit di avvio e di arresto) e di struttura (numero errato dei byte ricevuti, byte errato relativo al totale di controllo).

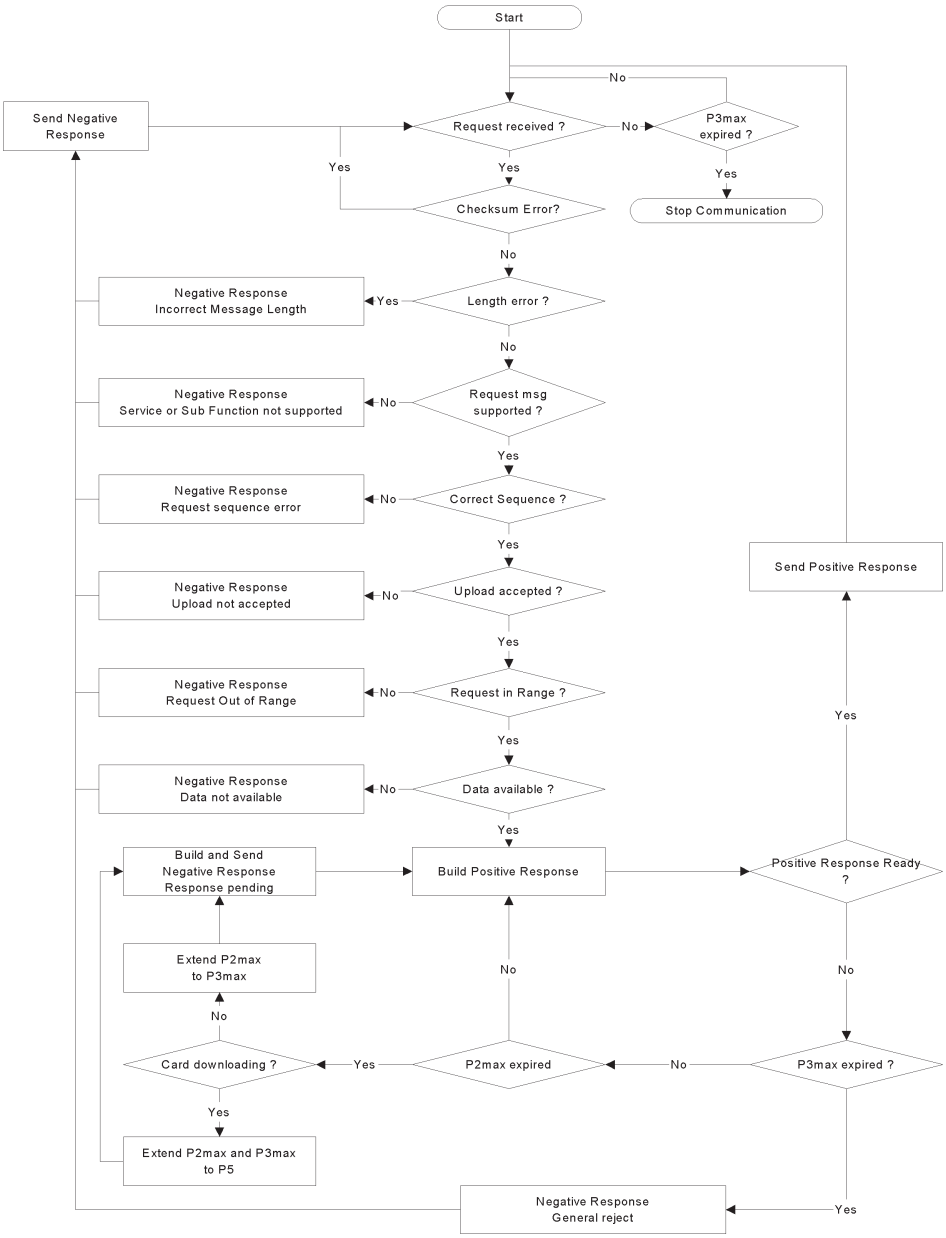
DDP_023 In caso di rilevamento di uno degli errori sopra menzionati da parte della VU, quest'ultima non invia alcuna risposta e ignora il messaggio ricevuto.

DDP_024 È possibile che la VU rilevi altri errori relativi al formato o al contenuto del messaggio ricevuto (ad esempio, messaggio non supportato) anche se questo soddisfa i requisiti previsti di lunghezza e totale di controllo; in tal caso, la VU risponde all'IDE con un messaggio di Risposta negativa che specifica la natura dell'errore in questione.

▼B

Figura 2

Gestione degli errori da parte della VU



2. **Rilevamento da parte dell'IDE di un errore di trasmissione della VU**

DDP_025 Per ogni messaggio ricevuto l'IDE rileva l'eventuale presenza di errori di temporizzazione, di formato dei byte (ad esempio: violazione dei bit di avvio e di arresto) e di struttura (numero errato dei byte ricevuti, byte errato relativo al totale di controllo).

DDP_026 L'IDE rileva errori di sequenza, ad esempio messaggi successivi con incrementi non corretti del contatore di sottomessaggi.

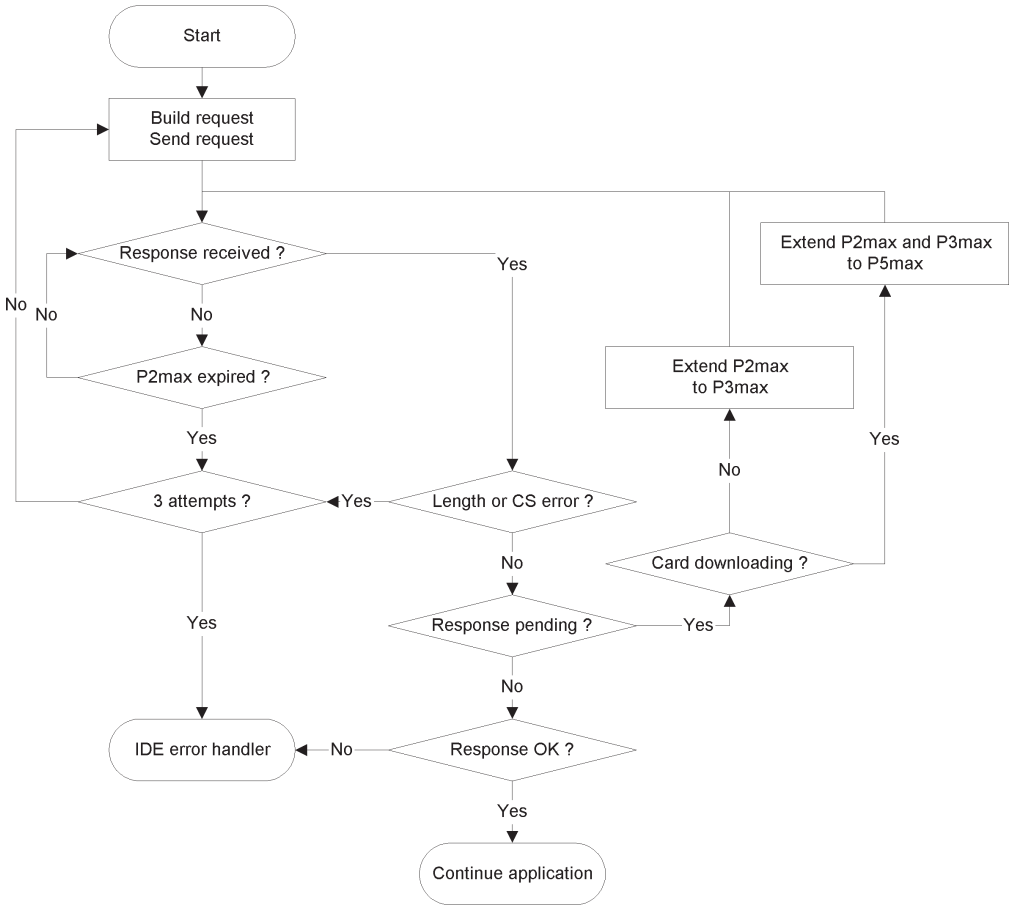
DDP_027 In caso di rilevamento di un errore da parte dell'IDE o in assenza di risposta da parte della VU entro un periodo di tempo pari a P2max, il messaggio di richiesta sarà nuovamente inviato per un numero massimo complessivo di tre trasmissioni. Ai fini di tale rilevamento di errori, la conferma di ricezione di un sottomessaggio sarà considerata come una richiesta inviata alla VU.

▼B

DDP_028 L'IDE deve attendere un intervallo di tempo pari a P3min prima dell'inizio di ciascuna trasmissione; il periodo di attesa viene misurato a partire dall'ultimo intervento calcolato di un bit di arresto dopo il rilevamento dell'errore.

Figura 3

Gestione degli errori da parte dell'IDE



2.2.6 *Contenuto del messaggio di risposta*

Il presente punto definisce il contenuto dei campi di dati dei vari messaggi di risposta positiva.

Gli elementi di dati sono definiti nel dizionario di dati di cui all'appendice 1.

Osservazioni: per i trasferimenti di generazione 2 ogni elemento di dati di alto livello è rappresentato da un record array, anche se esso contiene un solo record. Un record array inizia con un'intestazione, che contiene i tipi, le dimensioni e il numero di record. I record array sono sempre denominati «…RecordArray» (con intestazione) nelle seguenti tabelle.

2.2.6.1 Risposta positiva di trasferimento dati ispezione

DDP_029 Il campo dati del messaggio «Risposta positiva di trasferimento dati ispezione» deve fornire nell'ordine sotto indicato i seguenti dati corrispondenti ai valori esadecimali SID 76 e TREP 01, nonché alla suddivisione e al conteggio appropriati dei sottomessaggi:

▼B

Struttura dei dati generazione 1

Elemento di dati	Osservazioni
MemberStateCertificate VUCertificate	Certificati di sicurezza VU
VehicleIdentificationNumber VehicleRegistrationIdentification	Identificazione del veicolo
CurrentDateTime	Data e ora correnti della VU
VuDownloadablePeriod	Periodo disponibile per il trasferimento
CardSlotsStatus	Tipi di carte inserite nella VU
VuDownloadActivityData	Precedente trasferimento dalla VU
VuCompanyLocksData	Tutti i blocchi di un'impresa memorizzati. Se la sezione è vuota, viene inviato solo noOfLocks = 0.
VuControlActivityData	Tutti i record di controllo memorizzate nella VU. Se la sezione è vuota, viene inviato solo noOfControls = 0.
Signature	Firma RSA di tutti i dati (tranne i certificati) a partire dal VehicleIdentificationNumber fino all'ultimo byte dell'ultimo VuControlActivityData.

Struttura dei dati generazione 2

Elemento di dati	Osservazioni
MemberStateCertificateRecordArray	Certificato dello Stato membro
VUCertificateRecordArray	Certificato VU
VehicleIdentificationNumberRecordArray	Identificazione del veicolo
VehicleRegistrationNumberRecordArray	Numero d'immatricolazione del veicolo
CurrentDateTimeRecordArray	Data e ora correnti della VU
VuDownloadablePeriodRecordArray	Periodo disponibile per il trasferimento
CardSlotsStatusRecordArray	Tipi di carte inserite nella VU
VuDownloadActivityDataRecordArray	Precedente trasferimento dalla VU
VuCompanyLocksRecordArray	Tutti i blocchi di un'impresa memorizzati. Se la sezione è vuota, viene inviata un'intestazione di array con noOfRecords = 0.
VuControlActivityRecordArray	Tutti i record di controllo memorizzati nella VU. Se la sezione è vuota, viene inviata un'intestazione di array con noOfRecords = 0.
SignatureRecordArray	Firma ECC di tutti i dati precedenti esclusi i certificati.

2.2.6.2 Risposta positiva di trasferimento dati relativi alle attività

DDP_030 Il campo dati del messaggio «Risposta positiva di trasferimento dati relativi alle attività» fornisce nell'ordine sotto indicato i seguenti dati corrispondenti ai valori esadecimali SID 76 e TREP 02, nonché alla suddivisione e al conteggio appropriati dei sottomessaggi:

▼B

Struttura dei dati generazione 1

Elemento di dati	Osservazioni
TimeReal	Data della giornata oggetto del trasferimento di dati
OdometerValueMidnight	Odometro alla fine della giornata oggetto del trasferimento di dati
VuCardIWData	Dati dei cicli di inserimento ed estrazione delle carte. — Se questa sezione non contiene dati disponibili, viene inviato solo noOfVuCardIWRecords = 0. — Quando un VuCardIWRecord oltrepassa 00:00 (inserimento della carta il giorno precedente) o 24:00 (estrazione della carta il giorno seguente) deve figurare interamente nei due giorni in questione.
VuActivityDailyData	Lo stato dello slot a 00:00 e cambi di attività registrati per la giornata oggetto del trasferimento dati.
VuPlaceDailyWorkPeriodData	Dati relativi ai luoghi registrati nella giornata oggetto del trasferimento dati. Se la sezione è vuota, viene inviato solo noOfPlaceRecords = 0.
VuSpecificConditionData	Dati delle condizioni particolari registrati nella giornata oggetto del trasferimento dati. Se la sezione è vuota, viene inviato solo noOfSpecificConditionRecords=0.
Signature	Firma RSA di tutti i dati a partire da TimeReal fino all'ultimo byte dell'ultimo record di condizione particolare.

Struttura dei dati generazione 2

Elemento di dati	Osservazioni
DateOfDayDownloadedRecordArray	Data della giornata oggetto del trasferimento di dati
OdometerValueMidnightRecordArray	Odometro alla fine della giornata oggetto del trasferimento di dati
VuCardIWRecordArray	Dati dei cicli di inserimento ed estrazione delle carte. — Se la sezione è vuota, viene inviata un'intestazione di array con noOfRecords = 0. — Quando un VuCardIWRecord oltrepassa 00:00 (inserimento della carta il giorno precedente) o in 24:00 (estrazione della carta il giorno seguente) deve figurare interamente nei due giorni in questione.
VuActivityDailyRecordArray	Lo stato dello slot a 00:00 e cambi di attività registrati per la giornata oggetto del trasferimento dati.
VuPlaceDailyWorkPeriodRecordArray	Dati relativi ai luoghi registrati nella giornata oggetto del trasferimento dati. Se la sezione è vuota, viene inviata un'intestazione di array con noOfRecords = 0.
VuGNSSCDRecordArray	Posizioni GNSS del veicolo se il periodo di guida continuo del conducente raggiunge un multiplo di tre ore. Se la sezione è vuota, viene inviata un'intestazione di array con noOfRecords = 0.
VuSpecificConditionRecordArray	Dati delle condizioni particolari registrati nella giornata oggetto del trasferimento dati. Se la sezione è vuota, viene inviata un'intestazione di array con noOfRecords = 0.
SignatureRecordArray	Firma ECC di tutti i dati precedenti.

▼B

2.2.6.3 Risposta positiva di trasferimento dati relativi ad anomalie e guasti

DDP_031 Il campo dati del messaggio «Risposta positiva di trasferimento dati relativi ad anomalie e guasti» deve fornire nell'ordine sotto indicato i seguenti dati corrispondenti ai valori esadecimali SID 76 e TREP 03, nonché alla suddivisione e al conteggio appropriati dei sottomessaggi:

Struttura dei dati generazione 1

Elemento di dati	Osservazioni
VuFaultData	Tutti i guasti memorizzati o in corso nella VU. Se la sezione è vuota, viene inviato solo noOfVuFaults = 0.
VuEventData	Tutte le anomalie (ad eccezione dei superamenti di velocità) memorizzate o in corso nella VU. Se la sezione è vuota, viene inviato solo noOfVuEvents = 0.
VuOverSpeedingControlData	Dati relativi all'ultimo controllo del superamento di velocità (valore predefinito se non sono disponibili dati).
VuOverSpeedingEventData	Tutte le anomalie di superamento della velocità memorizzate nella VU. Se la sezione è vuota, viene inviato solo noOfVuOverSpeedingEvents = 0.
VuTimeAdjustmentData	Tutti gli eventi di regolazione dell'ora anomalie memorizzati nella VU (al di fuori di una taratura completa). Se la sezione è vuota, viene inviato solo noOfVuTimeAdjRecords = 0.
Signature	Firma RSA di tutti i dati a partire da noOfVuFaults fino all'ultimo byte dell'ultimo record di regolazione dell'ora.

Struttura dei dati generazione 2

Elemento di dati	Osservazioni
VuFaultRecordArray	Tutti i guasti memorizzati o in corso nella VU. Se la sezione è vuota, viene inviata un'intestazione di array con noOfRecords = 0.
VuEventRecordArray	Tutti gli eventi (ad eccezione dei superamenti di velocità) memorizzati o in corso nella VU. Se la sezione è vuota, viene inviata un'intestazione di array con noOfRecords = 0.
VuOverSpeedingControlDataRecordArray	Dati relativi all'ultimo controllo del superamento di velocità (valore predefinito se non sono disponibili dati).
VuOverSpeedingEventRecordArray	Tutti gli eventi di superamento della velocità memorizzati nella VU. Se la sezione è vuota, viene inviata un'intestazione di array con noOfRecords = 0.
VuTimeAdjustmentRecordArray	Tutti gli eventi di regolazione dell'ora anomalie memorizzati nella VU (al di fuori di una taratura completa). Se la sezione è vuota, viene inviata un'intestazione di array con noOfRecords = 0.
VuTimeAdjustmentGNSSRecordArray	
SignatureRecordArray	Firma ECC di tutti i dati precedenti.

▼B

2.2.6.4 Risposta positiva di trasferimento dati dettagliati relativi alla velocità

DDP_032 Il campo dati del messaggio «Risposta positiva di trasferimento dati dettagliati relativi alla velocità» deve fornire nell'ordine sotto indicato, i seguenti dati corrispondenti ai valori esadecimali SID 76 e TREP 04, nonché alla suddivisione e al conteggio appropriati dei sottomessaggi:

Struttura dei dati generazione 1

Elemento di dati	Osservazioni
VuDetailedSpeedData	Tutti i dati dettagliati relativi alla velocità memorizzati nella VU (un blocco di velocità al minuto di marcia del veicolo) 60 valori della velocità al minuto (uno al secondo).
Signature	Firma RSA di tutti i dati a partire da noOfSpeedBlocks fino all'ultimo byte dell'ultimo blocco di velocità.

Struttura dei dati generazione 2:

Elemento di dati	Osservazioni
VuDetailedSpeedBlockRecordArray	Tutti i dati dettagliati relativi alla velocità memorizzati nella VU (un blocco di velocità al minuto di marcia del veicolo) 60 valori della velocità al minuto (uno al secondo).
SignatureRecordArray	Firma ECC di tutti i dati precedenti.

2.2.6.5 Risposta positiva di trasferimento dati tecnici

DDP_033 Il campo dati del messaggio «Risposta positiva di trasferimento dati tecnici» deve fornire, nell'ordine sotto indicato, i seguenti dati corrispondenti ai valori esadecimali SID 76 e TREP 05, nonché alla suddivisione e al conteggio appropriati dei sottomessaggi:

Struttura dei dati generazione 1

Elemento di dati	Osservazioni
VuIdentification	
SensorPaired	
VuCalibrationData	Tutti i record di taratura memorizzati nella VU.
Signature	Firma RSA di tutti i dati a partire da vuManufacturerName fino all'ultimo byte dell'ultimo VuCalibrationRecord.

▼B

Struttura dei dati generazione 2

Elemento di dati	Osservazioni
VuIdentificationRecordArray	
VuSensorPairedRecordArray	Tutti gli accoppiamenti di MS memorizzati nella VU.
VuSensorExternalGNSSCoupledRecordArray	Tutte gli accoppiamenti del dispositivo GNSS esterno memorizzati nella VU
VuCalibrationRecordArray	Tutti i record di taratura memorizzati nella VU.
VuCardRecordArray	Tutti i dati relativi all'inserimento della carta memorizzati nella VU.
VuITSConsentRecordArray	
VuPowerSupplyInterruptionRecordArray	
SignatureRecordArray	Firma ECC di tutti i dati precedenti.

2.3. **Memorizzazione dei file ESM**

DDP_034 Se una sessione di trasferimento comprende dati relativi alla VU, l'IDE deve memorizzare in un unico file fisico tutti i dati ricevuti dalla VU nel corso della sessione nell'ambito dei messaggi di Risposta positiva di trasferimento dati. I dati memorizzati non comprendono le intestazioni dei messaggi, i contatori dei sottomessaggi, i sottomessaggi vuoti e i totali di controllo, ma comprendono SID e TREP (relativi soltanto al primo sottomessaggio nel caso di più sottomessaggi).

3. PROTOCOLLO DI TRASFERIMENTO DEI DATI DELLE CARTE TACHIGRAFICHE

3.1. **Campo di applicazione**

Il presente punto descrive il trasferimento diretto dei dati di una carta tachigrafica ad un IDE. Quest'ultimo non fa parte dell'ambiente sicuro; quindi non viene eseguita alcuna autenticazione tra la carta e l'IDE.

3.2. **Definizioni**

Sessione di trasferimento: ogni trasferimento di dati dell'ICC. La sessione comprende la procedura completa, dalla reinizializzazione dell'ICC da parte di un IFD fino alla disattivazione dell'ICC (estrazione della carta o reinizializzazione successiva).

File di dati con firma: un file proveniente dall'ICC. Il file è trasferito all'IFD con testo in chiaro. Nell'ICC il file viene «frammentato» (con la funzione di hash) e firmato, quindi la firma è trasferita all'IFD.

3.3. **Trasferimento dati carta**

DDP_035 Il trasferimento dei dati di una carta tachigrafica comprende le seguenti fasi:

— Trasferimento negli EF ICC e IC dell'informazione comune relativa alla carta. Questa informazione è facoltativa e non è resa sicura mediante firma digitale.

▼B

— Trasferimento degli EF Card_Certificate (o CardSignCertificate) e CA_Certificate. Questa informazione non è resa sicura mediante firma digitale.

Il trasferimento dei file in questione è obbligatorio per ogni sessione di trasferimento.

— Trasferimento degli altri EF di dati relativi alle diverse applicazioni (all'interno del Tachograph DF e Tachograph_G2 DF se pertinente) ad eccezione di EF Card_Download. Questa informazione è resa sicura mediante firma digitale.

— Per ogni sessione di trasferimento è obbligatorio il trasferimento almeno degli EF Application_Identification e ID.

— Nel trasferire i dati relativi alla carta del conducente è obbligatorio trasferire anche i seguenti EF:

- Events_Data,
- Faults_Data,
- Driver_Activity_Data,
- Vehicles_Used,
- Places,
- GNSS_Places (if relevant),
- Control_Activity_Data,
- Specific_Conditions.

— Nel trasferimento dei dati relativi alla carta del conducente, aggiornare LastCardDownload nell'EF Card_Download,

— Nel trasferimento dei dati relativi alla carta dell'officina, reinizializzare il contatore di taratura nell'EF Card_Download.

— Nel trasferimento dei dati relativi alla carta dell'officina l' EF Sensor_Installation_Data non va scaricato.

3.3.1 *Sequenza di inizializzazione*

DDP_036 L'IDE avvia la sequenza nel modo seguente:

Carta	Direzione	IDE/IFD	Significato/Osservazioni
	⇦	Reinizializzazione Hardware	
ATR	⇨		

È facoltativo utilizzare la PPS per passare ad una velocità di baud maggiore fintanto che l'ICC sia in grado di supportarla.

3.3.2 *Sequenza dei file di dati non firmati*

DDP_037 La sequenza per il trasferimento degli EF ICC, IC, Card_Certificate (o CardSignCertificate) e CA_Certificate è la seguente:

Carta	Direzione	IDE/IFD	Significato/Osservazioni
	⇦	**Seleziona file**	Seleziona mediante identificatori di file
OK	⇨		

▼B

Carta	Direzione	IDE/IFD	Significato/Osservazioni
	⇦	**Read binary**	Se il file contiene più dati della dimensione buffer del lettore o della carta, è necessario ripetere il comando fino all'avvenuta lettura del file completo
File dati OK	⇨	Invia dati in memoria a ESM	secondo **3.4** Formato di memorizzazione dei dati

Nota 1: prima di selezionare l'EF Card_Certificate (o CardSignCertificate) è necessario selezionare l'applicazione del tachigrafo (selezione mediante AID).

Nota 2: La selezione e la lettura di un file può anche essere effettuata in una sola volta utilizzando il comando Read binary con un breve identificatore EF.

3.3.3 *Sequenza dei file di dati firmati*

DDP_038 Per ciascuno dei seguenti file che devono essere trasferiti insieme alla rispettiva firma è necessario utilizzare la successiva sequenza:

Carta	Dir	IDE/IFD	Significato/Osservazioni
	⇦	**Seleziona file**	
OK	⇨		
	⇦	**Esegui Hash of file**	Calcola il valore di hash sul contenuto dei dati del file selezionato, mediante l'algoritmo di hash conformemente all'appendice 11. Il comando in questione non è del tipo ISO
Calcola il valore di hash del file e memorizza temporaneamente tale valore			
OK	⇨		
	⇦	**Read binary**	Se il file contiene più dati della dimensione buffer del lettore o della carta, è necessario ripetere il comando fino all'avvenuta lettura del file completo
File dati OK	⇨	Invia dati ricevuti in memoria a ESM	secondo **3.4** Formato di memorizzazione dei dati

▼B

Carta	Dir	IDE/IFD	Significato/Osservazioni
	⇦	**PSO: Compute Digital Signature**	
Esegue l'operazione di sicurezza «Compute Digital Signature» mediante il valore di hash temporaneamente memorizzato			
Signature OK	⇨	Aggiungi dati a quelli precedentemente memorizzati nell'ESM	secondo **3.4** Formato di memorizzazione dei dati

Nota: la selezione e la lettura di un file può anche essere effettuata in una sola volta utilizzando il comando Read binary con un breve identificatore EF. In questo caso l'EF può essere selezionato e letto prima di applicare il comando Perform Hash of File.

3.3.4 *Sequenza di azzeramento del contatore di taratura*

DDP_039 La sequenza di azzeramento del contatore `NoOfCalibrationsSinceDownload` nell'EF `Card_Download` in una carta dell'officina è la seguente:

Carta	Dir	IDE/IFD	Significato/Osservazioni
	⇦	**Seleziona file** EF Card_Download	Seleziona mediante identificatori di file
OK	⇨		
	⇦	**Update Binary** NoOfCalibrationsSinceDownload = '00 00'	
Reinizializza il numero di trasferimento della carta			
OK	⇨		

Nota: la selezione e la lettura di un file può anche essere effettuata in una sola volta utilizzando il comando Update binary con un breve identificatore EF.

3.4. **Formato di memorizzazione dei dati**

3.4.1 *Introduzione*

DDP_040 La memorizzazione dei dati trasferiti deve avvenire nel rispetto delle seguenti condizioni:

— I dati devono essere memorizzati in modo trasparente. Ciò significa che durante la memorizzazione è necessario rispettare l'ordine dei byte, così come quello dei bit all'interno dei byte trasferiti dalla carta.

— Tutti i file della carta trasferiti nell'ambito di una stessa sessione sono memorizzati nell'ESM in un unico file.

▼B

3.4.2 *Formato dei file*

DDP_041 Il formato dei file è costituito da una concatenazione di diversi oggetti TLV.

DDP_042 Il tag di un EF deve essere costituito dal FID seguito dall'appendice “00”.

DDP_043 Il tag di una firma relativa ad un EF deve essere costituito dal FID del file stesso seguito dall'appendice “01”.

DDP_044 La lunghezza è un valore di due byte. Tale valore definisce il numero di byte che costituiscono il campo valori. Il valore “FF FF” nel campo relativo alla lunghezza è riservato per un uso futuro.

DDP_045 In caso di mancato trasferimento di un file, non deve essere memorizzato alcun dato ad esso relativo (nessun tag né valore zero relativo alla lunghezza).

DDP_046 Una firma deve essere memorizzata come l'oggetto TLV immediatamente successivo all'oggetto TLV contenente i dati del file.

Definizione	Significato	Lunghezza
FID (2 byte) || “00“	Tag per EF (FID)	3 byte
FID (2 byte) || “01“	Tag per firma di EF (FID)	3 byte
xx xx	Lunghezza campo valori	2 byte

Esempio di dati contenuti in un file trasferito nell'ESM:

Tag	Lunghezza	Valore
00 02 00	00 11	Dati dell'EF ICC
C1 00 00	00 C2	Dati dell'EF Card_Certificate
		…
05 05 00	0A 2E	Dati dell'EFVehicles_Used
05 05 01	00 80	Firma dell'EFVehicles_Used

4. TRASFERIMENTO DEI DATI DI UNA CARTA TACHIGRAFICA MEDIANTE UN'UNITÀ ELETTRONICA DI BORDO.

DDP_047 La VU deve consentire di trasferire il contenuto della carta del conducente inserita ad un IDE ad essa collegata.

DDP_048 L'IDE invia un messaggio di «Richiesta di trasferimento dati della carta tachigrafica» alla VU per iniziare questo modo (cfr. 2.2.2.9).

DDP_049 La VU trasferisce quindi l'intero contenuto della carta, file dopo file, in conformità al protocollo di trasferimento dati della carta illustrato al punto 3, e invia tutti i dati ricevuti dalla carta all'IDE, nel formato file TLV appropriato (cfr. 3.4.2) e incapsulati all'interno di un messaggio «Risposta positiva di trasferimento dati».

▼B

DDP_050 L'IDE recupera i dati della carta dal messaggio «Risposta positiva di trasferimento dati» (eliminando tutte le intestazioni, i SID, i TREP, i contatori di sottomessaggi, e i totali di controllo) e li memorizza all'interno di un unico file fisico secondo quanto descritto al punto 2.3.

DDP_051 In seguito la VU, se del caso, aggiorna il file `Control_Activity_Data` o il file `Card_Download` della carta del conducente.

▼B

Appendice 8

PROTOCOLLO DI TARATURA

INDICE

1. INTRODUZIONE

2. TERMINI, DEFINIZIONI E RIFERIMENTI

3. PROSPETTO DEI SERVIZI

3.1. Servizi disponibili

3.2. Codici di risposta

4. SERVIZI DI COMUNICAZIONE

4.1. Servizio StartCommunication

4.2. Servizio StopCommunication

4.2.1 Descrizione del messaggio

4.2.2 Formato del messaggio

4.2.3 Definizione dei parametri

4.3. Servizio TesterPresent

4.3.1 Descrizione del messaggio

4.3.2 Formato del messaggio

5. SERVIZI DI GESTIONE

5.1. Servizio StartDiagnosticSession

5.1.1 Descrizione del messaggio

5.1.2 Formato del messaggio

5.1.3 Definizione dei parametri

5.2. Servizio SecurityAccess

5.2.1 Descrizione del messaggio

5.2.2 Formato del messaggio — SecurityAccess — requestSeed

5.2.3 Formato del messaggio — SecurityAccess — sendKey

6. SERVIZI DI TRASMISSIONE DATI

6.1. ReadDataByIdentifier service

6.1.1 Descrizione del messaggio

6.1.2 Formato del messaggio

6.1.3 Definizione dei parametri

6.2. Servizio WriteDataByIdentifier

6.2.1 Descrizione del messaggio

6.2.2 Formato del messaggio

6.2.3 Definizione dei parametri

▼B

7. CONTROLLO DEGLI IMPULSI DI PROVA — UNITÀ FUNZIONALE DI CONTROLLO DEI SEGNALI DI ENTRATA/USCITA

7.1. Servizio di InputOutputControlByIdentifier

7.1.1 Descrizione del messaggio

7.1.2 Formato del messaggio

7.1.3 Definizione dei parametri

8. FORMATO DEL PARAMETRO DATARECORDS

8.1. Valori limite dei parametri trasmessi

8.2. Formato del parametro dataRecords

1. INTRODUZIONE

La presente appendice descrive come avviene lo scambio di dati tra l'unità elettronica di bordo e un tester (apparecchio di prova) attraverso la linea K, che costituisce parte dell'interfaccia di taratura illustrata nell'appendice 6. Essa descrive inoltre il controllo della linea dei segnali di entrata/uscita sul connettore di taratura.

La procedura per stabilire le comunicazioni sulla linea K è descritta nella sezione 4 «Communication Services».

La presente appendice si avvale del concetto di «sessioni» diagnostiche per stabilire la finalità del controllo sulla linea K in diverse condizioni. L'impostazione predefinita è la «StandardDiagnosticSession» (sessione diagnostica standard), che consente la lettura di tutti i dati dell'unità elettronica di bordo ma non la scrittura di dati nell'unità stessa.

Il prospetto delle sessioni diagnostiche è riportato nella sezione 5 «Management Services».

La presente appendice riguarda entrambe le generazioni di VU e di carte dell'officina conformemente alle prescrizioni di interoperabilità di cui al presente regolamento.

CPR_001 La «ECUProgrammingSession» (sessione di programmazione ECU) consente l'inserimento dei dati nell'unità elettronica di bordo. In caso di inserimento dei dati di taratura, l'unità elettronica di bordo deve inoltre essere in modalità TARATURA (CALIBRATION).

La procedura di trasferimento dati sulla linea K è descritta nella sezione 6 «Data Transmission Services». Il formato dei dati trasferiti è descritto in dettaglio nella sezione 8 «dataRecords formats».

CPR_002 La «ECUAdjustmentSession» (sessione di regolazione ECU) consente di selezionare la modalità I/O della linea dei segnali di taratura attraverso l'interfaccia della linea K. Il controllo della linea dei segnali di entrata/uscita è descritto nella sezione 7 «Control of Test Pulses — Input/Output Control functional unit».

CPR_003 Nel presente documento l'indirizzo del tester è indicato come «tt». Nonostante vi possano essere indirizzi preferenziali, la VU deve rispondere correttamente a qualsiasi indirizzo di tester. L'indirizzo fisico della VU è 0xEE.

▼B

2. TERMINI, DEFINIZIONI E RIFERIMENTI

I protocolli, i messaggi ed i codici di errore si basano in gran parte sul progetto di norma ISO 14299-1 (Road vehicles — Diagnostic systems — Part 1: Diagnostic services, versione 6 del 22 febbraio 2001).

Per gli identificativi di servizio, le richieste di servizio e le relative risposte e per i parametri standard si utilizzano la codifica a byte e i valori esadecimali.

Il termine «tester» si riferisce all'apparecchio utilizzato per l'inserimento dei dati di programmazione/taratura nella VU.

I termini «client» e «server» si riferiscono rispettivamente al tester e alla VU.

Il termine ECU (Electronic Control Unit — Unità elettronica di controllo) si riferisce alla VU.

Riferimenti:

ISO 14230-2: Road Vehicles -Diagnostic Systems — Keyword Protocol 2000- Part 2: Data Link Layer.

First edition: 1999.

Vehicles — Diagnostic.

3. PROSPETTO DEI SERVIZI

3.1. **Servizi disponibili**

La seguente tabella fornisce il prospetto dei servizi disponibili nel tachigrafo e definiti nell'ambito del presente documento.

CPR_004 La tabella indica i servizi disponibili in una sessione diagnostica abilitata.

— La **1[a] colonna** elenca i servizi disponibili.

— La **2[a] colonna** indica il numero della sezione all'interno della presente appendice in cui il servizio è ulteriormente definito.

— La **3[a] colonna** assegna i valori degli identificativi di servizio per i messaggi di richiesta.

— La **4[a] colonna** specifica i servizi di **«StandardDiagnosticSession» (SD)** che devono essere implementati in ogni VU.

— La **5[a] colonna** specifica i servizi di **«ECUAdjustmentSession» (ECUAS)** che devono essere implementati per consentire il controllo della linea dei segnali I/O nel connettore di taratura situato sul pannello frontale della VU.

— La **6[a] colonna** specifica i servizi di **«ECUProgrammingSession» (ECUPS)** che devono essere implementati per consentire la programmazione dei parametri all'interno della VU.

▼B

Tabella 1

Tabella riassuntiva dei valori degli identificativi di servizio

			Sessioni diagnostiche		
Nome del servizio diagnostico	Sezione n.	Val. rich. SID	SD	ECUAS	ECUPS
StartCommunication	4.1	81	■	■	■
StopCommunication	4.2	82	■		
Testerpresent	4.3	3E	■	■	■
StartDiagnosticSession	5.1	10	■	■	■
SecurityAccess	5.2	27	■	■	■
ReadDataByIdentifier	6.1	22	■	■	■
WriteDataByIdentifier	6.2	2E			■
InputOutputControlByIdentifier	7.1	2F		■	

■ Questo simbolo indica che il servizio è obbligatorio nella corrispondente sessione diagnostica. L'assenza di simboli indica che il servizio in questione non è consentito nella corrispondente sessione diagnostica.

3.2. **Codici di risposta**

Per ogni servizio sono definiti appositi codici di risposta.

4. SERVIZI DI COMUNICAZIONE

Determinati servizi sono necessari per stabilire e mantenere le comunicazioni e non compaiono al livello di applicazione. I servizi disponibili sono descritti nella seguente tabella:

Tabella 2

Servizi di comunicazione

Nome del servizio	Descrizione
StartCommunication	Il client richiede l'inizio di una sessione di comunicazione con il/i server.
StopCommunication	Il client richiede il termine della sessione di comunicazione attiva.
Testerpresent	Il client segnala al server di essere ancora in contatto.

CPR_005 Il servizio StartCommunication è utilizzato per iniziare una comunicazione. Per poter eseguire qualsiasi servizio è necessario inizializzare la comunicazione in oggetto ed i parametri di comunicazione devono essere quelli adatti alla modalità richiesta.

4.1. **Servizio StartCommunication**

CPR_006 Alla ricezione di una primitiva di indicazione di StartCommunication, la VU deve verificare se nelle condizioni vigenti sia possibile inizializzare il collegamento della comunicazione richiesta. Le condizioni valide per l'inizializzazione del collegamento sono descritte nel documento della norma ISO 14230-2.

▼B

CPR_007 Quindi la VU deve compiere tutte le azioni necessarie a inizializzare il collegamento ed inviare una primitiva di risposta di StartCommunication con i parametri di Risposta Positiva selezionati.

CPR_008 Se una VU già inizializzata (con qualsiasi sessione diagnostica in corso) riceve un nuovo messaggio StartCommunication Request (ad esempio a causa del recupero dell'errore nel tester) la richiesta deve essere accettata e la VU nuovamente inizializzata.

CPR_009 Se per qualsiasi motivo non è possibile procedere all'inizializzazione del collegamento, la VU deve continuare a funzionare nelle condizioni immediatamente precedenti al tentativo di inizializzazione.

CPR_010 Il messaggio StartCommunication Request deve essere indirizzato fisicamente.

CPR_011 L'inizializzazione della VU per i servizi è effettuata con un metodo di «inizializzazione veloce», che prevede:

— un tempo di inattività del bus prima di qualsiasi attività,

— il susseguente invio da parte del tester di una configurazione di inizializzazione,

— la presenza nella risposta della VU di tutte le informazioni necessarie a stabilire la comunicazione.

CPR_012 Una volta completata l'inizializzazione:

— tutti i parametri di comunicazione sono impostati sui valori predefiniti nella Tabella 4, conformemente ai byte chiave,

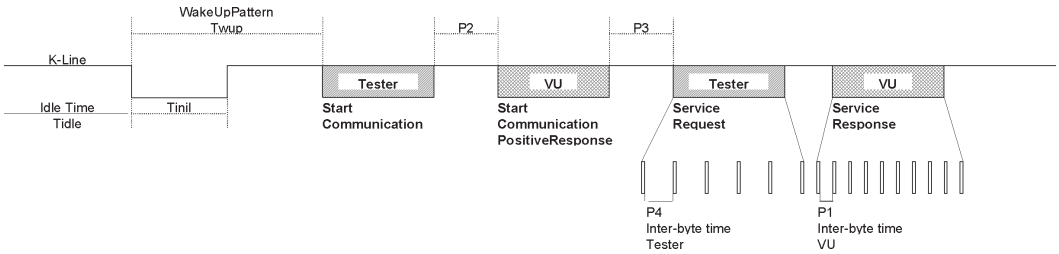
— la VU resta in attesa della prima richiesta da parte del tester,

— la VU risulta in modalità di diagnosi predefinita, ovvero impostata su StandardDiagnosticSession,

— la linea dei segnali I/O di taratura è nell'impostazione predefinita, ovvero disabilitata.

CPR_014 La velocità di trasmissione dei dati (data rate) sulla linea K deve essere di 10 400 baud.

CPR_016 L'inizializzazione veloce è avviata dal tester con la trasmissione della sequenza di riattivazione (Wup) sulla linea K. La sequenza inizia con un tempo breve di Tinil dopo il tempo di inattività sulla linea K. Il tester trasmette quindi il primo bit del servizio StartCommunication dopo un tempo di Twup successivo al primo fronte di discesa.



▼B

CPR_017 I valori di temporizzazione per l'inizializzazione veloce e le comunicazioni in generale sono illustrati nelle seguenti tabelle. Vi sono differenti possibilità per ciò che riguarda il tempo di inattività:

— prima trasmissione seguente l'accensione, Tidle = 300ms,

— dopo il completamento di un servizio StopCommunication, Tidle = P3min,

— dopo il termine della comunicazione a causa di un timeout (superamento del tempo limite) P3max, Tidle = 0.

Tabella 3

Valori di temporizzazione per l'inizializzazione veloce

Parametro		Valore minimo	Valore massimo
Tinil	25 ± 1 ms	24 ms	26 ms
Twup	50 ± 1 ms	49 ms	51 ms

Tabella 4

Valori di temporizzazione della comunicazione

Temporizzazione Parametro	Descrizione parametro	Valore minimo [ms]	Valore massimo [ms]
		min	max
P1	Intervallo di tempo tra byte per la risposta della VU	0	20
P2	Tempo intercorrente tra la richiesta del tester e la risposta della VU o tra due risposte della VU	25	250
P3	Tempo intercorrente tra la conclusione delle risposte della VU e l'inizio di una nuova richiesta del tester	55	5 000
P4	Intervallo di tempo tra byte per la richiesta del tester	5	20

CPR_018 Il formato del messaggio per l'inizializzazione veloce è descritto nelle tabelle seguenti. (NOTE: Hex means hexadecimal)

Tabella 5

Messaggio di StartCommunication Request

Byte #	Denominazione del parametro	Valore esadecimale	Mnemonico
# 1	Byte di formato — indirizzamento fisico	81	FMT
# 2	Byte dell'indirizzo di destinazione	EE	TGT
# 3	Byte dell'indirizzo di provenienza	tt	SRC

▼B

Byte #	Denominazione del parametro	Valore esadecimale	Mnemonico
# 4	**StartCommunication Request Service Id**	**81**	**SCR**
# 5	Totale di controllo	00-FF	CS

Tabella 6

Messaggio di StartCommunication Positive Response

Byte #	Denominazione del parametro	Valore esadecimale	Mnemonico
# 1	Byte di formato — indirizzamento fisico	80	FMT
# 2	Byte dell'indirizzo di destinazione	tt	TGT
# 3	Byte dell'indirizzo di provenienza	EE	SRC
# 4	Byte di lunghezza aggiuntivo	03	LEN
# 5	**StartCommunication Positive Response Service Id**	**C1**	**SCRPR**
# 6	Byte-chiave 1	EA	KB1
# 7	Byte-chiave 2	8F	KB2
# 8	Totale di controllo	00-FF	CS

CPR_019 Non vi è alcuna risposta negativa al messaggio StartCommunication Request; in assenza di messaggi di risposta positiva da trasmettere, la VU non viene inizializzata, rimane in modalità di funzionamento normale e non vi è trasmissione.

4.2. **Servizio StopCommunication**

4.2.1 *Descrizione del messaggio*

Questo servizio conclude una sessione di comunicazione.

CPR_020 Al ricevimento di una primitiva di indicazione di StopCommunication, la VU deve verificare se nelle condizioni vigenti sia possibile concludere la comunicazione in atto. In tal caso la VU compie tutte le azioni necessarie per concludere questa comunicazione.

CPR_021 Se la conclusione della comunicazione risulta attuabile, prima di procedere la VU invia una primitiva di risposta di StopCommunication con i parametri di Positive Response (risposta positiva) selezionati.

CPR_022 Se invece per qualsiasi motivo non è possibile concludere la comunicazione, la VU invia una primitiva di risposta di StopCommunication con il parametro di Negative Response (risposta negativa) selezionato.

CPR_023 In caso di riscontro da parte della VU di un superamento del tempo limite P3max, la comunicazione viene conclusa senza l'invio di una primitiva di risposta.

▼B

4.2.2 *Formato del messaggio*

CPR_024 I formati dei messaggi per le primitive di StopCommunication sono descritti nelle seguenti tabelle.

Tabella 7

Messaggio di StopCommunication Request

Byte #	Denominazione del parametro	Valore esadecimale	Mnemonico
# 1	Byte di formato — indirizzamento fisico	80	FMT
# 2	Byte dell'indirizzo di destinazione	EE	TGT
# 3	Byte dell'indirizzo di provenienza	tt	SRC
# 4	Byte di lunghezza aggiuntivo	01	LEN
# 5	**StopCommunication Request Service Id**	**82**	**SPR**
# 6	Totale di controllo	00-FF	CS

Tabella 8

Messaggio di StopCommunication Positive Response

Byte #	Denominazione del parametro	Valore esadecimale	Mnemonico
# 1	Byte di formato — indirizzamento fisico	80	FMT
# 2	Byte dell'indirizzo di destinazione	tt	TGT
# 3	Byte dell'indirizzo di provenienza	EE	SRC
# 4	Byte di lunghezza aggiuntivo	01	LEN
# 5	**StopCommunication Positive Response Service Id**	**C2**	**SPRPR**
# 6	Totale di controllo	00-FF	CS

Tabella 9

Messaggio di StopCommunication Negative Response

Byte #	Denominazione del parametro	Valore esadecimale	Mnemonico
# 1	Byte di formato — indirizzamento fisico	80	FMT
# 2	Byte dell'indirizzo di destinazione	tt	TGT
# 3	Byte dell'indirizzo di provenienza	EE	SRC
# 4	Byte di lunghezza aggiuntivo	03	LEN

▼B

Byte #	Denominazione del parametro	Valore esadecimale	Mnemonico
# 5	**negative Response Service Id**	**7F**	**NR**
# 6	StopCommunication Request Service Identification	82	SPR
# 7	responseCode = generalReject	10	RC_GR
# 8	Totale di controllo	00-FF	CS

4.2.3 *Definizione dei parametri*

Questo servizio non richiede la definizione di parametri.

4.3. **Servizio TesterPresent**

4.3.1 *Descrizione del messaggio*

Il servizio TesterPresent è impiegato dal tester per indicare al server di essere ancora in collegamento, in modo che il server non torni automaticamente alla modalità di funzionamento normale, interrompendo eventualmente la comunicazione. Tale servizio, attivato periodicamente, mantiene attiva la sessione diagnostica/di comunicazione reimpostando il timer P3 ogni volta che il servizio stesso viene richiesto.

4.3.2 *Formato del messaggio*

CPR_079 I formati dei messaggi per le primitive di TesterPresent sono descritti nelle seguenti tabelle.

Tabella 10

Messaggio di TesterPresent Request

Byte #	Denominazione del parametro	Valore esadecimale	Mnemonico
# 1	Byte di formato — indirizzamento fisico	80	FMT
# 2	Byte dell'indirizzo di destinazione	EE	TGT
# 3	Byte dell'indirizzo di provenienza	tt	SRC
# 4	Byte di lunghezza aggiuntivo	02	LEN
# 5	**TesterPresent Request Service Id**	**3E**	**TP**
# 6	Sub Function = responseRequired = [sì	01	RESPREQ_Y
	no]	02	RESPREQ_NO
# 7	Totale di controllo	00-FF	CS

CPR_080 Se il parametro responseRequired è impostato su «sì» il server deve rispondere con il seguente messaggio di risposta positiva. Se è impostato su «no» il server non invia alcuna risposta.

▼B

Tabella 11

Messaggio di TesterPresent Positive Response

Byte #	Denominazione del parametro	Valore esadecimale	Mnemonico
# 1	Byte di formato — indirizzamento fisico	80	FMT
# 2	Byte dell'indirizzo di destinazione	tt	TGT
# 3	Byte dell'indirizzo di provenienza	EE	SRC
# 4	Byte di lunghezza aggiuntivo	01	LEN
# 5	**TesterPresent Positive Response Service Id**	**7E**	**TPPR**
# 6	Totale di controllo	00-FF	CS

CPR_081 Il presente servizio utilizza i seguenti codici di risposta negativa:

Tabella 12

Messaggio di TesterPresent Negative Response

Byte #	Denominazione del parametro	Valore esadecimale	Mnemonico
# 1	Byte di formato — indirizzamento fisico	80	FMT
# 2	Byte dell'indirizzo di destinazione	tt	TGT
# 3	Byte dell'indirizzo di provenienza	EE	SRC
# 4	Byte di lunghezza aggiuntivo	03	LEN
# 5	**negative Response Service Id**	**7F**	**NR**
# 6	TesterPresent Request Service Identification	3E	TP
# 7	responseCode = [SubFunctionNotSupported-InvalidFormat	12	RC_SFNS_IF
	incorrectMessageLength]	13	RC_IML
# 8	Totale di controllo	00-FF	CS

▼B

5. SERVIZI DI GESTIONE

I servizi disponibili sono descritti nella seguente tabella:

Tabella 13

Servizi di gestione

Nome del servizio	Descrizione
StartDiagnosticSession	Il client richiede l'avvio della sessione diagnostica con una VU.
SecurityAccess	Il client richiede l'accesso a funzioni riservate ad utenti autorizzati.

5.1. **Servizio StartDiagnosticSession**

5.1.1 *Descrizione del messaggio*

CPR_025 Il servizio StartDiagnosticSession serve ad abilitare nel server sessioni diagnostiche differenti. Una sessione diagnostica abilita una serie specifica di servizi secondo la Tabella 17. Nel corso di una sessione possono essere attivati servizi specificamente legati alle necessità del costruttore del veicolo non previsti nel presente documento. Le regole di attuazione devono soddisfare i seguenti requisiti:

— nella VU deve essere sempre attiva una ed una sola sessione diagnostica,

— all'accensione, la Vu deve sempre attivare la StandardDiagnosticSession. Se non viene attivata nessun'altra sessione diagnostica, la StandardDiagnosticSession deve continuare a funzionare fintantoché la VU è accesa,

— se il tester richiede una sessione diagnostica già attiva, la VU deve inviare un messaggio di risposta positiva,

— quando il tester richiede una nuova sessione diagnostica, la VU deve innanzitutto inviare un messaggio di risposta positiva di StartDiagnosticSession prima di attivare la nuova sessione. Se non è in grado di avviare la nuova sessione diagnostica richiesta, la VU deve inviare un messaggio di risposta negativa di StartDiagnosticSession e mantenere attiva la sessione corrente.

CPR_026 L'avvio di una sessione diagnostica deve avere luogo soltanto in presenza di comunicazioni già stabilite tra il client e la VU.

CPR_027 I parametri di temporizzazione definiti nella Tabella 4 devono attivarsi in seguito all'invio completato con successo del messaggio StartDiagnosticSession, con parametro diagnosticSession impostato su «StandardDiagnosticSession» nel messaggio di richiesta nel caso in cui in precedenza sia già stata attivata un'altra sessione diagnostica.

5.1.2 *Formato del messaggio*

CPR_028 I formati dei messaggi per le primitive di StartDiagnosticSession sono descritti nelle seguenti tabelle.

▼B

Tabella 14

Messaggio di StartDiagnosticSession Request

Byte #	Denominazione del parametro	Valore esadecimale	Mnemonico
# 1	Byte di formato — indirizzamento fisico	80	FMT
# 2	Byte dell'indirizzo di destinazione	EE	TGT
# 3	Byte dell'indirizzo di provenienza	tt	SRC
# 4	Byte di lunghezza aggiuntivo	02	LEN
# 5	**StartDiagnosticSession Request Service Id**	**10**	**STDS**
# 6	diagnosticSession = [un valore da Tabella 17]	xx	DS_…
# 7	Totale di controllo	00-FF	CS

Tabella 15

Messaggio di StartDiagnosticSession Positive Response

Byte #	Denominazione del parametro	Valore esadecimale	Mnemonico
# 1	Byte di formato — indirizzamento fisico	80	FMT
# 2	Byte dell'indirizzo di destinazione	tt	TGT
# 3	Byte dell'indirizzo di provenienza	EE	SRC
# 4	Byte di lunghezza aggiuntivo	02	LEN
# 5	**StartDiagnosticSession Positive Response Service Id**	**50**	**STDSPR**
# 6	diagnosticSession = [stesso valore del byte # 6 Tabella 14]	xx	DS_…
# 7	Totale di controllo	00-FF	CS

Tabella 16

Messaggio di StartDiagnosticSession Negative Response

Byte #	Denominazione del parametro	Valore esadecimale	Mnemonico
# 1	Byte di formato — indirizzamento fisico	80	FMT
# 2	Byte dell'indirizzo di destinazione	tt	TGT
# 3	Byte dell'indirizzo di provenienza	EE	SRC

▼B

Byte #	Denominazione del parametro		Valore esadecimale	Mnemonico
# 4	Byte di lunghezza aggiuntivo		03	LEN
# 5	**Negative Response Service Id**		**7F**	**NR**
# 6	StartDiagnosticSession Request Service Id		10	STDS
# 7	ResponseCode =	[subFunctionNotSupported ([a])	12	RC_SFNS
		incorrectMessageLength ([b])	13	RC_IML
		conditionsNotCorrect ([c])	22	RC_CNC
# 8	Totale di controllo		00-FF	CS

([a]) il valore inserito nel byte # 6 del messaggio di richiesta non è supportato, ossia non è contenuto nella Tabella 17,
([b]) la lunghezza del messaggio non è corretta,
([c]) i criteri per la richiesta StartDiagnosticSession non sono soddisfatti.

5.1.3 *Definizione dei parametri*

CPR_029 Il parametro ***diagnosticSession (DS_)*** è utilizzato nell'ambito del servizio StartDiagnosticSession per selezionare il ruolo specifico del/i server. Nel presente documento sono descritte le seguenti sessioni diagnostiche:

Tabella 17

Definizione dei valori DiagnosticSession

Valore esadecimale	Descrizione	Mnemonico
81	**StandardDiagnosticSession** Questa sessione diagnostica abilita tutti i servizi riportati nella **Tabella 1 colonna 4 "SD"**. Tali servizi consentono la lettura dei dati inviati dal server (VU). Questa sessione diagnostica si attiva in seguito all'inizializzazione completata con successo tra client (tester) e server (VU) e può essere sovrascritta dalle altre sessioni diagnostiche descritte nella presente sezione.	**SD**
85	**ECUProgrammingSession** Questa sessione diagnostica abilita tutti i servizi riportati nella **Tabella 1 colonna 6"ECUPS"**. Tali servizi supportano la programmazione della memoria del server (VU). La sessione diagnostica può essere sovrascritta dalle altre sessioni diagnostiche descritte nella presente sezione.	**ECUPS**

▼B

Valore esadecimale	Descrizione	Mnemonico
87	**ECUAdjustmentSession** Questa sessione diagnostica abilita tutti i servizi riportati nella **Tabella 1 colonna 5 "ECUAS".** Tali servizi supportano il controllo messaggi in entrata/uscita del server (VU) e può essere sovrascritta dalle altre sessioni diagnostiche descritte nella presente sezione.	**ECUAS**

5.2. **Servizio SecurityAccess**

La scrittura dei dati di taratura è consentita solo se la VU si trova nella modalità CALIBRATION (TARATURA). Oltre all'inserimento di una carta dell'officina valida all'interno della VU, è necessario inserire nella VU il codice PIN appropriato prima che sia consentito l'accesso alla modalità CALIBRATION.

Quando la VU è in modalità CALIBRATION o CONTROL, è possibile anche l'accesso alla linea dei segnali di entrata/uscita di taratura.

Il servizio SecurityAccess fornisce un mezzo per l'inserimento del codice PIN e per segnalare al tester se la VU si trova in modalità CALIBRATION o meno.

È possibile inserire il codice PIN anche con procedure alternative.

5.2.1 *Descrizione del messaggio*

Il servizio SecurityAccess consiste nell'invio del messaggio SecurityAccess «requestSeed», seguito dal messaggio SecurityAccess «sendKey». È necessario eseguire il servizio in questione successivamente al servizio StartDiagnosticSession.

CPR_033 Il tester deve utilizzare il messaggio SecurityAccess «requestSeed» per verificare se l'unità elettronica di bordo sia pronta a ricevere il codice PIN.

CPR_034 Nel caso in cui l'unità elettronica di bordo si trovi già in modalità CALIBRATION, deve rispondere alla richiesta inviando un «seed» del valore di 0x0000 utilizzando il servizio SecurityAccess Positive Response.

CPR_035 Se l'unità elettronica di bordo è predisposta alla ricezione del codice PIN proveniente da una carta dell'officina per effettuarne la verifica, deve rispondere alla richiesta inviando un «seed» superiore a 0x0000 mediante il servizio SecurityAccess Positive Response.

CPR_036 In caso invece di unità elettronica di bordo non predisposta alla ricezione del codice PIN da parte del tester, a causa dell'inserimento di una carta dell'officina non valida, del mancato inserimento di una carta dell'officina o della predisposizione dell'unità elettronica di bordo alla ricezione del codice PIN attraverso altre procedure, la stessa VU deve rispondere alla richiesta con un messaggio di Negative Response (risposta negativa) contenente un codice di risposta impostato su conditionsNotCorrectOrRequestSequenceError.

CPR_037 Il tester deve utilizzare infine il messaggio SecurityAccess «sendKey» per inviare il codice PIN all'unità elettronica di bordo. Al fine di garantire il tempo necessario per l'esecuzione della procedura di autenticazione della carta, la VU deve impiegare il codice di risposta negativa requestCorrectlyReceived-ResponsePending per prolungare il tempo di risposta. Il tempo massimo di risposta non deve comunque

▼B

superare i 5 minuti. Quando il servizio richiesto è stato completato, la VU deve inviare un messaggio di risposta positiva o negativa, con un codice di risposta diverso dal precedente. Il codice negativo di risposta requestCorrectly-Received-ResponsePending può essere ripetuto dalla VU fintantoché il servizio richiesto non è stato completato ed il messaggio di risposta conclusivo non è stato inviato.

CPR_038 L'unità elettronica di bordo deve rispondere a tale richiesta attraverso il servizio SecurityAccess Positive Response soltanto quando si trova in modalità CALIBRATION.

CPR_039 Nei casi seguenti, l'unità elettronica di bordo deve rispondere alla richiesta in questione con un messaggio di Negative Response (risposta negativa) contenente un codice di risposta impostato su:

— subFunctionNot supported: formato non valido del parametro della sottofunzione (accessType),

— conditionsNotCorrectOrRequestSequenceError: VU non predisposta a ricevere l'inserimento del codice PIN,

— invalidKey: codice PIN non valido e numero massimo di tentativi di verifica del codice PIN non superato,

— exceededNumberOfAttempts: codice PIN non valido e numero massimo di tentativi di verifica del codice PIN superato,

— generalReject: codice PIN corretto ma reciproca autenticazione con la carta dell'officina fallita.

5.2.2 *Formato del messaggio — SecurityAccess — requestSeed*

CPR_040 I formati dei messaggi per le primitive di SecurityAccess «requestSeed» sono descritti nelle seguenti tabelle.

Tabella 18

Messaggio SecurityAccess Request- requestSeed

Byte #	Denominazione del parametro	Valore esadecimale	Mnemonico
# 1	Byte di formato — indirizzamento fisico	80	FMT
# 2	Byte dell'indirizzo di destinazione	EE	TGT
# 3	Byte dell'indirizzo di provenienza	tt	SRC
# 4	Byte di lunghezza aggiuntivo	02	LEN
# 5	**SecurityAccess Request Service Id**	**27**	**SA**
# 6	accessType — requestSeed	7D	AT_RSD
# 7	Totale di controllo	00-FF	CS

▼B

Tabella 19

Messaggio di SecurityAccess — requestSeed Positive Response

Byte #	Denominazione del parametro	Valore esadecimale	Mnemonico
# 1	Byte di formato — indirizzamento fisico	80	FMT
# 2	Byte dell'indirizzo di destinazione	tt	TGT
# 3	Byte dell'indirizzo di provenienza	EE	SRC
# 4	Byte di lunghezza aggiuntivo	04	LEN
# 5	**SecurityAccess Positive Response Service Id**	**67**	**SAPR**
# 6	accessType — requestSeed	7D	AT_RSD
# 7	Seed byte alto	00-FF	SEEDH
# 8	Seed byte basso	00-FF	SEEDL
# 9	Totale di controllo	00-FF	CS

Tabella 20

Messaggio di SecurityAccess Negative Response

Byte #	Denominazione del parametro	Valore esadecimale	Mnemonico
# 1	Byte di formato — indirizzamento fisico	80	FMT
# 2	Byte dell'indirizzo di destinazione	tt	TGT
# 3	Byte dell'indirizzo di provenienza	EE	SRC
# 4	Byte di lunghezza aggiuntivo	03	LEN
# 5	**negativeResponse Service Id**	**7F**	**NR**
# 6	SecurityAccess Request Service Id	27	SA
# 7	responseCode = [conditionsNotCorrectOrRequestSequenceError	22	RC_CNC
	incorrectMessageLength]	13	RC_IML
# 8	Totale di controllo	00-FF	CS

▼B

5.2.3 *Formato del messaggio — SecurityAccess — sendKey*

CPR_041 I formati dei messaggi per le primitive di SecurityAccess «sendKey» sono descritti nelle seguenti tabelle.

Tabella 21

Messaggio di SecurityAccess Request — sendKey Message

Byte #	Denominazione del parametro	Valore esadecimale	Mnemonico
# 1	Byte di formato — indirizzamento fisico	80	FMT
# 2	Byte dell'indirizzo di destinazione	EE	TGT
# 3	Byte dell'indirizzo di provenienza	tt	SRC
# 4	Byte di lunghezza aggiuntivo	m+2	LEN
# 5	**SecurityAccess Request Service Id**	**27**	**SA**
# 6	accessType — sendKey	7E	AT_SK
Dal # 7 al # m+6	Chiave # 1 (alto) … Chiave # m (basso, m deve essere compreso tra 4 e 8)	xx … xx	KEY
# m+7	Totale di controllo	00-FF	CS

Tabella 22

Messaggio di SecurityAccess — sendKey Positive Response

Byte #	Denominazione del parametro	Valore esadecimale	Mnemonico
# 1	Byte di formato — indirizzamento fisico	80	FMT
# 2	Byte dell'indirizzo di destinazione	tt	TGT
# 3	Byte dell'indirizzo di provenienza	EE	SRC
# 4	Byte di lunghezza aggiuntivo	02	LEN
# 5	**SecurityAccess Positive Response Service Id**	**67**	**SAPR**
# 6	accessType — sendKey	7E	AT_SK
# 7	Totale di controllo	00-FF	CS

▼B

Tabella 23

Messaggio di SecurityAccess Negative Response

Byte #	Denominazione del parametro		Valore esadecimale	Mnemonico
# 1	Byte di formato — indirizzamento fisico		80	FMT
# 2	Byte dell'indirizzo di destinazione		tt	TGT
# 3	Byte dell'indirizzo di provenienza		EE	SRC
# 4	Byte di lunghezza aggiuntivo		03	LEN
# 5	**NegativeResponse Service Id**		**7F**	**NR**
# 6	SecurityAccess Request Service Id		27	SA
# 7	ResponseCode =	[generalReject	10	RC_GR
		subFunctionNotSupported	12	RC_SFNS
		incorrectMessageLength	13	RC_IML
		conditionsNotCorrectOrRequestSequenceError	22	RC_CNC
		invalidKey	35	RC_IK
		exceededNumberOfAttempts	36	RC_ENA
		requestCorrectlyReceived-ResponsePending]	78	RC_RCR_RP
# 8	Totale di controllo		00-FF	CS

6. SERVIZI DI TRASMISSIONE DATI

I servizi disponibili sono descritti nella seguente tabella:

Tabella 24

Servizi di trasmissione dati

Nome del servizio	Descrizione
ReadDataByIdentifier	Il client richiede la trasmissione del valore corrente di un record con accesso mediante recordDataIdentifier.
WriteDataByIdentifier	Il client richiede la scrittura di un record con accesso mediante recordDataIdentifier.

▼B

6.1. **ReadDataByIdentifier service**

6.1.1 *Descrizione del messaggio*

CPR_050 Il servizio ReadDataByIdentifier è utilizzato dal client per richiedere valori dei dati registrati dal server. I dati sono identificati mediante parametro recordDataIdentifier. È responsabilità del fabbricante della VU assicurare che quando si utilizza questo servizio lo stato del server sia quello prescritto.

6.1.2 *Formato del messaggio*

CPR_051 I formati dei messaggi per le primitive di ReadDataByIdentifier sono descritti nelle seguenti tabelle.

Tabella 25

Messaggio di ReadDataByIdentifier Request

Byte #	Denominazione del parametro	Valore esadecimale	Mnemonico
# 1	Byte di formato — indirizzamento fisico	80	FMT
# 2	Byte dell'indirizzo di destinazione	EE	TGT
# 3	Byte dell'indirizzo di provenienza	tt	SRC
# 4	Byte di lunghezza aggiuntivo	03	LEN
# 5	**ReadDataByIdentifier Request Service Id**	**22**	**RDBI**
dal # 6 al # 7	recordDataIdentifier = [valore contenuto nella Tabella 28]	xxxx	RDI_…
# 8	Totale di controllo	00-FF	CS

Tabella 26

Messaggio di ReadDataByIdentifier Positive Response

Byte #	Denominazione del parametro	Valore esadecimale	Mnemonico
# 1	Byte di formato — indirizzamento fisico	80	FMT
# 2	Byte dell'indirizzo di destinazione	tt	TGT
# 3	Byte dell'indirizzo di provenienza	EE	SRC
# 4	Byte di lunghezza aggiuntivo	m+3	LEN
# 5	**ReadDataByIdentifier Positive Response Service Id**	**62**	**RDBIPR**
# 6 e # 7	recordDataIdentifier = [stesso valore dei byte # 6 e # 7, Tabella 25]	xxxx	RDI_…

▼B

Byte #	Denominazione del parametro		Valore esadecimale	Mnemonico
Dal # 8 al # m+7	dataRecord[] =	[data#1	xx	DREC_DATA1
		:	:	:
		data#m]	xx	DREC_DATAm
# m+8	Totale di controllo		00-FF	CS

Tabella 27

Messaggio di ReadDataByIdentifier Negative Response

Byte #	Denominazione del parametro		Valore esadecimale	Mnemonico
# 1	Byte di formato — indirizzamento fisico		80	FMT
# 2	Byte dell'indirizzo di destinazione		tt	TGT
# 3	Byte dell'indirizzo di provenienza		EE	SRC
# 4	Byte di lunghezza aggiuntivo		03	LEN
# 5	**NegativeResponse Service Id**		**7F**	**NR**
# 6	ReadDataByIdentifier Request Service Id		22	RDBI
# 7	ResponseCode=	[requestOutOfRange	31	RC_ROOR
		incorrectMessageLength	13	RC_IML
		conditionsNotCorrect]	22	RC_CNC
# 8	Totale di controllo		00-FF	CS

6.1.3 *Definizione dei parametri*

CPR_052 Il parametro ***recordDataIdentifier (RDI_)*** nel messaggio ReadDataByIdentifier Request identifica un record di dati.

CPR_053 I valori di recordDataIdentifier definiti dal presente documento sono illustrati nella tabella seguente.

La tabella relativa a recordDataIdentifier è costituita da quattro colonne e da più righe.

— Nella **1ª colonna (Valore esadecimale)** è riportato il «valore esadecimale» assegnato al parametro recordDataIdentifier specificato nella 3ª colonna.

— La **2ª colonna (Elemento di dati)** specifica l'elemento di dati dell'appendice 1 riferito a recordDataIdentifier (in alcuni casi è necessario transcodificare).

▼B

— La **3ª colonna (Descrizione)** indica il nome dello specifico recordDataIdentifier.

— La **4ª colonna (Mnemonico)** specifica l'identificativo mnemonico del parametro recordDataIdentifier in questione.

Tabella 28

Definizione dei valori recordDataIdentifier

Valore esadecimale	Elemento di dati	Nome del recordDataIdentifier (vedi formato nella sezione 8.2)	Mnemonico
F90B	CurrentDateTime	TimeDate	RDI_TD
F912	HighResOdometer	HighResolutionTotalVehicleDistance	RDI_HRTVD
F918	K-ConstantOfRecordingEquipment	Kfactor	RDI_KF
F91C	L-TyreCircumference	LfactorTyreCircumference	RDI_LF
F91D	W-VehicleCharacteristicConstant	WvehicleCharacteristicFactor	RDI_WVCF
F921	TyreSize	TyreSize	RDI_TS
F922	nextCalibrationDate	NextCalibrationDate	RDI_NCD
F92C	SpeedAuthorised	SpeedAuthorised	RDI_SA
F97D	vehicleRegistrationNation	RegisteringMemberState	RDI_RMS
F97E	VehicleRegistrationNumber	VehicleRegistrationNumber	RDI_ VRN
F190	VehicleIdentificationNumber	VIN	RDI_ VIN

CPR_054 Il parametro ***dataRecord (DREC_)*** è utilizzato nell'ambito del messaggio ReadDataByIdentifier Positive Response per fornire al client (tester) il record dei dati identificato dal parametro recordDataIdentifier. Il formato dei dati è indicato nella sezione 8. Ulteriori dataRecords facoltativi, tra cui i dati specifici in entrata, quelli interni e quelli in uscita della VU sono permessi, ma non sono definiti nel presente documento.

6.2. Servizio WriteDataByIdentifier

6.2.1 *Descrizione del messaggio*

CPR_056 Il servizio WriteDataByIdentifier è utilizzato dal client per registrare valori dei dati nel server. I dati sono identificati mediante parametro recordDataIdentifier. È responsabilità del fabbricante della VU assicurare che quando si utilizza questo servizio lo stato del server sia quello prescritto. Per aggiornare i parametri elencati nella Tabella 28 la VU deve trovarsi in modalità CALIBRATION.

6.2.2 *Formato del messaggio*

CPR_057 I formati dei messaggi per le primitive di WriteDataByIdentifier sono descritti nelle seguenti tabelle.

▼B

Tabella 29

Messaggio di WriteDataByIdentifier Request

Byte #	Denominazione del parametro	Valore esadecimale	Mnemonico
# 1	Byte di formato — indirizzamento fisico	80	FMT
# 2	Byte dell'indirizzo di destinazione	EE	TGT
# 3	Byte dell'indirizzo di provenienza	tt	SRC
# 4	Byte di lunghezza aggiuntivo	m+3	LEN
# 5	**WriteDataByIdentifier Request Service Id**	**2E**	**WDBI**
dal # 6 al # 7	recordDataIdentifier = [valore contenuto nella Tabella 28]	xxxx	RDI_…
#8 to m+7	dataRecord[] = [data#1 : data#m]	xx : xx	DREC_DATA1 : DREC_DATAm
# m+8	Totale di controllo	00-FF	CS

Tabella 30

Messaggio di WriteDataByIdentifier Positive Response

Byte #	Denominazione del parametro	Valore esadecimale	Mnemonico
# 1	Byte di formato — indirizzamento fisico	80	FMT
# 2	Byte dell'indirizzo di destinazione	tt	TGT
# 3	Byte dell'indirizzo di provenienza	EE	SRC
# 4	Byte di lunghezza aggiuntivo	03	LEN
# 5	**WriteDataByIdentifier Positive Response Service Id**	**6E**	**WDBIPR**
dal # 6 al # 7	recordDataIdentifier = [stesso valore dei byte # 6 e # 7, Tabella 29]	xxxx	RDI_…
# 8	Totale di controllo	00-FF	CS

▼B

Tabella 31

Messaggio di WriteDataByIdentifier Negative Response

Byte #	Denominazione del parametro		Valore esadecimale	Mnemonico
# 1	Byte di formato — indirizzamento fisico		80	FMT
# 2	Byte dell'indirizzo di destinazione		tt	TGT
# 3	Byte dell'indirizzo di provenienza		EE	SRC
# 4	Byte di lunghezza aggiuntivo		03	LEN
# 5	**NegativeResponse Service Id**		**7F**	**NR**
# 6	WriteDataByIdentifier Request Service Id		2E	WDBI
# 7	ResponseCode=	[requestOutOfRange	31	RC_ROOR
		incorrectMessageLength	13	RC_IML
		conditionsNotCorrect]	22	RC_CNC
# 8	Totale di controllo		00-FF	CS

6.2.3 *Definizione dei parametri*

Il parametro ***recordDataIdentifier (RDI_)*** è definito nella Tabella 28.

Il parametro ***dataRecord (DREC_)*** è utilizzato nell'ambito del messaggio WriteDataByIdentifier Request per fornire al server (VU) il record dei dati identificato dal parametro recordDataIdentifier. Il formato dei dati è indicato nella sezione 8.

7. CONTROLLO DEGLI IMPULSI DI PROVA — UNITÀ FUNZIONALE DI CONTROLLO DEI SEGNALI DI ENTRATA/USCITA

I servizi disponibili sono descritti nella seguente tabella:

Tabella 32

Unità funzionale di controllo dei segnali di entrata/uscita

Nome del servizio	Descrizione
InputOutputControlByIdentifier	Il client richiede il controllo di uno specifico segnale di entrata/uscita al/dal server.

7.1. **Servizio di InputOutputControlByIdentifier**

7.1.1 *Descrizione del messaggio*

Attraverso il connettore anteriore deve essere possibile effettuare un collegamento che consenta il controllo degli impulsi di prova o la loro verifica costante mediante tester adatto.

▼B

CPR_058 È possibile configurare tale linea dei segnali I/O di taratura mediante comando della linea K, utilizzando il servizio InputOutputControlByIdentifier per selezionare la funzione di entrata o di uscita richiesta per la linea in questione. La linea può assumere i diversi stati indicati di seguito:

— disabled (disabilitata),

— speedSignalInput, in cui la linea dei segnali I/O di taratura è utilizzata per inviare un segnale di velocità (segnale di prova — test signal) al posto del segnale di velocità inviato dal sensore di movimento; questa funzione non è disponibile in modalità CONTROL,

— realTimeSpeedSignalOutputSensor, in cui la linea dei segnali I/O di taratura è utilizzata per inviare il segnale di velocità del sensore di movimento,

— RTCOutput, in cui la linea dei segnali I/O di taratura è utilizzata per inviare il segnale dell'orologio UTC; questa funzione non è disponibile in modalità CONTROL.

CPR_059 L'operazione di configurazione dello stato della linea richiede che l'unità elettronica di bordo abbia iniziato una sessione di regolazione e che sia in modalità CALIBRATION o CONTROL. Se la VU è in modalità CALIBRATION, si possono selezionare i quattro stati della linea (disabled, speedSignalInput, realTimeSpeedSignalOutputSensor, RTCOutput). Se la VU è in modalità CONTROL, si possono selezionare solo due stati della linea (disabled, realTimeSpeedSignalOutputSensor). Al termine della sessione di regolazione o della modalità CALIBRATION o CONTROL, l'unità elettronica di bordo deve verificare che lo stato della linea dei segnali I/O di taratura sia nuovamente «disabled» (disabilitata) (impostazione predefinita).

CPR_060 Se sulla linea del segnale della velocità in tempo reale in entrata alla VU vengono ricevuti degli impulsi di velocità mentre la linea dei segnali I/O di taratura è impostata come entrata, è necessario impostare la linea dei segnali I/O di taratura come uscita o riportarla alla condizione di «disabled» (disabilitata).

CPR_061 La sequenza deve essere la seguente:

— stabilire la comunicazione mediante il servizio StartCommunication,

— iniziare una sessione di regolazione mediante il servizio StartDiagnosticSession e adottare la modalità di funzionamento CALIBRATION o CONTROL (l'ordine di queste due operazioni non è rilevante),

— modificare lo stato del segnale di uscita mediante l'operazione InputOutputControlByIdentifier Service.

7.1.2 *Formato del messaggio*

CPR_062 I formati dei messaggi per le primitive di InputOutputControlByIdentifier sono descritti nelle seguenti tabelle.

▼B

Tabella 33

Messaggio di InputOutputControlByIdentifier Request

Byte #	Denominazione del parametro	Valore esadecimale	Mnemonico
# 1	Byte di formato — indirizzamento fisico	80	FMT
# 2	Byte dell'indirizzo di destinazione	EE	TGT
# 3	Byte dell'indirizzo di provenienza	tt	SRC
# 4	Byte di lunghezza aggiuntivo	xx	LEN
# 5	**InputOutputControlByIdentifier Request Sid**	**2F**	**IOCBI**
# 6 e # 7	InputOutputIdentifier = [CalibrationInputOutput]	F960	IOI_CIO
# 8 o dal # 8 al # 9	ControlOptionRecord = [		COR_…
	inputOutputControlParameter — uno dei valori da Tabella 36	xx	IOCP_…
	controlState — uno dei valori da Tabella 37 (cfr. nota)]	xx	CS_…
# 9 oppure # 10	Totale di controllo	00-FF	CS

Nota: Il parametro controlState è presente soltanto in alcuni casi (cfr. punto 7.1.3).

Tabella 34

Messaggio di InputOutputControlByIdentifier Positive Response

Byte #	Denominazione del parametro	Valore esadecimale	Mnemonico
# 1	Byte di formato — indirizzamento fisico	80	FMT
# 2	Byte dell'indirizzo di destinazione	tt	TGT
# 3	Byte dell'indirizzo di provenienza	EE	SRC
# 4	Byte di lunghezza aggiuntivo	xx	LEN
# 5	**inputOutputControlByIdentifier Positive Response SId**	**6F**	**IOCBIPR**
# 6 e # 7	inputOutputIdentifier = [CalibrationInputOutput]	F960	IOI_CIO
# 8 o dal # 8 al # 9	controlStatusRecord = [		CSR_
	inputOutputControlParameter (stesso valore del byte # 8 Tabella 33)	xx	IOCP_…
	controlState (stesso valore del byte # 9 Tabella 33)] (se del caso)	xx	CS_…
# 9 oppure # 10	Totale di controllo	00-FF	CS

▼B

Tabella 35

Messaggio di InputOutputControlByIdentifier Negative Response

Byte #	Denominazione del parametro	Valore esadecimale	Mnemonico
# 1	Byte di formato — indirizzamento fisico	80	FMT
# 2	Byte dell'indirizzo di destinazione	tt	TGT
# 3	Byte dell'indirizzo di provenienza	EE	SRC
# 4	Byte di lunghezza aggiuntivo	03	LEN
# 5	**negativeResponse Service Id**	**7F**	**NR**
# 6	inputOutputControlByIdentifier Request SId	2F	IOCBI
# 7	responseCode=[		
	incorrectMessageLength	13	RC_IML
	conditionsNotCorrect	22	RC_CNC
	requestOutOfRange	31	RC_ROOR
	deviceControlLimitsExceeded]	7A	RC_DCLE
# 8	Totale di controllo	00-FF	CS

7.1.3 *Definizione dei parametri*

CPR_064 Il parametro ***inputOutputControlParameter (IOCP_)*** è definito nella seguente tabella.

Tabella 36

Definizione dei valori inputOutputControlParameter

Valore esadecimale	Descrizione	Mnemonico
00	**ReturnControlToECU** Questo valore indica al server (VU) che il tester non ha più il controllo della linea dei segnali I/O di taratura.	RCTECU
01	**ResetToDefault** Questo valore indica al server (VU) che si richiede di riportare alla propria impostazione predefinita («reset») la linea dei segnali I/O di taratura.	RTD

▼B

Valore esadecimale	Descrizione	Mnemonico
03	**ShortTermAdjustment** Questo valore indica al server (VU) che si richiede di adeguare la linea dei segnali I/O di taratura al valore indicato nel parametro controlState.	STA

CPR_065 Il parametro ***controlState*** è presente soltanto quando il parametro inputOutputControlParameter è impostato su ShortTermAdjustment ed è definito nella seguente tabella:

Tabella 37

Definizione dei valori controlState

Modalità	Valore esadecimale	Descrizione
Disable	00	La linea I/O è disabilitata (impostazione predefinita)
Enable	01	La linea I/O di taratura è abilitata come speedSignalInput
Enable	02	La linea I/O di taratura è abilitata come realTimeSpeedSignalOutputSensor
Enable	03	La linea I/O di taratura è abilitata come RTCOutput

8. FORMATO DEL PARAMETRO DATARECORDS

La presente sezione contiene informazioni in merito a:

— le regole generali da applicare a serie di parametri trasmessi dalla VU al tester,

— i formati da impiegare nelle operazioni di trasferimento attuate tramite i servizi di trasmissione dati di cui alla sezione 6.

CPR_067 Tutti i parametri indicati devono essere supportati dalla VU.

CPR_068 I dati trasmessi dalla VU al tester in risposta ad un messaggio di richiesta devono essere di tipo misurato (ovvero valore corrente del parametro richiesto, secondo quanto misurato o osservato dalla VU).

8.1. **Valori limite dei parametri trasmessi**

CPR_069 Tabella 38 definisce i limiti adottati per determinare la validità dei parametri trasmessi.

CPR_070 I valori della serie «codice di errore» permettono alla VU di indicare immediatamente che non sono al momento disponibili dati parametrici validi, in seguito ad errori intervenuti nel tachigrafo.

CPR_071 I valori della serie «non disponibile» permettono alla VU di trasmettere un messaggio che contiene un parametro non disponibile o non supportato dal modulo in questione. I valori della serie «non richiesto» permettono di trasmettere messaggi di comando e di identificare i parametri per i quali non ci si attende alcuna risposta dall'apparecchio cui sono inviati.

▼B

CPR_072 Se il malfunzionamento di un componente non permette la trasmissione di dati validi per un determinato parametro, al loro posto deve essere trasmesso il codice di errore contenuto nella Tabella 38. Se tuttavia il dato misurato o calcolato risulta valido, benché superi i valori limite stabiliti per lo specifico parametro, non deve essere impiegato alcun codice d'errore. I dati devono essere trasmessi utilizzando, a seconda del caso, il valore parametrico massimo o minimo.

Tabella 38

Serie di dataRecords

Nome della serie	1 byte (Valore esadecimale)	2 byte (Valore esadecimale)	4 byte (Valore esadecimale)	ASCII
Segnale valido	da 00 a FA	da 0000 a FAFF	da 00000000 a FAFFFFFF	da 1 a 254
Codice specifico del parametro	FB	da FB00 a FBFF	da FB000000 a FBFFFFFF	nessuno
Serie riservata per futuri indicatori (in bit)	da FC a FD	da FC00 a FDFF	da FC000000 a FDFFFFFF	nessuna
Codice di errore	FE	da FE00 a FEFF	da FE000000 a FEFFFFFF	0
Non disponibile o non richiesto	FF	da FF00 a FFFF	da FF000000 a FFFFFFFF	FF

CPR_073 Se i parametri sono codificati in ASCII, il carattere ASCII «*» è riservato quale delimitatore.

8.2. **Formato del parametro dataRecords**

Le seguenti tabelle da Tabella 39 a Tabella 42 indicano i formati da impiegare utilizzando i servizi ReadDataByIdentifier e WriteDataByIdentifier.

CPR_074 La Tabella 39 indica lunghezza, risoluzione e limiti operativi della serie per ogni parametro identificato da un recordDataIdentifier:

Tabella 39

Formati dei dataRecords

Denominazione del parametro	Lunghezza dati (in byte)	Risoluzione	Limiti operativi
TimeDate	8	Cfr. informazioni dettagliate in Tabella 40	
HighResolutionTotalVehicleDistance	4	5 m/bit gain, 0 m offset	da 0 a + 21 055 406 km
Kfactor	2	0,001 impulsi/m /bit gain, 0 offset	da 0 a 64,255 impulsi/m
LfactorTyreCircumference	2	0,125 10^{-3} m /bit gain, 0 offset	da 0 a 8,031 m
WvehicleCharacteristicFactor	2	0,001 impulsi/m /bit gain, 0 offset	da 0 a 64,255 impulsi/m
TyreSize	15	ASCII	ASCII
NextCalibrationDate	3	Cfr. informazioni dettagliate in Tabella 41	
SpeedAuthorised	2	1/256 km/h/bit gain, 0 offset	da 0 a 250,996 km/h

▼B

Denominazione del parametro	Lunghezza dati (in byte)	Risoluzione	Limiti operativi
RegisteringMemberState	3	ASCII	ASCII
VehicleRegistrationNumber	14	Cfr. informazioni dettagliate in Tabella 42	
VIN	17	ASCII	ASCII

CPR_075 La Tabella 40 indica i formati dei diversi tipi di byte impiegati dal parametro TimeDate:

Tabella 40

Formato dettagliato del parametro TimeDate (recordDataIdentifier value # F90B)

Byte	Definizione dei parametri	Risoluzione	Limiti operativi
1	Secondi	0,25 s/bit gain, 0 s offset	da 0 a 59,75s
2	Minuti	1 min/bit gain, 0 min offset	da 0 a 59 min
3	Ore	1 h/bit gain, 0 h offset	da 0 a 23 ore
4	Mese	1 mese/bit gain, 0 mese offset	da 1 a 12 mesi
5	Giorno	0,25 giorni/bit gain, 0 giorni offset (cfr. la nota seguente Tabella 41)	da 0,25 a 31,75 giorni
6	Anno	1 anno/bit gain, + 1985 anno offset (cfr. la nota seguente Tabella 41)	dall'anno 1985 al 2235
7	Local Minute Offset	1 min/bit gain, –125 min offset	da – 59 a + 59 min
8	Local Hour Offset	1 h/bit gain, – 125 h offset	da – 23 a + 23 ore

CPR_076 La Tabella 41 indica i formati dei diversi tipi di byte impiegati dal parametro NextCalibrationDate.

Tabella 41

Formato dettagliato del parametro NextCalibrationDate (recordDataIdentifier value # F922)

Byte	Definizione dei parametri	Risoluzione	Limiti operativi
1	Mese	1 mese/bit gain, 0 mese offset	da 1 a 12 mesi
2	Giorno	0,25 giorni/bit gain, 0 giorni offset (cfr. la nota seguente)	da 0,25 a 31,75 giorni
3	Anno	1 anno/bit gain, +1985 anno offset (cfr. la nota seguente)	dall'anno 1985 al 2235

▼B

Nota relativa all'impiego del parametro «Giorno»:

1) Nella data, il valore 0 non è un valore valido. I valori 1, 2, 3 e 4 sono utilizzati per identificare il primo giorno del mese, 5, 6, 7 e 8 per identificare il secondo e così via.

2) Tale parametro non influenza né modifica il parametro relativo all'ora.

Nota relativa all'impiego del parametro «Anno»:

il valore 0 corrisponde all'anno 1985, il valore 1 corrisponde al 1986 e così via.

CPR_078 La Tabella 42 indica i formati dei diversi tipi di byte impiegati dal parametro VehicleRegistrationNumber.

Tabella 42

Formato dettagliato del parametro VehicleRegistrationNumber (recordDataIdentifier value # F97E)

Byte	Definizione dei parametri	Risoluzione	Limiti operativi
1	Pagina di codice (definito nell'appendice 1)	ASCII	da 01 a 0A
da 2 a 14	Vehicle Registration Number (numero di immatricolazione) (definito nell'appendice 1)	ASCII	ASCII

▼B

Appendice 9.

OMOLOGAZIONE ELENCO DELLE PROVE MINIME PRESCRITTE

INDICE

1. INTRODUZIONE

2. PROVE FUNZIONALI PER L'UNITÀ ELETTRONICA DI BORDO

3. PROVE FUNZIONALI PER IL SENSORE DI MOVIMENTO

4. PROVE FUNZIONALI PER LE CARTE TACHIGRAFICHE

5. PROVE DEL DISPOSITIVO GNSS ESTERNO

6. PROVE DEL DISPOSITIVO DI COMUNICAZIONE REMOTA

7. PROVE FUNZIONALI SU CARTA

8. PROVE DI INTEROPERABILITÀ

1. INTRODUZIONE

1.1. **Omologazione**

L'omologazione CE di un apparecchio di controllo (o suo componente) o di una carta tachigrafica si basa su:

— una **certificazione di sicurezza**, basata sulle specifiche dei criteri comuni rispetto ad un obiettivo di sicurezza pienamente conforme all'appendice 10 del presente allegato (da completare/modificare),

— una **certificazione funzionale**, effettuata dalle autorità competenti degli Stati membri, che attesta la conformità dell'elemento sottoposto alle prove ai requisiti del presente allegato in termini di funzioni eseguite, precisione delle misurazioni e caratteristiche ambientali,

— una **certificazione di interoperabilità**, effettuata dall'organismo competente, che attesta la piena interoperabilità dell'apparecchio di controllo (o carta tachigrafica) con i modelli di carta tachigrafica (o apparecchio di controllo) necessari (cfr. capitolo 8 del presente allegato).

La presente appendice specifica le prove minime che le autorità competenti degli Stati membri devono eseguire nell'ambito delle prove funzionali, nonché le prove minime che l'organismo competente deve eseguire nell'ambito delle prove di interoperabilità. Le procedure da seguire per l'esecuzione delle prove e il tipo di prove non sono ulteriormente specificati.

Gli aspetti concernenti la certificazione della sicurezza non sono contemplati dalla presente appendice. Se alcune prove richieste per l'omologazione vengono effettuate nell'ambito delle procedure di valutazione e certificazione della sicurezza, non è necessario che tali prove vengano ripetute. In quest'ultimo caso, solo i risultati delle prove della sicurezza possono essere oggetto di controlli. A titolo d'informazione, nella presente appendice i requisiti che devono essere sottoposti a prova (o che sono strettamente collegati alle prove previste) nell'ambito della certificazione della sicurezza sono segnalati con un asterisco «*».

I requisiti numerati si riferiscono all'allegato, mentre quelli non numerati si riferiscono alle altre appendici (ad es. PIC_001 si riferisce al requisito PIC_001 dell'appendice 3 Pittogrammi).

La presente appendice esamina separatamente l'omologazione del sensore di movimento, dell'unità elettronica di bordo e del dispositivo GNSS esterno come componenti dell'apparecchio di controllo. Ogni componente riceve il

▼B

proprio certificato di omologazione in cui vengono indicati gli altri componenti compatibili. La prova funzionale del sensore di movimento (o del dispositivo GNSS esterno) è eseguita insieme all'unità elettronica di bordo e viceversa.

Non è prescritta l'interoperabilità tra ogni modello di sensore di movimento (o dispositivo GNSS esterno) e ogni modello di unità elettronica di bordo. Quindi l'omologazione di un sensore di movimento (o dispositivo GNSS esterno) può essere accordata solo se abbinata all'omologazione di una unità elettronica di bordo e viceversa.

1.2. **Riferimenti**

Nella presente appendice si rimanda alle norme seguenti.

IEC 60068-2-1: Environmental testing — Part 2-1: Tests — Test A: Cold (Prove ambientali — Parte 2-1: Prove — Prova A: Freddo)

IEC 60068-2-2: Basic environmental testing procedures; part 2: tests; tests B: dry heat (sinusoidal) [Procedure di prove ambientali di base; Prove; Prove B: Calore secco (sinusoidale)].

IEC 60068-2-6: Environmental testing — Part 2: Tests — Test Fc: Vibration (Prove ambientali — Parte 2: Prove — Prova Fc: Vibrazioni)

IEC 60068-2-14: Environmental testing; Part 2-14: Tests; Test N: Change of temperature (Prove ambientali; Parti 2-14: Prove; Prova N: Cambiamento di temperatura)

IEC 60068-2-27: Environmental testing. Part 2: Tests. Test Ea and guidance: Shock (Prove ambientali. Parte 2: Prove. Prova Ea e guida: Urti)

IEC 60068-2-30: Environmental testing — Part 2-30: Tests — Test Db: Damp heat, cyclic (12 h + 12 h cycle) [Prove ambientali — Parti 2-30: Prove — Prova Db: Calore umido, ciclico (ciclo di 12 h + 12 h)]

IEC 60068-2-64: Environmental testing — Part 2-64: Tests — Test Fh: Vibration, broadband random and guidance (Prove ambientali — Parti 2-64: Prove — Prova Fh: Vibrazioni, a banda larga casuali, e guida)

IEC 60068-2-78 Environmental testing — Part 2-78: Tests — Test Cab: Damp heat, steady state (Prove ambientali — Parti 2-78: Prove — Prova Cab: Calore umido, statico)

ISO 16750-3 — Mechanical loads (2012-12) (Carichi meccanici)

ISO 16750-4 — Climatic loads (2010-04) (Carichi climatici)

ISO 20653: Road vehicles — Degree of protection (IP code) — Protection of electrical equipment against foreign objects, water and access [Veicoli stradali — Grado di protezione (codice IP) — Protezione delle apparecchiature da oggetti estranei, dall'acqua e dall'accesso]

ISO 10605:2008 + Technical Corrigendum (rettifica tecnica): 2010 + AMD1:2014 Road vehicles — Test methods for electrical disturbances from electrostatic discharge (Veicoli stradali — Metodi di prova dei disturbi elettrici da scariche elettrostatiche)

ISO 7637-1:2002 + AMD1: 2008 Road vehicles — Electrical disturbances from conduction and coupling — Part 1: Definitions and general considerations (Veicoli stradali — Disturbi elettrici da conduzione e accoppiamento — Parte 1: Definizioni e considerazioni generali).

ISO 7637-2 Road vehicles — Electrical disturbances from conduction and coupling — Part 2: Definitions and general considerations (Veicoli stradali — Disturbi elettrici da conduzione e accoppiamento — Parte 2: Definizioni e considerazioni generali).

ISO 7637-3 Road vehicles — Electrical disturbances from conduction and coupling — Part 3: Electrical transient transmission by capacitive and inductive coupling via lines other than supply lines (Veicoli stradali — Disturbi elettrici da conduzione e accoppiamento — Parte 3: Trasmissione di transitori elettrici mediante accoppiamento capacitivo e induttivo attraverso linee diverse da quelle di alimentazione).

ISO/IEC 7816-1 Identification cards — Integrated circuit(s) cards with contacts — Part 1: Physical characteristics. (Carte di identificazione — Carte a circuito integrato con contatti — Parte 1: Caratteristiche fisiche).

▼B

ISO/IEC 7816-2 Information technology — Identification cards — Integrated circuit(s) cards with contacts — Part 2: Dimensions and location of the contacts (Tecnologia dell'informazione — Carte di identificazione — Carte a circuito integrato con contatti — Parte 2: Dimensioni e posizione dei contatti).

ISO/IEC 7816-3 Information technology — Identification cards — Integrated circuit(s) cards with contacts — Part 3: Electronic signals and transmission protocol (Tecnologia dell'informazione — Carte di identificazione — Carte a circuito integrato con contatti — Parte 3: Segnali elettronici e protocollo di trasmissione).

ISO/IEC 10373-1:2006 + AMD1:2012 Identification cards — Test methods — Part 1: General characteristics (Carte di identificazione — Metodi di prova — Parte 1: Caratteristiche generali)

ISO/IEC 10373-3:2010 + Technical Corrigendum (rettifica tecnica):2013 Identification cards — Test methods — Part 3: Integrated circuit cards with contacts and related interface devices (Carte di identificazione — Metodi di prova — Parte 3: Carte a circuito integrato con contatti e relative interfacce)

ISO 16844-3:2004, Cor 1:2006 Road vehicles — Tachograph systems — Part 3: Motion sensor interface (with vehicle units) [Veicoli stradali — Sistemi tachigrafici — Parte 3: Interfaccia del sensore di movimento (con le unità elettroniche di bordo)].

ISO 16844-4 Road vehicles — Tachograph systems — Part 4: CAN interface (Veicoli stradali — Sistemi tachigrafici — Parte 4: Interfaccia CAN)

ISO 16844-6 Road vehicles — Tachograph systems — Part 6: Diagnostics (Veicoli stradali — Sistemi tachigrafici — Parte 6: Diagnostica)

ISO 16844-7 Road vehicles — Tachograph systems — Part 7: Parameters (Veicoli stradali — Sistemi tachigrafici — Parte 7: Parametri)

ISO 534 Paper and board – Determination of thickness, density and specific volume (Carta e cartone – Determinazione dello spessore, della densità e del volume specifico)

UN ECE R10 Uniform provisions concerning the approval of vehicles with regard to electromagnetic compatibility (United Nation Economic Commission for Europe) [Disposizioni uniformi relative all'omologazione di veicoli relativamente alla loro compatibilità elettromagnetica (commissione economica per l'Europa delle Nazioni Unite)]

2. PROVE FUNZIONALI PER L'UNITÀ ELETTRONICA DI BORDO

N.	Prova	Descrizione	Requisiti applicabili
1	**Esame amministrativo**		
1.1	Documentazione	Correttezza della documentazione	
1.2	Risultati delle prove del fabbricante	Risultati delle prove effettuate dal fabbricante durante l'integrazione Attestati cartacei	88, 89,91
2	**Esame visivo**		
2.1	Conformità alla documentazione		
2.2	Identificazione/marcature		da 224 a 226
2.3	Materiali		da 219 a 223
2.4	Sigillatura		398, da 401 a 405
2.5	Interfacce esterne		
3	**Prove funzionali**		
3.1	Funzioni		03, 04, 05, 07, 382,
3.2	Modalità di funzionamento		da 09 a 11*, 132, 133
3.3	Funzioni e diritti di accesso ai dati		12* 13*,, 382, 383, da 386 a 389
3.4	Controllo inserimento ed estrazione carte		15, 16, 17, 18, 19*, 20*, 132
3.5	Misurazione di velocità e distanza		da 21 a 31

▼B

N.	Prova	Descrizione	Requisiti applicabili
3.6	Misurazione del tempo (prova effettuata a 20 °C)		da 38 a 43
3.7	Controllo delle attività del conducente		da 44 a 53, 132
3.8	Controllo delle condizioni di guida		54, 55, 132
3.9	Immissioni manuali		da 56 a 62
3.10	Gestione dei blocchi di un'impresa		da 63 a 68
3.11	Verifica delle attività di controllo		69, 70
3.12	Rilevamento di anomalie e/o guasti		da 71 a 88 132
3.13	Dati di identificazione dell'apparecchio		93*, 94*, 97, 100
3.14	Dati relativi all'inserimento e all'estrazione della carta del conducente		da 102* a 104*
3.15	Dati relativi all'attività del conducente		da 105* a 107*
3.16	Dati sui luoghi e sulle posizioni		da 108* a 112*
3.17	Dati relativi all'odometro		da 113* a 115*
3.18	Dati dettagliati relativi alla velocità		116*
3.19	Dati relativi alle anomalie		117*
3.20	Dati relativi ai guasti		118*
3.21	Dati relativi alla taratura		da 119* a 121*
3.22	Dati relativi alla regolazione dell'ora		124*, 125*
3.23	Dati relativi alle attività di controllo		126*, 127*
3.24	Dati relativi ai blocchi di un'impresa		128*
3.25	Dati relativi al trasferimento		129*
3.26	Dati relativi a condizioni particolari		130*, 131*
3.27	Registrazione e memorizzazione nelle carte tachigrafiche		134, 135, 136*, 137*, 139*, 140, 141 142, 143, 144*, 145*, 146*, 147, 148
3.28	Visualizzazione		90, 132, da 149 a 166 PIC_001, DIS_001
3.29	Stampa		90, 132, da 167 a 179, PIC_001, da PRT_001 a PRT_014
3.30	Avviso		132, da 180 a 189, PIC_001
3.31	Trasferimento di dati verso un dispositivo esterno		90, 132, da 190 a 194
3.32	Comunicazione remota per controlli su strada mirati		da 195 a 197
3.33	Trasmissione di dati ad altri dispositivi esterni		198, 199

▼B

N.	Prova	Descrizione	Requisiti applicabili
3.34	Taratura		da 202 a 206*, 383, 384, da 386 a 391
3.35	Controlli su strada della taratura		da 207 a 209
3.36	Regolazione dell'ora		da 210 a 212*
3.37	Non interferenza di funzioni supplementari		06, 425
3.38	Interfaccia del sensore di movimento		02, 122
3.39	Dispositivo GNSS esterno		03, 123
3.40	Verificare che la VU individui, registri e memorizzi le anomalie e/o i guasti definiti dal fabbricante della VU quando un sensore di movimento abbinato reagisce ai campi magnetici che ostacolano il rilevamento dei dati di movimento del veicolo.		217
3.41	Cypher suite e parametri Domain standardizzati		CSM_48, CSM_50
4	**Prove ambientali**		
4.1	Temperatura	Verificare la funzionalità mediante: prova conformemente alla norma ISO 16750-4, capitolo 5.1.1.2: Prova di funzionamento a bassa temperatura (72 h @ -20 °C) Questa prova si riferisce alla norma IEC 60068-2-1: Prove ambientali — Parti 2-1: Prove — Prova A: Freddo Prova conformemente a ISO 16750-4: Capitolo 5.1.2.2: Prova di funzionamento ad alta temperatura (72 h a 70 °C) Questa prova si riferisce alla norma IEC 60068-2-2: Procedure di prove ambientali di base; parte 2: prove; prove B: calore secco Prova conformemente a ISO 16750-4: Capitolo 5.3.2 Cambiamento rapido di temperatura con durata specifica della transizione (– 20 °C/ 70 °C, 20 cicli, tempo di permanenza di 2h a ogni temperatura) Si può effettuare una serie ridotta di prove (fra quelle definite alla sezione 3 della presente tabella) alla temperatura più bassa, alla temperatura più alta e durante i cicli di temperature	213
4.2	Umidità	Verificare che l'unità elettronica di bordo possa sopportare un'umidità ciclica (prova termica), mediante prova Db, IEC 60068-2-30, sei cicli di 24 ore, ciascuno con temperature che variano da + 25 °C a + 55 °C ed un'umidità relativa del 97 % a + 25 °C e del 93 % a + 55 °C	214

▼B

N.	Prova	Descrizione	Requisiti applicabili
4.3	Prove meccaniche	1. Vibrazioni sinusoidali. Verificare che l'unità elettronica di bordo possa sopportare vibrazioni sinusoidali aventi le seguenti caratteristiche: spostamento costante tra 5 e 11 Hz: picco di 10 mm accelerazione costante tra 11 e 300 Hz: 5 g Questo requisito si verifica in base alla norma IEC 60068-2-6, prova Fc, con una durata minima della prova di 3×12 ore (12 ore per asse) La norma ISO 16750-3 non prescrive una prova di vibrazione sinusoidale per i dispositivi posizionati nella cabina del veicolo staccata. 2. Vibrazioni casuali: Prova conformemente a ISO 16750-3: Capitolo 4.1.2.8: Prova VIII: Veicolo commerciale, cabina del veicolo staccata Prova delle vibrazioni casuali, 10…2 000 Hz, RMS verticale 21,3 m/s^2, RMS longitudinale 11,8 m/s^2, RMS laterale 13,1 m/s^2, 3 assi, 32 h per asse, incluso il ciclo di temperatura -20…70 °C. Questa prova si riferisce alla norma IEC 60068-2-64: Prove ambientali — Parti 2-64: Prove — Prova Fh: Vibrazioni, a banda larga casuali e guida 3. Urti: urto meccanico con mezzo seno 3g conformemente a ISO 16750. Le prove sopra descritte sono effettuate su campioni diversi del modello di apparecchio sottoposto alle prove	219
4.4	Protezione contro l'acqua e i corpi estranei	Prova conformemente a ISO 20653: Veicoli stradali — Grado di protezione (codice IP) — Protezione delle apparecchiature da oggetti estranei, dall'acqua e dall'accesso (senza modifica dei parametri); Valore minimo IP 40	220, 221
4.5	Protezione contro sovratensione	Verificare che l'unità elettronica di bordo possa sopportare un'alimentazione di: Versioni da 24 V: 34V a + 40 °C 1 ora Versioni da 12 V: 17V a + 40 °C 1 ora (ISO 16750-2)	216

▼B

N.	Prova	Descrizione	Requisiti applicabili
4.6	Protezione contro polarità inversa	Verificare che l'unità elettronica di bordo possa sopportare un'inversione dell'alimentazione (ISO 16750-2)	216
4.7	Protezione contro cortocircuiti	Verificare che i segnali in ingresso e in uscita siano protetti contro i cortocircuiti rispetto ad alimentazione e massa (ISO 16750-2)	216
5	**Prove della compatibilità elettromagnetica**		
5.1	Emissioni irradiate e sensibilità ai disturbi	Conformità al regolamento ECE R10	218
5.2	Scariche elettrostatiche	Conformità alla norma ISO 10605:2008 + Rettifica tecnica:2010 + AMD1:2014: +/– 4kV per il contatto e +/– 8kV per lo scarico di aria	218
5.3	Sensibilità ai transitori condotti nell'alimentazione	Per le versioni da 24 V: conformità a ISO 7637-2 + regolamento ECE n. 10 Rev. 3: impulso 1a: Vs = – 450V Ri = 50 ohm impulso 2a: Vs = + 37V Ri = 2 ohm impulso 2b: Vs = + 20V R i= 0,05 ohm impulso 3a: Vs = – 150V Ri = 50 ohm impulso 3b: Vs = + 150V Ri = 50 ohm impulso 4: Vs =– 16V Va = – 12V t6 = 100ms impulso 5: Vs = + 120V Ri = 2,2 ohm td = 250ms Per le versioni da 12 V: conformità a ISO 7637-1 + regolamento ECE n. 10 Rev. 3: impulso 1: Vs = – 75V Ri = 10 ohm impulso 2a: Vs = + 37V Ri = 2 ohm impulso 2b: Vs = + 10V Ri = 0,05 ohm impulso 3a: Vs = – 112V Ri = 50 ohm impulso 3b: Vs = + 75V Ri = 50 ohm impulso 4: Vs = – 6V Va = – 5V t6 = 15ms impulso 5: Vs = + 65V Ri = 3ohm td = 100ms L'impulso 5 va controllato solo per le unità elettroniche di bordo destinate al montaggio in veicoli per i quali non è prevista una protezione comune esterna contro le cadute della potenza di carico Per la proposta relativa alle cadute della potenza di carico fare riferimento alla norma ISO 16750-2, 4a edizione, capitolo 4.6.4.	218

▼B

3. PROVE FUNZIONALI PER IL SENSORE DI MOVIMENTO

N.	Prova	Descrizione	Requisiti applicabili
1.	**Esame amministrativo**		
1.1	Documentazione	Correttezza della documentazione	
2.	**Esame visivo**		
2.1.	Conformità alla documentazione		
2.2.	Identificazione/marcature		225, 226,
2.3	Materiali		da 219 a 223
2.4.	Sigillatura		398, da 401 a 405
3.	**Prove funzionali**		
3.1	Dati di identificazione del sensore		da 95 a 97*
3.2	Abbinamento sensore di movimento — unità elettronica di bordo		122*, 204
3.3	Rilevamento del movimento Precisione della misurazione del movimento		da 30 a 35
3.4	Interfaccia dell'unità elettronica di bordo		02
3.5	Verificare che il sensore di movimento sia insensibile ai campi magnetici costanti. In alternativa, verificare che il sensore di movimento reagisca ai campi magnetici costanti che ostacolano il rilevamento dei dati di movimento del veicolo in modo che la VU collegata possa individuare, registrare e memorizzare i guasti del sensore		217
4.	**Prove ambientali**		
4.1	Temperatura di esercizio	Verificare la funzionalità (secondo quanto definito alla prova n. 3.3) nel campo di temperatura [- 40 °C; + 135 °C], mediante: prova Ad, IEC 60068-2-1, per una durata di 96 ore alla temperatura più bassa To_{min}, prova Bd, IEC 60068-2-2, per una durata di 96 ore alla temperatura più alta To_{max} Prova conformemente a ISO 16750-4: Capitolo 5.1.1.2: Prova di funzionamento a bassa temperatura (24 h @ – 40 °C) Questa prova si riferisce alla norma IEC 60068-2-1: Prove ambientali — Parti 2-1: Prove — Prova A: Freddo, prova Bd, IEC 68-2-2, per una durata di 96 ore alla temperatura più bassa di – 40 °C. Prova conformemente a ISO 16750-4: Capitolo 5.1.2.2: Prova di funzionamento ad alta temperatura (96 h @135 °C) Questa prova si riferisce alla norma IEC 60068-2-2: Procedure di prove ambientali di base; parte 2: prove; prove B: calore secco	213

▼B

N.	Prova	Descrizione	Requisiti applicabili
4.2	Cicli di temperature	Prova conformemente a ISO 16750-4: Capitolo 5.3.2 Cambiamento rapido di temperatura con durata specifica della transizione (– 40 °C/ 135 °C, 20 cicli, tempo di permanenza di 30 min a ogni temperatura) IEC 60068-2-14: Prove ambientali; Parti 2-14: Prove; Prova N: Variazione di temperatura	213
4.3	Cicli di umidità	Verificare la funzionalità (secondo quanto definito alla prova n. 3.3), mediante prova Db, IEC 60068-2-30, sei cicli di 24 ore, ciascuno con temperature che variano da + 25 °C a + 55 °C e un'umidità relativa del 97 % a + 25 °C e del 93 % a + 55 °C	214
4.4	Vibrazioni	ISO 16750-3: Capitolo 4.1.2.6: Prova VI: Veicolo commerciale, motore, cambio Prova delle vibrazioni in modalità mista, tra cui a) Prova delle vibrazioni sinusoidali, 20...520 Hz, 11,4 …120 m/s^2, <= 0,5 oct/min b) Prova delle vibrazioni casuali, 10...2 000 Hz, RMS 177 m/s^2 94 h per asse, incluso il ciclo di temperatura -20…70 °C Questa prova si riferisce alla norma IEC 60068-2-80: Prove ambientali — Parti 2-80: Prove — Prova Fi: Vibrazioni — Modalità mista	219
4.5	Urti meccanici	ISO 16750-3: Capitolo 4.2.3 Prova VI: Prove per i dispositivi nel o sul cambio urto mezzo-sinusoidale, accelerazione da definire nell'intervallo 3 000…15 000 m/s^2, durata dell'impulso da definire, tuttavia < 1 ms, numero di urti: da definire Questa prova si riferisce alla norma IEC 60068-2-27: Prove ambientali. Parte 2: Prove. Prova Ea e guida: Urti.	219
4.6	Protezione contro l'acqua e i corpi estranei	Prova conformemente a ISO 20653: Veicoli stradali — Grado di protezione (codice IP) — Protezione delle apparecchiature da oggetti estranei, dall'acqua e dall'accesso (Valore target IP 64)	220, 221
4.7	Protezione contro polarità inversa	Verificare che il sensore di movimento possa sopportare un'inversione dell'alimentazione	216
4.8	Protezione contro cortocircuiti	Verificare che i segnali in ingresso e in uscita siano protetti contro i cortocircuiti rispetto ad alimentazione e massa	216

▼B

N.	Prova	Descrizione	Requisiti applicabili
5.	**Compatibilità elettromagnetica**		
5.1	Emissioni irradiate e sensibilità ai disturbi	Verifica della conformità al regolamento ECE R10	218
5.2	Scariche elettrostatiche	Conformità alla norma ISO 10605:2008 + Rettifica tecnica:2010 + AMD1:2014: +/– 4kV per il contatto e +/– 8kV per lo scarico di aria	218
5.3	Sensibilità ai transitori condotti nelle linee dati	Per le versioni da 24 V: conformità a ISO 7637-2 + regolamento ECE n. 10 Rev. 3: impulso 1a: Vs = – 450V Ri = 50 ohm impulso 2a: Vs = + 37V Ri = 2 ohm impulso 2b: Vs = + 20V Ri = 0,05 ohm impulso 3a: Vs = – 150V Ri = 50 ohm impulso 3b: Vs = + 150V Ri = 50 ohm impulso 4: Vs = – 16V Va = – 12V t6 = 100ms impulso 5: Vs = + 120V Ri = 2,2 ohm td = 250ms Per le versioni da 12 V: conformità a ISO 7637-1 + regolamento ECE n. 10 Rev. 3: impulso 1: Vs = – 75V Ri = 10 ohm impulso 2a: Vs = + 37V Ri = 2 ohm impulso 2b: Vs = + 10V Ri = 0,05 ohm impulso 3a: Vs = – 112V Ri = 50 ohm impulso 3b: Vs = + 75V Ri = 50 ohm impulso 4: Vs = – 6V Va = – 5V t6=15ms impulso 5: Vs = + 65V Ri = 3ohm td = 100ms L'impulso 5 va controllato solo per le unità elettroniche di bordo destinate al montaggio in veicoli per i quali non è prevista una protezione comune esterna contro le cadute della potenza di carico Per la proposta relativa alle cadute della potenza di carico fare riferimento alla norma ISO 16750-2, 4a edizione, capitolo 4.6.4.	218

4. PROVE FUNZIONALI PER LE CARTE TACHIGRAFICHE

Le prove conformemente alla presente sezione 4,

n. 5, «Prove dei protocolli»,

n. 6, «Struttura della carta» e

n. 7, «Prove funzionali»

possono essere eseguite dall'addetto alla valutazione o alla certificazione durante la procedura di certificazione della sicurezza del modulo chip basata sui criteri comuni (CC).

Le prove numero 2.3 e 4.2 sono identiche. Esse sono le prove meccaniche della combinazione carta e modulo chip. Se uno di questi componenti (carta, modulo chip) viene modificato, tali prove diventano necessarie.

▼B

N.	Prova	Descrizione	Requisiti applicabili
1.	**Esame amministrativo**		
1.1	Documentazione	Correttezza della documentazione	
2	**Carta**		
2.1	Stampa	Accertarsi che tutte le caratteristiche di protezione e i dati visibili siano stampati correttamente sulla carta e siano conformi. [Designatore] Allegato 1C, capitolo 4.1 «Dati visibili», 227) Il lato anteriore deve contenere: i termini «Carta del conducente» o «Carta di controllo» o «Carta dell'officina» o «Carta dell'azienda» stampati in maiuscolo nella lingua o nelle lingue ufficiali dello Stato membro che rilascia la carta, a seconda del tipo di carta; [Nome dello Stato membro] Allegato 1C, capitolo 4.1 «Dati visibili», 228) Il lato anteriore deve contenere: il nome dello Stato membro che rilascia la carta (facoltativo). [Sigla] Allegato 1C, capitolo 4.1 «Dati visibili», 229) Il lato anteriore deve contenere: la sigla distintiva dello Stato membro che rilascia la carta, stampata in negativo in un rettangolo azzurro e circondata da dodici stelle gialle. [Numerazione] Allegato 1C, capitolo 4.1 «Dati visibili», 232) Il retro della carta deve contenere: la spiegazione delle voci numerate che appaiono sul lato anteriore della carta; [Colore] Allegato 1C, capitolo 4.1 «Dati visibili», 234) Le carte tachigrafiche devono essere stampate con i seguenti colori di fondo predominanti: — carta del conducente: bianco, — carta dell'officina: rosso, — carta di controllo: azzurro, — carta dell'azienda: giallo.	da 227 a 229, 232, da 234 a 236

▼B

N.	Prova	Descrizione	Requisiti applicabili
		[Sicurezza] Allegato 1C, capitolo 4.1 «Dati visibili», 235) Le carte tachigrafiche devono presentare almeno le caratteristiche seguenti per essere protette contro la falsificazione e la manomissione: — un fondo di sicurezza finemente arabescato e stampa a iride, — almeno una linea bicromatica microstampata.	
		[Marcature] Allegato 1C, capitolo 4.1 «Dati visibili», 236) Gli Stati membri possono aggiungere altri colori o iscrizioni, come simboli nazionali ed altre caratteristiche di sicurezza.	
		[Marchio di omologazione] Le carte tachigrafiche devono essere contrassegnate con un marchio di omologazione. Il marchio di omologazione deve essere composto: — di un rettangolo, all'interno del quale si trova la lettera «e» seguita da un numero distintivo o da una lettera distintiva del paese che ha rilasciato l'omologazione, — di un numero di omologazione corrispondente al numero della scheda di omologazione della carta tachigrafica, posto in una posizione qualsiasi in prossimità del rettangolo.	
2.2	Prove meccaniche	[Dimensioni della carta] Le carte tachigrafiche devono essere conformi alla norma ISO/IEC 7810, Carte di identificazione — Caratteristiche fisiche, [5] Dimensioni della carta, [5.1] Dimensioni della carta [5.1.1] Dimensioni della carta e tolleranze, carta tipo ID-1 Carta non usata	240, 243 ISO/IEC 7810
		[Bordi della carta] Le carte tachigrafiche devono essere conformi alla norma ISO/IEC 7810, Carte di identificazione — Caratteristiche fisiche, [5] Dimensioni della carta, [5.1] Dimensioni della carta [5.1.2] Bordi della carta	

▼B

N.	Prova	Descrizione	Requisiti applicabili
		[Costruzione della carta] Le carte tachigrafiche devono essere conformi alla norma ISO/IEC 7810, Carte di identificazione — Caratteristiche fisiche, [6] Costruzione della carta	
		[Materiali costruttivi della carta] Le carte tachigrafiche devono essere conformi alla norma ISO/IEC 7810, Carte di identificazione — Caratteristiche fisiche, [7] Materiali costruttivi della carta	
		[Resistenza alla flessione] Le carte tachigrafiche devono essere conformi alla norma ISO/IEC 7810, Carte di identificazione — Caratteristiche fisiche, [8] Caratteristiche della carta [8.1] Resistenza alla flessione	
		[Tossicità] Le carte tachigrafiche devono essere conformi alla norma ISO/IEC 7810, Carte di identificazione — Caratteristiche fisiche, [8] Caratteristiche della carta [8.3] Tossicità	
		[Resistenza agli agenti chimici] Le carte tachigrafiche devono essere conformi alla norma ISO/IEC 7810, Carte di identificazione — Caratteristiche fisiche, [8] Caratteristiche della carta [8.4] Resistenza agli agenti chimici	
		[Stabilità della carta] Le carte tachigrafiche devono essere conformi alla norma ISO/IEC 7810, Carte di identificazione — Caratteristiche fisiche, [8] Caratteristiche della carta [8.5] Stabilità dimensionale della carta e deformazione dovuta alla temperatura e all'umidità	

▼B

N.	Prova	Descrizione	Requisiti applicabili
		[Luce] Le carte tachigrafiche devono essere conformi alla norma ISO/IEC 7810, Carte di identificazione — Caratteristiche fisiche, [8] Caratteristiche della carta [8.6] Luce	
		[Durabilità] Allegato 1C, capitolo 4.4 «Specifiche ambientali ed elettriche», 241) Le carte tachigrafiche devono essere in grado di funzionare correttamente per un periodo di cinque anni, se impiegate nel rispetto delle specifiche ambientali ed elettriche.	
		[Resistenza dello strato esterno] Le carte tachigrafiche devono essere conformi alla norma ISO/IEC 7810, Carte di identificazione — Caratteristiche fisiche, [8] Caratteristiche della carta [8.8] Resistenza dello strato esterno	
		[Aderenza o blocco] Le carte tachigrafiche devono essere conformi alla norma ISO/IEC 7810, Carte di identificazione — Caratteristiche fisiche, [8] Caratteristiche della carta [8.9] Aderenza o blocco	
		[Deformazione] Le carte tachigrafiche devono essere conformi alla norma ISO/IEC 7810, Carte di identificazione — Caratteristiche fisiche, [8] Caratteristiche della carta [8.11] Deformazione globale della carta	
		[Resistenza al calore] Le carte tachigrafiche devono essere conformi alla norma ISO/IEC 7810, Carte di identificazione — Caratteristiche fisiche, [8] Caratteristiche della carta [8.12] Resistenza al calore	

▼B

N.	Prova	Descrizione	Requisiti applicabili
		[Distorsioni superficiali] Le carte tachigrafiche devono essere conformi alla norma ISO/IEC 7810, Carte di identificazione — Caratteristiche fisiche, [8] Caratteristiche della carta [8.13] Distorsioni superficiali	
		[Contaminazione] Le carte tachigrafiche devono essere conformi alla norma ISO/IEC 7810, Carte di identificazione — Caratteristiche fisiche, [8] Caratteristiche della carta [8.14] Contaminazione e interazione dei componenti della carta	
2.3	Prove meccaniche con modulo chip integrato	[Flessione] Le carte tachigrafiche devono essere conformi alla norma ISO/IEC 7810:2003/Amd. 1:2009, Carte di identificazione — Caratteristiche fisiche, Modifica 1: Criteri per carte con circuiti integrati [9.2] Sollecitazione dinamica alla flessione Numero totale di cicli di flessione: 4 000.	ISO/IEC 7810
		[Torsione] Le carte tachigrafiche devono essere conformi alla norma ISO/IEC 7810:2003/Amd. 1:2009, Carte di identificazione — Caratteristiche fisiche, Modifica 1: Criteri per carte con circuiti integrati [9.3] Sollecitazione dinamica alla torsione Numero totale di cicli di torsione: 4 000.	
3	**Modulo**		
3.1	Modulo	Il modulo è costituito dall'involucro totale e dalla piastra a contatto. [Profilo superficiale] Le carte tachigrafiche devono essere conformi alla norma ISO/IEC 7816-1:2011, Carte di identificazione — Carte a circuito integrato — Parte 1: Carte con contatti — Caratteristiche fisiche [4.2] Profilo superficiale dei contatti	ISO/IEC 7816

▼B

N.	Prova	Descrizione	Requisiti applicabili
		[Resistenza meccanica] Le carte tachigrafiche devono essere conformi alla norma ISO/IEC 7816-1:2011, Carte di identificazione — Carte a circuito integrato — Parte 1: Carte con contatti — Caratteristiche fisiche [4.3] Resistenza meccanica (della carta e dei contatti)	
		[Resistenza elettrica] Le carte tachigrafiche devono essere conformi alla norma ISO/IEC 7816-1:2011, Carte di identificazione — Carte a circuito integrato — Parte 1: Carte con contatti — Caratteristiche fisiche [4.4] Resistenza elettrica (dei contatti)	
		[Dimensione:] Le carte tachigrafiche devono essere conformi alla norma ISO/IEC 7816-2:2007, Carte di identificazione — Carte a circuito integrato — Parte 2: Carte con contatti — Dimensione e posizione dei contatti [3] Dimensione dei contatti	
		[Posizione] Le carte tachigrafiche devono essere conformi alla norma ISO/IEC 7816-2:2007, Carte di identificazione — Carte a circuito integrato — Parte 2: Carte con contatti — Dimensione e posizione dei contatti [4] Numero e posizione dei contatti Nel caso di moduli con sei contatti, i contatti «C4» e «C8» non sono inclusi nella prova prescritta.	
4	**Chip**		
4.1	Chip	[Temperatura di esercizio] Il chip della carta tachigrafica deve funzionare in un campo di temperatura ambientale compreso tra -25 °C e +85 °C.	da 241 a 244 ECE R10 ISO/IEC 7810 ISO/IEC 10373

▼B

N.	Prova	Descrizione	Requisiti applicabili
		[Temperatura e umidità] Allegato 1C, capitolo 4.4 «Specifiche ambientali ed elettriche», 241) Le carte tachigrafiche devono essere in grado di funzionare correttamente in tutte le condizioni climatiche abituali nel territorio della Comunità e almeno nel campo di temperatura compreso tra – 25 °C e + 70 °C, con picchi occasionali fino a + 85 °C, dove per «occasionale» s'intende non superiore a 4 ore per volta e non superiore a 100 volte nell'intero periodo di durata della carta. Le carte tachigrafiche devono essere esposte, in fasi successive, alle seguenti temperature e tassi di umidità per i periodi indicati. Dopo ogni fase viene provata la funzionalità elettrica delle carte tachigrafiche. 1. Temperatura di – 20 °C per 2 h. 2. Temperatura di +/– 0 °C per 2 h. 3. Temperatura di + 20 °C, 50 % RH, per 2 h. 4. Temperatura di + 50 °C, 50 % RH, per 2 h. 5. Temperatura di + 70 °C, 50 % RH, per 2 h. La temperatura viene aumentata in modo intermittente a + 85 °C, 50 % RH, per 60 min. 6. Temperatura di + 70 °C, 85 % RH, per 2 h. La temperatura viene aumentata in modo intermittente a + 85 °C, 85 % RH, per 30 min.	
		[Umidità] Allegato 1C, capitolo 4.4 «Specifiche ambientali ed elettriche», 242) Le carte tachigrafiche devono essere in grado di funzionare correttamente nel campo di umidità compreso tra 10 % e 90 %.	
		[Compatibilità elettromagnetica — EMC] Allegato 1C, capitolo 4.4 «Specifiche ambientali ed elettriche», 244) Durante il funzionamento le carte tachigrafiche devono essere conformi alla norma ECE R10 relativa alla compatibilità elettromagnetica.	

▼B

N.	Prova	Descrizione	Requisiti applicabili
		[Elettricità statica] Allegato 1C, capitolo 4.4 «Specifiche ambientali ed elettriche», 244) Durante il funzionamento le carte tachigrafiche devono essere protette contro le scariche elettrostatiche. Le carte tachigrafiche devono essere conformi alla norma ISO/IEC 7810:2003/Amd. 1:2009, Carte di identificazione — Caratteristiche fisiche, Modifica 1: Criteri per carte con circuiti integrati [9.4] Elettricità statica [9.4.1] Carte IC a contatto Tensione di prova: 4 000 V.	
		[Raggi X] Le carte tachigrafiche devono essere conformi alla norma ISO/IEC 7810:2003/Amd. 1:2009, Carte di identificazione — Caratteristiche fisiche, Modifica 1: Criteri per carte con circuiti integrati [9.1] Raggi X	
		[Luce ultravioletta] ISO/IEC 10373-1:2006, Carte di identificazione — Metodi di prova — Parte 1: Caratteristiche generali [5.11] Luce ultravioletta	
		[a 3 ruote] Le carte tachigrafiche devono essere conformi alla norma ISO/IEC 10373-1:2006/Amd. 1:2012, Carte di identificazione — Metodi di prova — Parte 1: Caratteristiche generali, Modifica 1 [5.22] ICC — Resistenza meccanica: prova a 3 ruote per gli ICC con contatti	
		[Avvolgimento] Le carte tachigrafiche devono essere conformi alla norma MasterCard CQM V2.03:2013 [11.1.3] R-L3-14-8: Prova della robustezza dell'avvolgimento [13.2.1.32] TM-422: Affidabilità meccanica: Prova di avvolgimento	

▼B

N.	Prova	Descrizione	Requisiti applicabili
4.2	Modulo del chip per le prove meccaniche integrato nella carta stessa-> uguale a 2.3	[Flessione] Le carte tachigrafiche devono essere conformi alla norma ISO/IEC 7810:2003/Amd. 1:2009, Carte di identificazione — Caratteristiche fisiche, Modifica 1: Criteri per carte con circuiti integrati [9.2] Sollecitazione dinamica alla flessione Numero totale di cicli di flessione: 4 000. [Torsione] Le carte tachigrafiche devono essere conformi alla norma ISO/IEC 7810:2003/Amd. 1:2009, Carte di identificazione — Caratteristiche fisiche, Modifica 1: Criteri per carte con circuiti integrati [9.3] Sollecitazione dinamica alla torsione Numero totale di cicli di torsione: 4 000.	ISO/IEC 7810
5	**Prove dei protocolli**		
5.1	ATR	Verificare la conformità dell'ATR	ISO/IEC 7816-3 TCS_14, TCS_17, TCS_18
5.2	T=0	Verificare la conformità del protocollo T = 0	ISO/IEC 7816-3 TCS_11, TCS_12, TCS_13, TCS_15
5.3	PTS	Verificare la conformità del comando PTS passando all'impostazione T = 1 da T = 0	ISO/IEC 7816-3 TCS_12, TCS_19, TCS_20, TCS_21
5.4	T=1	Verificare la conformità del protocollo T = 1	ISO/IEC 7816-3 TCS_11, TCS_13, TCS_16
6	**Struttura della carta**		
6.1		Controllare la conformità della struttura dei file della carta, verificando la presenza dei file obbligatori nella carta e le relative condizioni di accesso	da TCS_22 a TCS_28 da TCS_140 a TCS_179
7	**Prove funzionali**		
7.1	Elaborazione normale	Verificare almeno una volta ogni uso ammesso di ciascun comando (per es.: verificare il comando UPDATE BINARY con CLA = '00', CLA = '0C' e con parametri P1, P2 e Lc diversi). Verificare che le operazioni siano state effettivamente eseguite nella carta (per es.: leggendo il file su cui è stato eseguito il comando)	da TCS_29 a TCS_139

▼B

N.	Prova	Descrizione	Requisiti applicabili
7.2	Messaggi di errore	Verificare almeno una volta ogni messaggio di errore (secondo quanto specificato all'appendice 2) per ciascun comando. Verificare almeno una volta ogni errore generico (eccetto per gli errori di integrità «**6400**» verificati nell'ambito della certificazione della sicurezza)	
7.3	Cypher suite e parametri Domain standardizzati		CSM_48, CSM_50
8	**Personalizzazione**		
8.1	Personalizzazione ottica	Allegato 1C, capitolo 4.1 «Dati visibili», 230) Il lato anteriore deve contenere: le informazioni specifiche della carta. Allegato 1C, capitolo 4.1 «Dati visibili», 231) Il lato anteriore deve contenere: le date, indicate nel formato «gg/mm/aaaa» o «gg.mm.aaaa» (giorno, mese, anno). Allegato 1C, capitolo 4.1 «Dati visibili», 235) Le carte tachigrafiche devono presentare almeno le caratteristiche seguenti per essere protette contro la falsificazione e la manomissione: — sovrapposizione del fondo di sicurezza e della fotografia.	230, 231, 235

5. PROVE DEL DISPOSITIVO GNSS ESTERNO

N.	Prova	Descrizione	Requisiti applicabili
1.	**Esame amministrativo**		
1.1	Documentazione	Correttezza della documentazione	
2.	**Ispezione visiva del dispositivo GNSS esterno**		
2.1.	Conformità alla documentazione		
2.2.	Identificazione/marcature		da 224 a 226
2.3	Materiali		da 219 a 223
3.	**Prove funzionali**		
3.1	Dati di identificazione del sensore		98.99
3.2	Modulo GNSS esterno — accoppiamento dell'unità elettronica di bordo		123, 205

▼B

N.	Prova	Descrizione	Requisiti applicabili
3.3	Posizione GNSS		36, 37
3.4	Interfaccia dell'unità elettronica di bordo quando il ricevitore GNSS è esterno all'unità elettronica di bordo		03
3.5	Cypher suite e parametri Domain standardizzati		CSM_48, CSM_50
4.	**Prove ambientali**		
4.1	Temperatura	Verificare la funzionalità mediante: prova conformemente alla norma ISO 16750-4, capitolo 5.1.1.2: Prova di funzionamento a bassa temperatura (72 h @ – 20 °C) Questa prova si riferisce alla norma IEC 60068-2-1: Prove ambientali — Parti 2-1: Prove — Prova A: Freddo Prova conformemente a ISO 16750-4: Capitolo 5.1.2.2: Prova di funzionamento ad alta temperatura (72 h @ 70 °C) Questa prova si riferisce alla norma IEC 60068-2-2: Procedure di prove ambientali di base; parte 2: prove; prove B: calore secco Prova conformemente a ISO 16750-4: Capitolo 5.3.2 Cambiamento rapido di temperatura con durata specifica della transizione (– 20 °C/70 °C, 20 cicli, tempo di permanenza di 1 h a ogni temperatura) Si può effettuare una serie ridotta di prove (fra quelle definite alla sezione 3 della presente tabella) alla temperatura più bassa, alla temperatura più alta e durante i cicli di temperature	213
4.2	Umidità	Verificare che l'unità elettronica di bordo possa sopportare un'umidità ciclica (prova termica), mediante prova Db, IEC 60068-2-30, sei cicli di 24 ore, ciascuno con temperature che variano da + 25 °C a + 55 °C ed un'umidità relativa del 97 % a + 25 °C e del 93 % a + 55 °C	214
4.3	Prove meccaniche	1. Vibrazioni sinusoidali. Verificare che l'unità elettronica di bordo possa sopportare vibrazioni sinusoidali aventi le seguenti caratteristiche: spostamento costante tra 5 e 11 Hz: picco di 10 mm accelerazione costante tra 11 e 300 Hz: 5 g Questo requisito si verifica in base alla norma IEC 60068-2-6, prova Fc, con una durata minima della prova di 3 × 12 ore (12 ore per asse) La norma ISO 16750-3 non prescrive una prova di vibrazione sinusoidale per i dispositivi posizionati nella cabina del veicolo staccata.	219

▼B

N.	Prova	Descrizione	Requisiti applicabili
		2. Vibrazioni casuali: Prova conformemente a ISO 16750-3: Capitolo 4.1.2.8: Prova VIII: Veicolo commerciale, cabina del veicolo staccata Prova delle vibrazioni casuali, 10…2 000 Hz, RMS verticale 21,3 m/s^2, RMS longitudinale 11,8 m/s^2, RMS laterale 13,1 m/s^2, 3 assi, 32 h per asse, incluso il ciclo di temperatura – 20…70 °C. Questa prova si riferisce alla norma IEC 60068-2-64: Prove ambientali — Parti 2-64: Prove — Prova Fh: Vibrazioni, a banda larga casuali e guida 3. Urti: urto meccanico con mezzo seno 3g conformemente a ISO 16750. Le prove sopra descritte sono effettuate su campioni diversi del modello di apparecchio sottoposto alle prove	
4.4	Protezione contro l'acqua e i corpi estranei	Prova conformemente a ISO 20653: Veicoli stradali — Grado di protezione (codice IP) — Protezione delle apparecchiature da oggetti estranei, dall'acqua e dall'accesso (senza modifica dei parametri)	220, 221
4.5	Protezione contro sovratensione	Verificare che l'unità elettronica di bordo possa sopportare un'alimentazione di: Versioni da 24 V: 34V a + 40 °C 1 ora Versioni da 12 V: 17V a + 40 °C 1 ora (ISO 16750-2, capitolo 4.3)	216
4.6	Protezione contro polarità inversa	Verificare che l'unità elettronica di bordo possa sopportare un'inversione dell'alimentazione (ISO 16750-2, capitolo 4.7)	216
4.7	Protezione contro cortocircuiti	Verificare che i segnali in ingresso e in uscita siano protetti contro i cortocircuiti rispetto ad alimentazione e massa (ISO 16750-2, capitolo 4.10)	216
5	**Prove della compatibilità elettromagnetica**		
5.1	Emissioni irradiate e sensibilità ai disturbi	Conformità al regolamento ECE R10	218

▼B

N.	Prova	Descrizione	Requisiti applicabili
5.2	Scariche elettrostatiche	Conformità alla norma ISO 10605:2008 + Rettifica tecnica:2010 + AMD1:2014: +/– 4kV per il contatto e +/– 8kV per lo scarico di aria	218
5.3	Sensibilità ai transitori condotti nell'alimentazione	Per le versioni da 24 V: conformità a ISO 7637-2 + regolamento ECE n. 10 Rev. 3: impulso 1a: Vs = – 450V Ri = 50 ohm impulso 2a: Vs = + 37V Ri = 2 ohm impulso 2b: Vs = + 20V Ri = 0,05 ohm impulso 3a: V s= – 150V Ri = 50 ohm impulso 3b: Vs=+150V Ri=50 ohm impulso 4: Vs = – 16V Va = – 12V t6 = 100ms impulso 5: Vs = + 120V Ri = 2,2 ohm td = 250ms Per le versioni da 12 V: conformità a ISO 7637-1 + regolamento ECE n. 10 Rev. 3: impulso 1: Vs = – 75V Ri = 10 ohm impulso 2a: Vs = + 37V Ri = 2 ohm impulso 2b: Vs = + 10V Ri = 0,05 ohm impulso 3a: Vs = – 112V Ri = 50 ohm impulso 3b: Vs = + 75V Ri = 50 ohm impulso 4: Vs = – 6V Va = – 5V t6 = 15ms impulso 5: Vs = + 65V Ri = 3ohm td = 100ms L'impulso 5 va controllato solo per le unità elettroniche di bordo destinate al montaggio in veicoli per i quali non è prevista una protezione comune esterna contro le cadute della potenza di carico Per la proposta relativa alle cadute della potenza di carico fare riferimento alla norma ISO 16750-2, 4a edizione, capitolo 4.6.4.	218

6. PROVE DEL DISPOSITIVO DI COMUNICAZIONE REMOTA

N.	Prova	Descrizione	Requisiti applicabili
1.	**Esame amministrativo**		
1.1	Documentazione	Correttezza della documentazione	
2.	**Esame visivo**		
2.1.	Conformità alla documentazione		
2.2.	Identificazione/marcature		225, 226
2.3	Materiali		da 219 a 223
4.	**Prove ambientali**		
4.1	Temperatura	Verificare la funzionalità mediante: prova conformemente alla norma ISO 16750-4, capitolo 5.1.1.2: Prova di funzionamento a bassa temperatura (72 h @ -20 °C) Questa prova si riferisce alla norma IEC 60068-2-1: Prove ambientali — Parti 2-1: Prove — Prova A: Freddo	213

▼B

N.	Prova	Descrizione	Requisiti applicabili
		Prova conformemente a ISO 16750-4: Capitolo 5.1.2.2: Prova di funzionamento ad alta temperatura (72 h @ 70 °C) Questa prova si riferisce alla norma IEC 60068-2-2: Procedure di prove ambientali di base; parte 2: prove; prove B: calore secco Prova conformemente a ISO 16750-4: Capitolo 5.3.2 Cambiamento rapido di temperatura con durata specifica della transizione (-20 °C/70 °C, 20 cicli, tempo di permanenza di 1 h (?) a ogni temperatura) Si può effettuare una serie ridotta di prove (fra quelle definite alla sezione 3 della presente tabella) alla temperatura più bassa, alla temperatura più alta e durante i cicli di temperature	
4.4	Protezione contro l'acqua e i corpi estranei	Prova conformemente a ISO 20653: Veicoli stradali — Grado di protezione (codice IP) — Protezione delle apparecchiature da oggetti estranei, dall'acqua e dall'accesso (valore target IP40)	220, 221
5	**Prove della compatibilità elettromagnetica**		
5.1	Emissioni irradiate e sensibilità ai disturbi	Conformità al regolamento ECE R10	218
5.2	Scariche elettrostatiche	Conformità alla norma ISO 10605:2008 + Rettifica tecnica:2010 + AMD1:2014: +/– 4kV per il contatto e +/– 8kV per lo scarico di aria	218
5.3	Sensibilità ai transitori condotti nell'alimentazione	Per le versioni da 24 V: conformità a ISO 7637-2 + regolamento ECE n. 10 Rev. 3: impulso 1a: Vs = – 450V Ri = 50 ohm impulso 2a: Vs = + 37V Ri = 2 ohm impulso 2b: Vs = + 20V Ri = 0,05 ohm impulso 3a: Vs = – 150V Ri = 50 ohm impulso 3b: Vs = + 150V Ri = 50 ohm impulso 4: Vs = – 16V Va = – 12V t6 = 100ms impulso 5: Vs = + 120V Ri = 2,2 ohm td = 250ms Per le versioni da 12 V: conformità a ISO 7637-1 + regolamento ECE n. 10 Rev. 3: impulso 1: Vs = – 75V Ri = 10 ohm impulso 2a: Vs = + 37V Ri = 2 ohm impulso 2b: Vs = +10V Ri = 0,05 ohm impulso 3a: Vs = – 112V Ri = 50 ohm impulso 3b: Vs = + 75V Ri = 50 ohm impulso 4: Vs = – 6V Va = – 5V t6 = 15ms impulso 5: Vs = + 65V Ri = 3ohm td = 100ms L'impulso 5 va controllato solo per le unità elettroniche di bordo destinate al montaggio in veicoli per i quali non è prevista una protezione comune esterna contro le cadute della potenza di carico Per la proposta relativa alle cadute della potenza di carico fare riferimento alla norma ISO 16750-2, 4a edizione, capitolo 4.6.4.	218

▼B

7. PROVE FUNZIONALI SU CARTA

N.	Prova	Descrizione	Requisiti applicabili
1.	**Esame amministrativo**		
1.1	Documentazione	Correttezza della documentazione	
2	**Prove generali**		
2.1	Numero di caratteri per riga	Ispezione ottica delle stampe.	172
2.2	Dimensione minima dei caratteri	Esame visivo delle stampe e ispezione dei caratteri.	173
2.3	Insieme standard di caratteri supportati	La stampante deve poter stampare i caratteri specificati nell'appendice 1, capitolo 4, «Insiemi di caratteri».	174
2.4	Definizione delle stampe	Controllo dell'omologazione del tachigrafo e esame visivo delle stampe	174
2.5	Leggibilità e identificazione delle stampe	Ispezione delle stampe Dimostrata dal fabbricante mediante verbali e protocolli di prova. Tutti i numeri di omologazione dei tachigrafi con cui è possibile usare la carta per stampante sono iscritti sulla carta.	175, 177, 178
2.6	Aggiunta di note scritte a mano	Esame visivo: È disponibile il campo per la firma del conducente. Sono disponibili campi per altre voci scritte a mano.	180
2.7	Ulteriori dettagli sulla carta.	Sul lato frontale e sul retro della carta possono essere riportati ulteriori dettagli e informazioni, che non devono tuttavia interferire con la leggibilità delle stampe. Esame visivo.	177, 178
3	**Prove di archiviazione**		
3.1	Calore secco	Precondizionamento: 16 ore a + 23 °C ± 2 °C/55 % ± 3 % di umidità relativa Ambiente di prova: 72 ore a + 70 °C ± 2 °C Recupero: 16 ore a + 23 °C ± 2 °C/55 % ± 3 % di umidità relativa	176, 178 IEC 60068-2-2-Bb
2.2	Calore umido	Precondizionamento: 16 ore a + 23 °C ± 2 °C/55 % ± 3 % di umidità relativa Ambiente di prova: 144 ore a + 55 °C ± 2 °C/93 % ± 3 % di umidità relativa Recupero: 16 ore a + 23 °C ± 2 °C/55 % ± 3 % di umidità relativa	176, 178 IEC 60068-2-78-Cab

▼B

N.	Prova	Descrizione	Requisiti applicabili
4	**Prove di servizio della carta**		
4.1	Resistenza dello sfondo all'umidità (carta non stampata)	Precondizionamento: 16 ore a + 23 °C ± 2 °C/55 % ± 3 % di umidità relativa Ambiente di prova: 144 ore a + 55 °C ± 2 °C/93 % ± 3 % di umidità relativa Recupero: 16 ore a + 23 °C ± 2 °C/55 % ± 3 % di umidità relativa	176, 178 IEC 60068-2-78-Cab
4.2	Stampabilità	Precondizionamento: 24 ore a + 40 °C ± 2 °C/93 % ± 3 % di umidità relativa Ambiente di prova: stampa prodotta a + 23 °C ± 2 °C Recupero: 16 ore a + 23 °C ± 2 °C/55 % ± 3 % di umidità relativa	176, 178
4.3	Resistenza al calore	Precondizionamento: 16 ore a + 23 °C ± 2 °C/55 % ± 3 % di umidità relativa Ambiente di prova: 2 ore a + 70 °C ± 2 °C, calore secco Recupero: 16 ore a + 23 °C ± 2 °C/55 % ± 3 % di umidità relativa	176, 178 IEC 60068-2-2-Bb
4.4	Resistenza alle temperature basse	Precondizionamento: 16 ore a + 23 °C ± 2 °C/55 % ± 3 % di umidità relativa Ambiente di prova: 24 ore – 20°C ± 3 °C, freddo secco Recupero: 16 ore a + 23 °C ± 2 °C/55 % ± 3 % di umidità relativa	176, 178 ISO 60068-2-1-Ab
4.5	Resistenza alla luce	Precondizionamento: 16 ore a + 23 °C ± 2 °C/55 % ± 3 % di umidità relativa Ambiente di prova: 100 ore con un'illuminazione di 5 000 Lux a + 23 °C ± 2 °C/55 % ± 3 % di umidità relativa Recupero: 16 ore a + 23 °C ± 2 °C/55 % ± 3 % di umidità relativa	176, 178

Criteri di leggibilità per le prove 3.x e 4.x:

La leggibilità delle stampe è garantita se i valori di densità ottica sono conformi ai limiti seguenti:

caratteri stampati: min. 1,0

sfondo (carta non stampata): max. 0,2

I valori di densità ottica delle stampe devono essere misurati conformemente alla norma DIN EN ISO 534.

Le stampe non devono evidenziare cambiamenti di dimensioni e devono rimanere chiaramente leggibili.

8. PROVE DI INTEROPERABILITÀ

N.	Prova	Descrizione
9.1 Prove di interoperabilità tra unità elettroniche di bordo e carte tachigrafiche		
1	Autenticazione reciproca	Verificare che l'autenticazione reciproca tra l'unità elettronica di bordo e la carta tachigrafica funzioni normalmente

▼B

N.	Prova	Descrizione
2	Prove di scrittura/lettura	Predisporre uno scenario di attività tipico sull'unità elettronica di bordo. Lo scenario deve essere adattato al tipo di carta sottoposta alla prova e prevedere la scrittura nel maggior numero possibile di EF nella carta Verificare mediante un trasferimento dei dati dell'unità elettronica di bordo che tutte le registrazioni corrispondenti siano state effettuate correttamente Verificare mediante un trasferimento dei dati della carta che tutte le registrazioni corrispondenti siano state effettuate correttamente Verificare mediante stampe giornaliere che tutte le registrazioni corrispondenti si possano leggere correttamente
9.2 Prove di interoperabilità tra unità elettroniche di bordo e sensori di movimento		
1	Abbinamento	Verificare che l'abbinamento delle unità elettroniche di bordo e dei sensori di movimento funzioni normalmente
2	Prove delle attività	Predisporre uno scenario di attività tipico sul sensore di movimento. Lo scenario deve includere un'attività normale e creare il maggior numero possibile di anomalie o guasti. Verificare mediante un trasferimento dei dati dell'unità elettronica di bordo che tutte le registrazioni corrispondenti siano state effettuate correttamente Verificare mediante un trasferimento dei dati della carta che tutte le registrazioni corrispondenti siano state effettuate correttamente Verificare mediante una stampa giornaliera che tutte le registrazioni corrispondenti si possano leggere correttamente
9.3 Prove di interoperabilità tra unità elettroniche di bordo e dispositivi GNSS esterni (se applicabile)		
1	Autenticazione reciproca	Verificare che l'autenticazione reciproca (accoppiamento) tra l'unità elettronica di bordo e il modulo GNSS esterno funzioni normalmente
2	Prove delle attività	Predisporre uno scenario di attività tipico sul GNSS esterno. Lo scenario deve includere un'attività normale e creare il maggior numero possibile di anomalie o guasti. Verificare mediante un trasferimento dei dati dell'unità elettronica di bordo che tutte le registrazioni corrispondenti siano state effettuate correttamente Verificare mediante un trasferimento dei dati della carta che tutte le registrazioni corrispondenti siano state effettuate correttamente Verificare mediante una stampa giornaliera che tutte le registrazioni corrispondenti si possano leggere correttamente

▼B

Appendice 10

REQUISITI DI SICUREZZA

La presente appendice specifica i requisiti di sicurezza informatici per i componenti del sistema tachigrafico intelligente (tachigrafo di seconda generazione).

SEC_001 La certificazione di sicurezza dei seguenti componenti del sistema tachigrafico intelligente deve essere conforme allo standard Common Criteria (criteri comuni):

— unità elettronica di bordo (VU),

— carta tachigrafica,

— sensore di movimento,

— dispositivo GNSS esterno.

SEC_002 I requisiti minimi di sicurezza informatica che devono essere soddisfatti da ogni componente che necessita della certificazione di sicurezza sono definiti in un profilo di protezione del componente, conforme allo standard Common Criteria.

SEC_003 La Commissione europea dovrà assicurarsi che quattro profili di protezione conformi al presente allegato siano patrocinati, elaborati, approvati dagli organismi pubblici di certificazione della sicurezza informatica organizzati nell'ambito del Joint Interpretation Working Group (JIWG), il gruppo di lavoro che sostiene il reciproco riconoscimento dei certificati sotto l'egida dell'accordo europeo SOGIS-MRA (Agreement on Mutual Recognition of Information Technology Security Evaluation Certificates) e registrati:

— profilo di protezione dell'unità elettronica di bordo (VU),

— profilo di protezione della carta tachigrafica,

— profilo di protezione del sensore di movimento,

— profilo di protezione del dispositivo GNSS esterno.

Il profilo di protezione dell'unità elettronica di bordo (VU) deve affrontare i casi in cui la VU è destinata ad essere utilizzata sia con un dispositivo GNSS esterno che senza. Nel primo caso i requisiti di sicurezza del dispositivo GNSS esterno sono previsti nel profilo di protezione ad esso dedicato.

SEC_004 I fabbricanti dei componenti devono perfezionare e completare l'apposito profilo di protezione del componente a seconda della necessità, senza modificare né cancellare le specifiche relative alle minacce, agli obiettivi, alle procedure e alle funzioni di sicurezza, al fine di formulare un obiettivo di sicurezza rispetto al quale richiedere la certificazione di sicurezza del componente.

SEC_005 Nel corso del processo di valutazione deve essere indicata la stretta conformità di tale obiettivo di sicurezza specifico al profilo di protezione corrispondente.

SEC_006 Il livello di garanzia per ciascun profilo di protezione deve essere EAL4, aumentato dai componenti di garanzia ATE_DPT.2 e AVA_VAN.5.

▼B

Appendice 11

MECCANISMI COMUNI DI SICUREZZA

INDICE

PREAMBOLO

PARTE A SISTEMA TACHIGRAFICO DI PRIMA GENERAZIONE

1. INTRODUZIONE

1.1. Riferimenti

1.2. Simboli e abbreviazioni

2. SISTEMI E ALGORITMI CRITTOGRAFICI

2.1. Sistemi crittografici

2.2. Algoritmi crittografici

2.2.1 Algoritmo RSA

2.2.2 Algoritmo di hash

2.2.3 Algoritmo di cifratura dei dati

3. CHIAVI E CERTIFICATI

3.1. Generazione e distribuzione di chiavi

3.1.1 Generazione e distribuzione di chiavi RSA

3.1.2 Chiavi di prova RSA

3.1.3 Chiavi per i sensori di movimento

3.1.4 Generazione e distribuzione di chiavi T-DES

3.2. Chiavi

3.3. Certificati

3.3.1 Contenuto dei certificati

3.3.2 Rilascio dei certificati

3.3.3 Verifica e apertura dei certificati

4. MECCANISMO DI AUTENTICAZIONE RECIPROCA

5. MECCANISMI DI RISERVATEZZA, INTEGRITÀ E AUTENTICAZIONE DEI TRASFERIMENTI DI DATI TRA VU E CARTE

5.1. Messaggistica sicura (Secure Messaging)

5.2. Trattamento degli errori della messaggistica sicura

5.3. Algoritmo per il calcolo di totali di controllo crittografico

5.4. Algoritmo per il calcolo di crittogrammi dei DO di riservatezza

6. MECCANISMI DI FIRMA DIGITALE PER IL TRASFERIMENTO DEI DATI

6.1. Generazione della firma

▼B

6.2.	Verifica della firma
PARTE B	SISTEMA TACHIGRAFICO DI SECONDA GENERAZIONE
7.	INTRODUZIONE
7.1.	Riferimenti
7.2.	Simboli e abbreviazioni
7.3.	Definizioni
8.	SISTEMI E ALGORITMI CRITTOGRAFICI
8.1.	Sistemi crittografici
8.2.	Algoritmi crittografici
8.2.1	Algoritmi simmetrici
8.2.2	Algoritmi asimmetrici e parametri di dominio standardizzati (standardized domain parameters)
8.2.3	Algoritmi di hash
8.2.4	Suite crittografiche (cipher suites)
9.	CHIAVI E CERTIFICATI
9.1.	Coppie di chiavi asimmetriche e certificati delle chiavi pubbliche
9.1.1	Principi generali
9.1.2	Livello europeo
9.1.3	Livello di Stato membro
9.1.4	Livello di apparecchio: unità elettroniche di bordo (VU)
9.1.5	Livello di apparecchio: carte tachigrafiche
9.1.6	Livello di apparecchio: dispositivi GNSS esterni
9.1.7	Riepilogo: sostituzione dei certificati
9.2.	Chiavi simmetriche
9.2.1	Chiavi per la sicurezza della comunicazione tra VU e sensore di movimento
9.2.2	Chiavi per la sicurezza della comunicazione DSRC
9.3.	Certificati
9.3.1	Principi generali
9.3.2	Contenuto del certificato
9.3.3	Richiesta di certificati
10.	AUTENTICAZIONE RECIPROCA E MESSAGGISTICA SICURA TRA VU E CARTA
10.1.	Principi generali
10.2.	Verifica reciproca della catena di certificati
10.2.1	Verifica della catena di certificati della carta da parte della VU

▼B

10.2.2 Verifica della catena di certificati della VU da parte della carta

10.3. Autenticazione della VU

10.4. Autenticazione del chip e accordo sulla chiave di sessione

10.5. Messaggistica sicura (Secure Messaging)

10.5.1 Principi generali

10.5.2 Struttura dei messaggi sicuri

10.5.3 Interruzione di una sessione di messaggistica sicura

11. ACCOPPIAMENTO, AUTENTICAZIONE RECIPROCA E MESSAGGISTICA SICURA TRA VU E DISPOSITIVO GNSS ESTERNO

11.1. Principi generali

11.2. Accoppiamento tra VU e dispositivo GNSS esterno

11.3. Verifica reciproca della catena di certificati

11.3.1 Principi generali

11.3.2 Durante l'accoppiamento tra VU e EFG

11.3.3 Durante il funzionamento normale

11.4. Autenticazione della VU, autenticazione del chip e accordo sulla chiave di sessione

11.5. Messaggistica sicura

12. ABBINAMENTO E COMUNICAZIONE TRA VU E SENSORE DI MOVIMENTO

12.1. Principi generali

12.2. Abbinamento tra VU e sensore di movimento usando diverse generazioni di chiavi

12.3. Abbinamento e comunicazione tra VU e sensore di movimento usando AES

12.4. Abbinamento tra VU e sensore di movimento per diverse generazioni di apparecchi

13. SICUREZZA PER LA COMUNICAZIONE REMOTA ATTRAVERSO DSRC

13.1. Principi generali

13.2. Cifratura del payload del tachigrafo e generazione del MAC

13.3. Verifica e decifratura del payload del tachigrafo

14. FIRMA DEL TRASFERIMENTO DEI DATI E VERIFICA DELLE FIRME

14.1. Principi generali

14.2. Generazione della firma

14.3. Verifica della firma

▼B

PREAMBOLO

La presente appendice specifica i meccanismi di sicurezza atti a garantire:

— l'autenticazione reciproca tra i diversi componenti del sistema tachigrafico;

— la riservatezza, l'integrità, l'autenticità e/o la non disconoscibilità dei dati trasferiti tra diversi componenti del sistema tachigrafico o a dispositivi di memorizzazione esterni.

La presente appendice si articola in due parti. La parte A definisce i meccanismi di sicurezza per il sistema tachigrafico di prima generazione (tachigrafo digitale). La parte B definisce i meccanismi di sicurezza per il sistema tachigrafico di seconda generazione (tachigrafo intelligente).

I meccanismi di cui alla parte A della presente appendice si applicano se almeno uno dei componenti del sistema tachigrafico coinvolti nell'autenticazione reciproca e/o nella procedura di trasferimento dei dati è di prima generazione.

I meccanismi di cui alla parte B della presente appendice si applicano se entrambi i componenti del sistema tachigrafico coinvolti nell'autenticazione reciproca e/o nella procedura di trasferimento dei dati sono di seconda generazione.

L'appendice 15 fornisce maggiori informazioni in merito all'uso di componenti di prima generazione in combinazione con componenti di seconda generazione.

PARTE A

SISTEMA TACHIGRAFICO DI PRIMA GENERAZIONE

1. INTRODUZIONE

1.1. **Riferimenti**

Nella presente appendice si rimanda alle seguenti norme:

SHA-1	National Institute of Standards and Technology (NIST). *FIPS Publication 180-1: Secure Hash Standard*. April 1995.
PKCS1	RSA Laboratories. PKCS # 1: *RSA Encryption Standard*. Version 2.0. October 1998.
TDES	National Institute of Standards and Technology (NIST). *FIPS Publication 46-3: Data Encryption Standard*. Draft 1999.
TDES-OP	ANSI X9.52, Triple Data Encryption Algorithm Modes of Operation. 1998.
ISO/IEC 7816-4	Information Technology — Identification cards — Integrated circuit(s) cards with contacts — Part 4: Interindustry commands for interexchange. First edition: 1995 + Amendment 1: 1997 (Tecnologie dell'informazione — Carte di identificazione — Carte a circuito/i integrato/i con contatti — Parte 4: Comandi interindustriali per l'interscambio. Prima edizione 1995 + Modifica 1: 1997).
ISO/IEC 7816-6	Information Technology — Identification cards — Integrated circuit(s) cards with contacts — Part 6: Interindustry data elements. First edition: 1996 + Cor 1: 1998 (Tecnologie dell'informazione — Carte di identificazione — Carte a circuito/i integrato/i con contatti — Parte 6: Elementi di dati interindustriali. Prima edizione 1996 + Cor 1: 1998).
ISO/IEC 7816-8	Information Technology — Identification cards — Integrated circuit(s) cards with contacts — Part 8: Security related interindustry commands. First edition 1999 (Tecnologie dell'informazione — Carte di identificazione — Carte a circuito/i integrato/i con contatti — Parte 8: Comandi interindustriali concernenti la sicurezza. Prima edizione 1999).
ISO/IEC 9796-2	Information Technology — Security techniques — Digital signature schemes giving message recovery — Part 2: Mechanisms using a hash function. First edition: 1997. (Tecnologie dell'informazione — Tecniche di sicurezza — Schemi per firme digitali con recupero dei messaggi — Parte 2: Meccanismi che usano una funzione di hash. Prima edizione 1997).

▼B

ISO/IEC 9798-3	Information Technology — Security techniques — Entity authentication mechanisms — Part 3: Entity authentication using a public key algorithm. Second edition 1998 (Tecnologie dell'informazione — Tecniche di sicurezza — Meccanismi di autenticazione di entità — Parte 3: Autenticazione di entità con un algoritmo a chiave pubblica. Seconda edizione 1998)
ISO 16844-3	Road vehicles — Tachograph systems — Part 3: Motion sensor interface (Veicoli stradali — Sistemi tachigrafici — Parte 3: Interfaccia del sensore di movimento).

1.2. **Simboli e abbreviazioni**

Nella presente appendice sono stati usati i seguenti simboli e abbreviazioni:

(K_a, K_b, K_c)	insieme di chiavi usate dall'algoritmo di cifratura Triple Data Encryption Algorithm,
CA	autorità di certificazione,
CAR	riferimento dell'autorità di certificazione,
CC	totale di controllo crittografico,
CG	crittogramma,
CH	intestazione del comando (Command Header),
CHA	autorizzazione del titolare del certificato,
CHR	riferimento del titolare del certificato,
D()	decifrazione con DES,
DE	elemento di dati (Data Element),
DO	oggetto di dati (Data Object),
d	chiave privata RSA, esponente privato,
e	chiave pubblica RSA, esponente pubblico,
E()	cifratura con DES,
EQT	apparecchio,
Hash()	valore di hash, un prodotto di *Hash*,
Hash	funzione di hash,
KID	identificativo della chiave,
Km	chiave in TDES, chiave master (master key) definita nella norma ISO 16844-3,
Km_{VU}	chiave in TDES inserita nell'unità elettronica di bordo dei veicoli,
Km_{WC}	chiave in TDES inserita nella carta dell'officina,
m	messaggio, un numero intero compreso tra 0 e *n*-1,
n	chiavi RSA, modulo,
PB	byte di riempimento,
PI	byte indicatore di riempimento (da usare nel crittogramma per i DO di riservatezza),
PV	valore in chiaro,
s	firma, un numero intero compreso tra 0 e *n*-1,
SSC	contatore sequenza di invio,
SM	messaggistica sicura,
TCBC	modalità di funzionamento a blocchi incatenati (Chipher Block Chaining) del TDEA,

▼B

TDEA	algoritmo di cifratura Triple Data Encryption Algorithm,
TLV	valore lunghezza tag (Tag Length Value),
VU	unità elettronica di bordo,
X.C	certificato dell'utente X rilasciato da un'autorità di certificazione,
X.CA	autorità di certificazione dell'utente X,
X.CA.PK $_{o}$ X.C	operazione di apertura di un certificato per estrarre una chiave pubblica; si tratta di un operatore infisso, il cui operando di sinistra è la chiave pubblica di un'autorità di certificazione e il cui operando di destra è il certificato rilasciato da tale autorità di certificazione; il risultato è la chiave pubblica dell'utente X il cui certificato è l'operando di destra,
X.PK	chiave privata RSA di un utente X,
X.PK[I]	cifratura RSA di un'informazione I, utilizzando la chiave pubblica dell'utente X,
X.SK	chiave privata RSA di un utente X,
X.SK[I]	cifratura RSA di un'informazione I, utilizzando la chiave privata dell'utente X,
‘xx’	valore esadecimale,
||	operatore di concatenamento.

2. SISTEMI E ALGORITMI CRITTOGRAFICI

2.1. **Sistemi crittografici**

CSM_001 Le unità elettroniche di bordo e le carte tachigrafiche devono utilizzare un sistema crittografico RSA tradizionale a chiave pubblica per fornire i seguenti meccanismi di sicurezza:

— autenticazione tra unità elettroniche di bordo e carte,

— trasporto di chiavi di sessione Triple-DES (TDES) tra unità elettroniche di bordo e carte tachigrafiche,

— firma digitale dei dati trasferiti dalle unità elettroniche di bordo o dalle carte tachigrafiche a dispositivi esterni.

CSM_002 Le unità elettroniche di bordo e le carte tachigrafiche devono utilizzare un sistema di crittografia simmetrica Triple DES per prevedere un meccanismo atto a garantire l'integrità dei dati durante lo scambio di dati dell'utente tra unità elettroniche di bordo e carte tachigrafiche e per garantire, se del caso, la riservatezza dello scambio di dati tra unità elettroniche di bordo e carte tachigrafiche.

2.2. **Algoritmi crittografici**

2.2.1 *Algoritmo RSA*

CSM_003 L'algoritmo RSA è interamente definito dalle seguenti relazioni:

▼B

$$X.SK[m] = s = m^d \bmod n$$

$$X.PK[s] = m = s^e \bmod n$$

Una descrizione più esauriente della funzione RSA è riportata nel riferimento [PKCS1]. L'esponente pubblico *e* nei calcoli dell'RSA è un numero intero compreso tra 3 e n-1 che soddisfa la seguente equazione: gcd(e, lcm(p-1, q-1))=1.

2.2.2 *Algoritmo di hash*

CSM_004 I meccanismi di firma digitale devono utilizzare l'algoritmo di hash SHA-1 definito nel riferimento [SHA-1].

2.2.3 *Algoritmo di cifratura dei dati*

CSM_005 Nella modalità di funzionamento a blocchi incatenati (Chipher Block Chaining) occorre usare algoritmi basati su DES.

3. CHIAVI E CERTIFICATI

3.1. **Generazione e distribuzione di chiavi**

3.1.1 *Generazione e distribuzione di chiavi RSA*

CSM_006 Le chiavi RSA devono essere generate in base a tre livelli gerarchici funzionali:

— livello europeo,

— livello di Stato membro,

— livello di apparecchio.

CSM_007 A livello europeo, deve essere generata un'unica coppia di chiavi europee (EUR.SK e EUR.PK). La chiave privata europea deve essere usata per certificare le chiavi pubbliche degli Stati membri. Devono essere conservate registrazioni di tutte le chiavi certificate. Queste funzioni devono essere espletate da un'autorità europea di certificazione, sotto l'autorità e la responsabilità della Commissione europea.

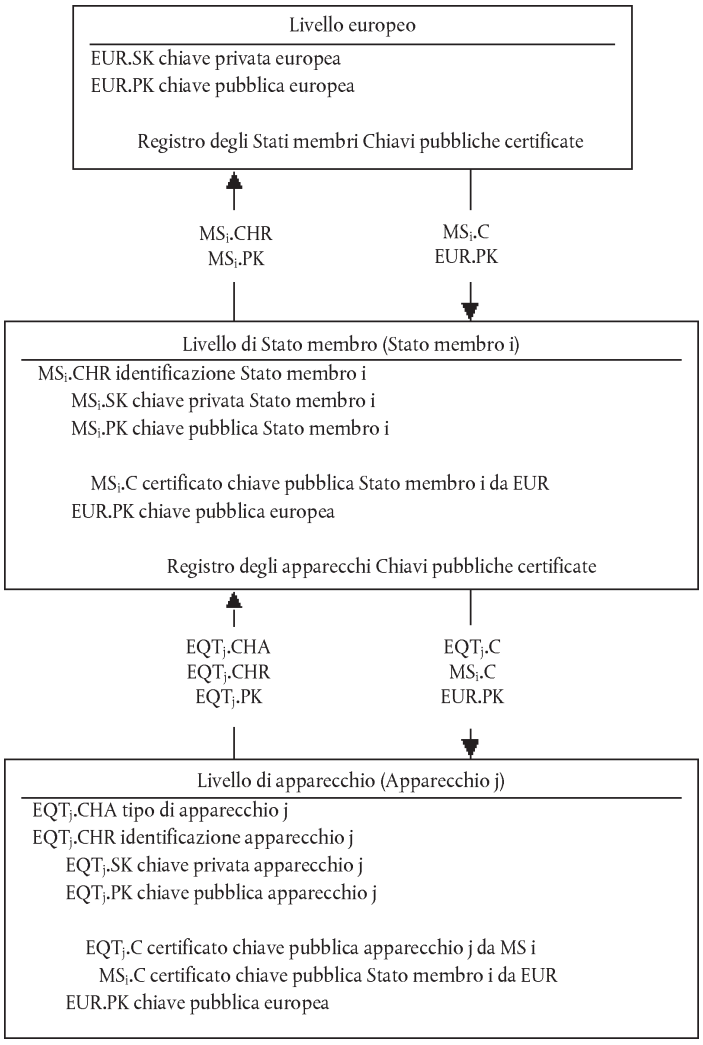
CSM_008 A livello di Stato membro, deve essere generata una coppia di chiavi dello Stato membro (MS.SK e MS.PK). Le chiavi pubbliche degli Stati membri devono essere certificate dall'autorità europea di certificazione. La chiave privata degli Stati membri deve essere usata per certificare le chiavi pubbliche da inserire nell'apparecchio (unità elettronica di bordo o carta tachigrafica). Devono essere conservate registrazioni di tutte le chiavi pubbliche certificate insieme all'identificazione dell'apparecchio cui sono destinate. Queste funzioni devono essere espletate da un'autorità di certificazione nazionale dello Stato membro. Gli Stati membri possono cambiare periodicamente la propria coppia di chiavi.

CSM_009 A livello di apparecchio, deve essere generata e inserita in ciascun apparecchio un'unica coppia di chiavi (EQT.SK e EQT.PK). Le chiavi pubbliche degli apparecchi devono essere certificate da un'autorità di certificazione nazionale dello Stato membro. Queste funzioni possono essere espletate dai fabbricanti di apparecchi, dai centri che personalizzano gli apparecchi o dalle autorità degli Stati membri. Questa coppia di chiavi è usata per l'autenticazione, la firma digitale e i servizi di cifratura.

CSM_010 Durante la generazione, il trasporto (se del caso) e l'immagazzinamento deve essere preservata la riservatezza delle chiavi private.

▼B

L'illustrazione seguente riepiloga il flusso di dati della suddetta procedura:



3.1.2 *Chiavi di prova RSA*

CSM_011 Ai fini delle prove dell'apparecchio (comprese le prove di interoperabilità), l'autorità europea di certificazione deve generare un'apposita diversa coppia di chiavi di prova europee e almeno due coppie di chiavi di prova per ogni Stato membro, le cui chiavi pubbliche devono essere certificate con la chiave di prova privata europea. I fabbricanti devono inserire nell'apparecchio sottoposto alle prove di omologazione chiavi di prova certificate da una di tali chiavi di prova degli Stati membri.

3.1.3 *Chiavi per i sensori di movimento*

La riservatezza delle tre chiavi Triple DES descritte di seguito deve essere opportunamente garantita quando vengono generate, trasferite (se del caso) e memorizzate.

Per assicurare la compatibilità con componenti di tachigrafi conformi alla norma ISO 16844, l'autorità di certificazione europea e le autorità di certificazione degli Stati membri devono inoltre garantire quanto segue:

CSM_036 l'autorità di certificazione europea deve generare KmVU e KmWC, due chiavi Triple DES uniche e indipendenti, e la chiave Km, come: $Km = Km_{VU}$ XOR Km_{WC}. L'autorità di certificazione europea deve inviare tali chiavi, applicando le opportune procedure di sicurezza, alle autorità di certificazione degli Stati membri che ne fanno richiesta.

▼B

CSM_037 Le autorità di certificazione degli Stati membri devono:

— utilizzare Km per crittare i dati relativi ai sensori di movimento richiesti dai produttori di tali sensori (i dati da crittare con Km sono indicati nella norma ISO 16844-3),

— inviare Km_{VU} ai fabbricanti delle unità elettroniche di bordo, applicando le opportune procedure di sicurezza, in modo che essi possano inserirla in tali unità,

— assicurare che Km_{WC} sia inserita in tutte le carte di officina (`SensorInstallationSecData` nel file elementare `Sensor_Installation_Data`) nel corso della personalizzazione della carta.

3.1.4 *Generazione e distribuzione di chiavi T-DES*

CSM_012 Nell'ambito della procedura di autenticazione reciproca, le unità elettroniche di bordo e le carte tachigrafiche devono generare e scambiare i dati necessari a elaborare una chiave comune di sessione Triple DES. Per garantire la riservatezza, tale scambio di dati deve essere protetto mediante un meccanismo di cifratura RSA.

CSM_013 Questa chiave deve essere usata per tutte le successive operazioni crittografiche che utilizzano la messaggistica sicura. La sua validità deve scadere al termine della sessione (estrazione o reinizializzazione della carta) e/o dopo 240 impieghi (un impiego della chiave = un comando che utilizza la messaggistica sicura inviato alla carta e relativa risposta).

3.2. **Chiavi**

CSM_014 La lunghezza delle chiavi RSA deve essere la seguente (indipendentemente dal livello): modulo *n* 1 024 bit, esponente pubblico *e* 64 bit al massimo, esponente privato *d* 1 024 bit.

CSM_015 Le chiavi Triple DES devono avere il formato (K_a, K_b, K_a), dove K_a e K_b sono chiavi indipendenti lunghe 64 bit. Non deve essere impostato alcun bit di rilevamento dell'errore di parità.

3.3. **Certificati**

CSM_016 I certificati delle chiavi pubbliche RSA devono essere verificabili mediante carta (card verifiable) e non autodescrittivi (non self-descriptive) (rif.: ISO/CEI 7816-8)

3.3.1 *Contenuto dei certificati*

CSM_017 I certificati delle chiavi pubbliche RSA sono costruiti con i dati sotto riportati nell'ordine seguente:

Dati	Formato	Byte	Osservazioni
CPI	INTEGER	1	Identificativo del profilo del certificato (“01” per questa versione).
CAR	OCTET STRING	8	Riferimento dell'autorità di certificazione.
CHA	OCTET STRING	7	Autorizzazione del titolare del certificato.

▼B

Dati	Formato	Byte	Osservazioni
EOV	TimeReal	4	Termine di validità del certificato. Facoltativo, riempito con “FF” se non utilizzato.
CHR	OCTET STRING	8	Riferimento del titolare del certificato.
n	OCTET STRING	128	Chiave pubblica (modulo).
e	OCTET STRING	8	Chiave pubblica (esponente pubblico).
		164	

Note:

1. L'«identificativo del profilo del certificato» (CPI) definisce la struttura precisa di un certificato di autenticazione. Si può usare come un identificativo interno all'apparecchio di un elenco di intestazioni (headerlist) pertinente che descrive il concatenamento di elementi di dati nel certificato.

   L'elenco di intestazioni (headerlist) associato al contenuto di questo certificato è il seguente:

‘4D’	‘16’	‘5F 29’	‘01’	‘42’	‘08’	‘5F 4B’	‘07’	‘5F 24’	‘04’	‘5F 20’	‘08’	‘7F 49’	‘05’	‘81’	‘81 80’	‘82’	‘08’
Tag elenco di intestazioni esteso (Extended Headerlist Tag)	Lunghezza elenco di intestazioni	Tag CPI	Lunghezza CPI	Tag CAR	Lunghezza CAR	Tag CHA	Lunghezza CHA	Tag EOV	Lunghezza EOV	Tag CHR	Lunghezza CHR	Tag chiave pubblica (costruito)	Lunghezza DO successivi	Tag modulo	Lunghezza modulo	Tag esponente pubblico	Lunghezza esponente pubblico

2. Il «riferimento dell'autorità di certificazione» (CAR) ha lo scopo di identificare l'autorità di certificazione che rilascia il certificato, in modo che l'elemento di dati si possa contemporaneamente usare come un identificativo della chiave dell'autorità in riferimento alla chiave pubblica dell'autorità di certificazione (per la codifica, cfr. identificativo della chiave).

3. L'«autorizzazione del titolare del certificato» (CHA) è usata per identificare i diritti del titolare del certificato. È costituita dall'ID dell'applicazione tachigrafica e del tipo di apparecchio cui è destinato il certificato (secondo l'elemento di dati `EquipmentType`, “00” per uno Stato membro).

▼B

4. Il «riferimento del titolare del certificato» (CHR) ha lo scopo di identificare inequivocabilmente il titolare del certificato, in modo che l'elemento di dati si possa contemporaneamente usare come un identificativo della chiave di un soggetto in riferimento alla chiave pubblica del titolare del certificato.

5. Gli identificativi delle chiavi identificano inequivocabilmente il titolare del certificato o le autorità di certificazione. Sono codificati come segue:

5.1. Apparecchio (VU o carta):

Dati	Numero di serie dell'apparecchio	Data	Tipo	Fabbricante
Lunghezza	4 byte	2 byte	1 byte	1 byte
Valore	Numero intero	mm aa codifica BCD	Specifico per ciascun fabbricante	Codice fabbricante

Nel caso di una VU, il fabbricante, quando richiede i certificati, può conoscere o meno l'identificazione dell'apparecchio in cui saranno inserite le chiavi.

Nel primo caso, il fabbricante invia l'identificazione dell'apparecchio con la chiave pubblica all'autorità di certificazione del suo Stato membro. Il certificato conterrà l'identificazione dell'apparecchio e il fabbricante deve garantire che le chiavi e il certificato siano inseriti nell'apparecchio cui sono destinati. Il formato dell'identificativo della chiave è quello sopra riportato.

Nel secondo caso, il fabbricante deve identificare inequivocabilmente ciascuna richiesta di certificato e inviare tale identificazione con la chiave pubblica all'autorità di certificazione del suo Stato membro. Il certificato conterrà l'identificazione della richiesta. Il fabbricante deve comunicare all'autorità del suo Stato membro l'assegnazione della chiave all'apparecchio (cioè identificazione della richiesta di certificato, identificazione dell'apparecchio) dopo l'installazione della chiave nell'apparecchio. L'identificativo della chiave ha il formato seguente:

Dati	Numero di serie richiesta certificato	Data	Tipo	Fabbricante
Lunghezza	4 byte	2 byte	1 byte	1 byte
Valore	Numero intero	mm aa codifica BCD	“FF”	Codice fabbricante

▼B

5.2. Autorità di certificazione:

Dati	Identificazione autorità	Numero di serie chiave	Informazioni supplementari	Identificativo
Lunghezza	4 byte	1 byte	2 byte	1 byte
Valore	1 byte codice numerico paese 3 byte codice alfanumerico paese	Numero intero	Codifica aggiuntiva (specifica per CA) “FF FF” se non utilizzata	‘01’

Il numero di serie della chiave è usato per distinguere le diverse chiavi di uno Stato membro, nel caso in cui la chiave venga cambiata.

6. I verificatori dei certificati devono sapere implicitamente che la chiave pubblica certificata è una chiave RSA concernente l'autenticazione, la verifica delle firme digitali e la cifratura per i servizi di riservatezza [il certificato non contiene un identificativo di oggetto (object identifier) che lo specifichi].

3.3.2 *Rilascio dei certificati*

CSM_018 Il certificato rilasciato è una firma digitale con recupero parziale del contenuto del certificato conformemente alla norma ISO/IEC 9796-2 (tranne l'allegato A4), con il CAR aggiunto in coda.

$$X.C = X.CA.SK[\text{‘6A’} \parallel C_r \parallel \mathit{Hash}(Cc) \parallel \text{‘BC’}] \parallel C_n \parallel X.CAR$$

Dove il contenuto del certificato = Cc =	C_r	$\parallel$	C_n
	106 byte		58 byte

Note:

1. Questo certificato ha una lunghezza di 194 byte.

2. Il CAR, essendo nascosto dalla firma, è anche aggiunto in coda alla firma, in modo da consentire di selezionare la chiave pubblica dell'autorità di certificazione per la verifica del certificato.

3. Il verificatore del certificato deve conoscere implicitamente l'algoritmo usato dall'autorità di certificazione per firmare il certificato.

4. L'elenco di intestazioni associato al certificato rilasciato è il seguente:

‘7F 21’	‘09’	‘5F 37’	‘81 80’	‘5F 38’	‘3A’	‘42’	‘08’
Tag certificato CV (costruito)	Lunghezza DO successivi	Tag firma	Lunghezza firma	Tag resto	Lunghezza resto	Tag CAR	Lunghezza CAR

▼B

3.3.3 *Verifica e apertura dei certificati*

La verifica e l'apertura dei certificati consistono nel verificare la firma in base alla norma ISO/IEC 9796-2, recuperare il contenuto del certificato e la chiave pubblica in esso contenuta: X.PK = X.CA.PK_o X.C, e nel verificare la validità del certificato.

CSM_019 La procedura prevede le fasi seguenti:

Verifica firma e recupero contenuto:

— da X.C recuperare Sign, C_n' e CAR': X.C = Sign (128 byte) || C_n' (58 byte) || CAR' (8 byte)

— da CAR' selezionare la corretta chiave pubblica dell'autorità di certificazione (se non ancora effettuato con altri mezzi)

— aprire Sign con la chiave pubblica di CA: Sr'= X.CA.PK [Sign],

— controllare che Sr' inizi con ‘6A’ e termini con ‘BC’

— calcolare C_r' e H' da: Sr' = ‘6A’ || C_r' (106 byte) || H' (20 byte) || ‘BC’

— recuperare il contenuto del certificato C' = C_r ‘|| C_n’

— controllare che *Hash*(C') = H'

Se i controlli danno esito positivo il certificato è autentico, il suo contenuto è C'.

Verificare la validità. Da C':

— se applicabile, controllare data termine validità.

Recuperare e memorizzare la chiave pubblica, l'identificativo della chiave, l'autorizzazione del titolare del certificato e il termine di validità del certificato da C':

— X.PK = n || e

— X.KID = CHR

— X.CHA = CHA

— X.EOV = EOV

4. MECCANISMO DI AUTENTICAZIONE RECIPROCA

L'autenticazione reciproca tra le carte e le VU si basa sul principio seguente:

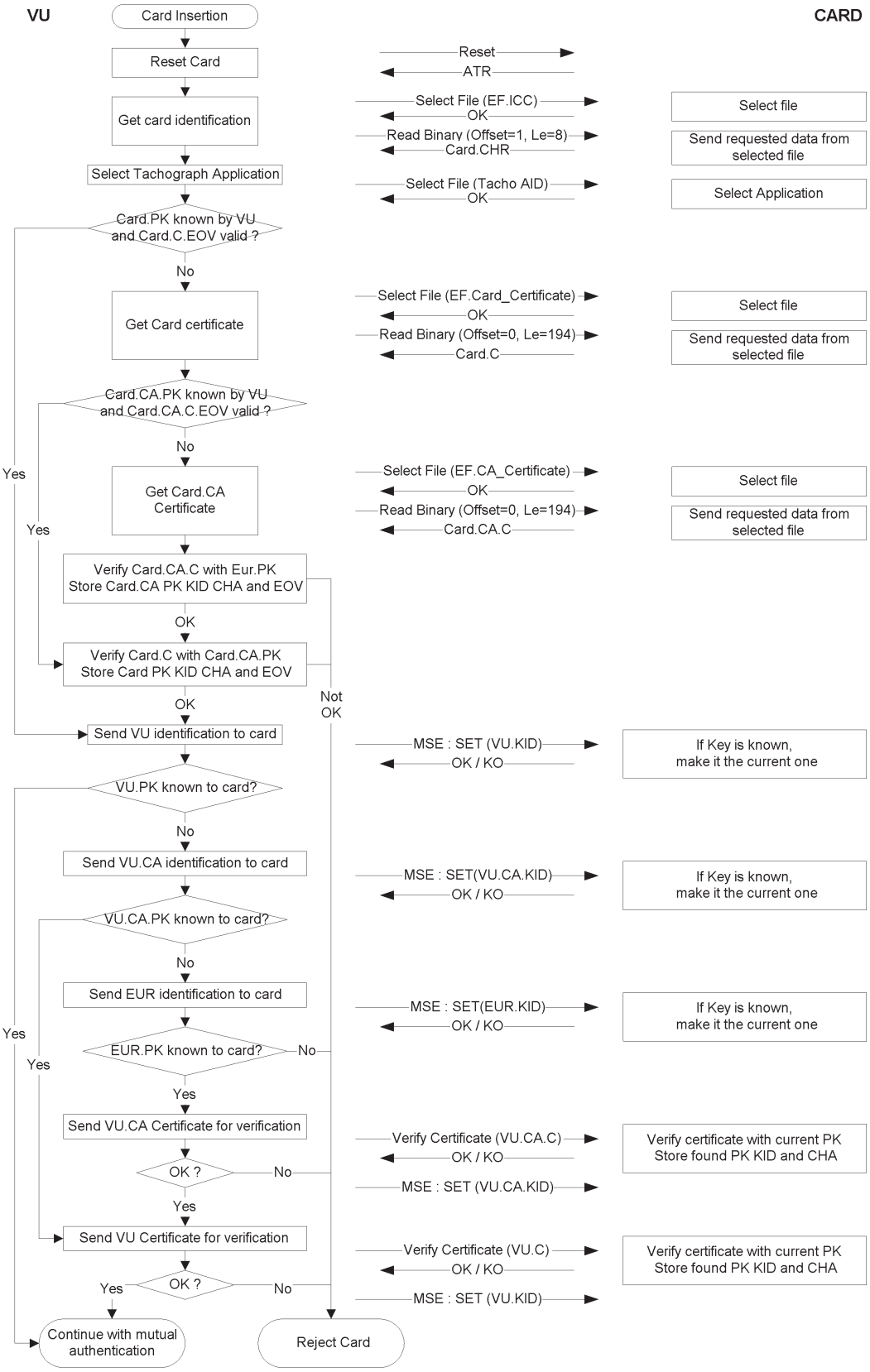
ogni parte deve dimostrare all'altra di possedere una coppia di chiavi valida, di cui la chiave pubblica è stata certificata da un'autorità di certificazione di uno Stato membro, la quale è stata a sua volta certificata dall'autorità di certificazione europea.

Tale dimostrazione è effettuata firmando con la chiave privata un numero casuale inviato dall'altra parte, che deve recuperare il numero casuale inviato quando verifica tale firma.

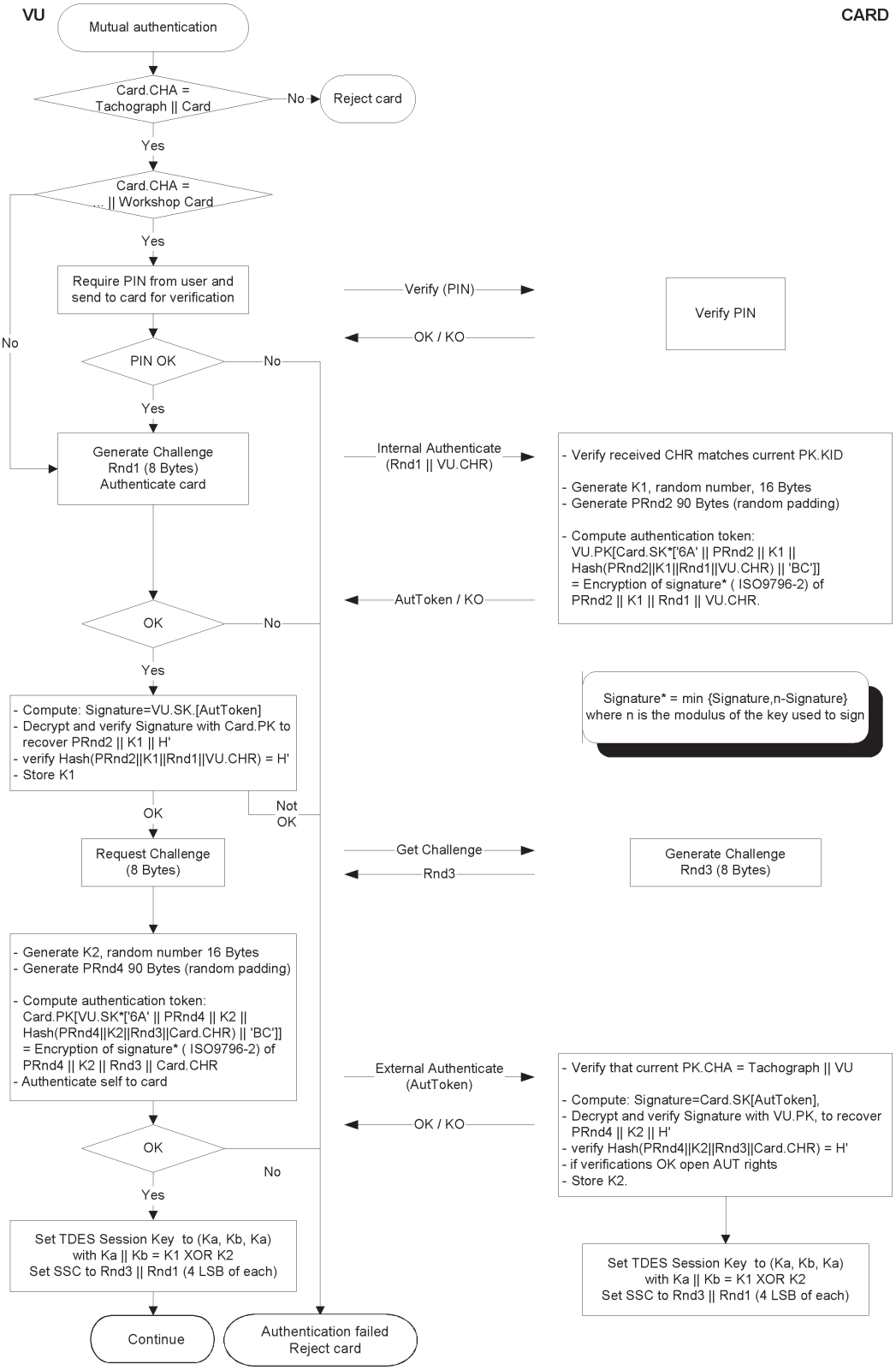
Il meccanismo è attivato dalla VU all'atto dell'inserimento della carta. Inizia con lo scambio di certificati e l'apertura delle chiavi pubbliche e termina con l'impostazione di una chiave di sessione.

▼B

CSM_020 Si deve utilizzare il seguente protocollo [le frecce indicano i comandi e i dati scambiati (cfr. appendice 2)]:



▼B


VU
CARD
Mutual authentication
Card.CHA = Tachograph || Card
No
Reject card
Yes
Card.CHA = ... || Workshop Card
Yes
Require PIN from user and send to card for verification
Verify (PIN)
Verify PIN
OK / KO
No
PIN OK
No
Yes
Generate Challenge Rnd1 (8 Bytes) Authenticate card
Internal Authenticate (Rnd1 || VU.CHR)
- Verify received CHR matches current PK.KID
- Generate K1, random number, 16 Bytes
- Generate PRnd2 90 Bytes (random padding)
- Compute authentication token: VU.PK[Card.SK*['6A' || PRnd2 || K1 || Hash(PRnd2||K1||Rnd1||VU.CHR) || 'BC']] = Encryption of signature* (ISO9796-2) of PRnd2 || K1 || Rnd1 || VU.CHR.
AutToken / KO
OK
No
Yes
Signature* = min {Signature,n-Signature} where n is the modulus of the key used to sign
- Compute: Signature=VU.SK.[AutToken]
- Decrypt and verify Signature with Card.PK to recover PRnd2 || K1 || H'
- verify Hash(PRnd2||K1||Rnd1||VU.CHR) = H'
- Store K1
OK
Not OK
Request Challenge (8 Bytes)
Get Challenge
Rnd3
Generate Challenge Rnd3 (8 Bytes)
- Generate K2, random number 16 Bytes
- Generate PRnd4 90 Bytes (random padding)
- Compute authentication token: Card.PK[VU.SK*['6A' || PRnd4 || K2 || Hash(PRnd4||K2||Rnd3||Card.CHR) || 'BC']] = Encryption of signature* (ISO9796-2) of PRnd4 || K2 || Rnd3 || Card.CHR
- Authenticate self to card
External Authenticate (AutToken)
- Verify that current PK.CHA = Tachograph || VU
- Compute: Signature=Card.SK[AutToken],
- Decrypt and verify Signature with VU.PK, to recover PRnd4 || K2 || H'
- verify Hash(PRnd4||K2||Rnd3||Card.CHR) = H'
- if verifications OK open AUT rights
- Store K2.
OK / KO
OK
No
Yes
Set TDES Session Key to (Ka, Kb, Ka) with Ka || Kb = K1 XOR K2 Set SSC to Rnd3 || Rnd1 (4 LSB of each)
Set TDES Session Key to (Ka, Kb, Ka) with Ka || Kb = K1 XOR K2 Set SSC to Rnd3 || Rnd1 (4 LSB of each)
Continue
Authentication failed Reject card

▼B

5. MECCANISMI DI RISERVATEZZA, INTEGRITÀ E AUTENTICAZIONE DEI TRASFERIMENTI DI DATI TRA VU E CARTE

5.1. **Messaggistica sicura (Secure Messaging)**

CSM_021 L'integrità dei trasferimenti di dati tra VU e carte deve essere protetta mediante messaggistica sicura (SM), in conformità alle norme [ISO/IEC 7816-4] e [ISO/IEC 7816-8].

CSM_022 Quando è necessario proteggere i dati durante il trasferimento, un oggetto di dati del totale di controllo crittografico (Cryptographic Checksum Data Object) deve essere aggiunto in coda agli oggetti di dati inviati all'interno del comando o della risposta. Il totale di controllo crittografico deve essere verificato dal destinatario.

CSM_023 Il totale di controllo crittografico dei dati inviati all'interno di un comando deve integrare l'intestazione del comando e tutti gli oggetti di dati inviati (= > CLA = '0C', e tutti gli oggetti di dati devono essere incapsulati con tag in cui b1 = 1).

CSM_024 I byte di informazione-stato della risposta devono essere protetti da un totale di controllo crittografico quando la risposta non contiene campi di dati.

CSM_025 I totali di controllo crittografico devono avere una lunghezza di 4 byte.

Quando si usa la messaggistica sicura, la struttura dei comandi e delle risposte è quindi la seguente:

i DO utilizzati sono una serie parziale dei DO della messaggistica sicura descritti nella norma ISO/IEC 7816-4:

Tag	Mnemonico	Significato
'81'	T_{PV}	Valore in chiaro, dati non codificati BER-TLV (da proteggere con CC)
'97'	$\mathbf{T_{LE}}$	Valore di Le nel comando non sicuro (da proteggere con CC)
'99'	T_{SW}	Informazione-stato (da proteggere con CC)
'8E'	T_{CC}	Totale di controllo crittografico
'87'	$T_{PI\ CG}$	Byte indicatore di riempimento || Crittogramma (valore in chiaro, non codificato in BER-TLV)

▼B

Data una coppia comando-risposta non sicuri:

Intestazione comando				Contenuto comando		
CLA	INS	P1	P2	[Campo L_c]	[Campo dati]	[Campo L_e]
quattro byte				L byte, indicati come B_1 — B_L		

Corpo della risposta	Coda della risposta	
[Campo dati]	SW1	SW2
Byte dati L_r	due byte	

La corrispondente coppia comando-risposta sicuri è:

Comando sicuro:

Intestazione comando (CH)				Contenuto comando										
CLA	INS	P1	P2	[Nuovo campo L_c]	[Nuovo campo dati]									[Nuovo campo L_e]
‘OC’				Lunghezza Nuovo campo dati	T_{PV}	L_{PV}	PV	T_{LE}	L_{LE}	L_e	T_{CC}	L_{CC}	CC	‘00’
					‘81’	L_c	Campo dati	‘97’	‘01’	L_e	‘8E’	‘04’	CC	

Dati da integrare nel totale di controllo = CH || PB || T_{PV} || L_{PV} || PV || T_{LE} || L_{LE} || L_e || PB

PB = Byte di riempimento (80 .. 00), in base alle norme ISO-IEC 7816-4 e ISO 9797, metodo 2.

DO PV e LE sono presenti solo se sono presenti dati corrispondenti nel comando non sicuro.

Risposta sicura:

1. Caso in cui il campo dati della risposta non è vuoto e non deve essere protetto a fini di riservatezza:

Corpo della risposta						Coda della risposta
[Nuovo campo dati]						Nuovi SW1 SW2
T_{PV}	L_{PV}	PV	T_{CC}	L_{CC}	CC	
‘81’	L_r	Campo dati	‘8E’	‘04’	CC	

Dati da integrare nel totale di controllo = T_{PV} || L_{PV} || PV || PB

2. Caso in cui il campo dati della risposta non è vuoto e deve essere protetto a fini di riservatezza:

▼B

Corpo della risposta						Coda della risposta
[Nuovo campo dati]						Nuovi SW1 SW2
$T_{PI\ CG}$	$L_{PI\ CG}$	PI CG	T_{CC}	L_{CC}	CC	
'87'		PI || CG	'8E'	'04'	CC	

Dati da trasportare da CG: dati non codificati BER-TLV e byte di riempimento.

Dati da integrare nel totale di controllo = $T_{PI\ CG}$ || $L_{PI\ CG}$ || PI CG || PB

3. Caso in cui il campo dati della risposta è vuoto:

Corpo della risposta						Coda della risposta
[Nuovo campo dati]						Nuovi SW1 SW2
T_{SW}	L_{SW}	SW	T_{CC}	L_{CC}	CC	
'99'	'02'	Nuovi SW1 SW2	'8E'	'04'	CC	

Dati da integrare nel totale di controllo = T_{SW} || L_{SW} || SW || PB

5.2. **Trattamento degli errori della messaggistica sicura**

CSM_026 Quando la carta tachigrafica riconosce un errore di SM durante l'interpretazione di un comando, i byte di stato devono essere restituiti senza SM. Secondo la norma ISO/IEC 7816-4, i seguenti byte di stato sono definiti come indicazioni di errore di SM:

'66 88': verifica di un totale di controllo crittografico fallita,

'69 87': oggetti di dati SM previsti mancanti,

'69 88': oggetti di dati SM non corretti.

CSM_027 Quando la carta tachigrafica restituisce i byte di stato senza DO SM o con un DO SM errato, la sessione deve essere annullata dalla VU.

5.3. **Algoritmo per il calcolo di totali di controllo crittografico**

CSM_028 I totali di controllo crittografico sono costruiti utilizzando un retail MAC, secondo ANSI X9.19, con DES:

— fase iniziale: il blocco di controllo iniziale y0 è E(Ka, SSC);

— fase sequenziale: i blocchi di controllo y1, .., yn sono calcolati usando Ka;

— fase finale: il totale di controllo crittografico è calcolato in base all'ultimo blocco di controllo yn come segue: E(Ka, D(Kb, yn)).

dove E() significa cifratura con DES e D() significa decifrazione con DES.

Vengono trasferiti i quattro byte più significativi del totale di controllo crittografico.

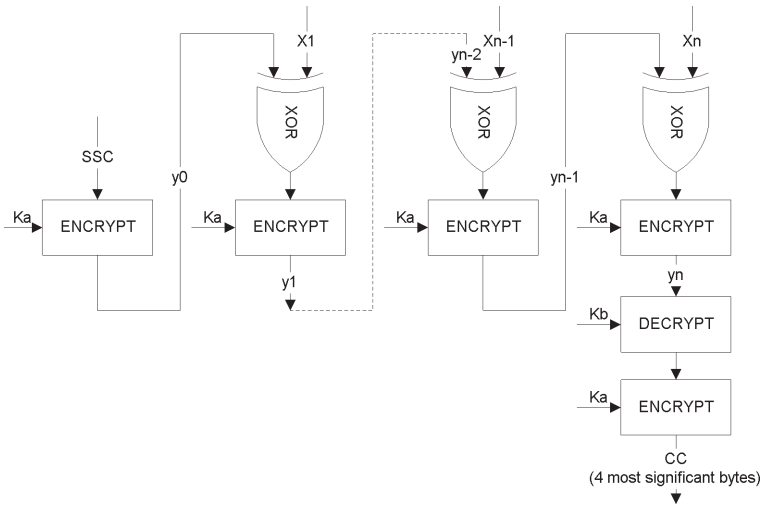
▼B

CSM_029 Il contatore sequenza di invio (SSC) deve essere inizializzato durante la procedura di accordo sulla chiave (key agreement procedure):

SSC iniziale: Rnd3 (4 byte meno significativi) || Rnd1 (4 byte meno significativi).

CSM_030 Il contatore sequenza di invio va aumentato di un'unità prima di ogni calcolo del MAC (cioè, l'SSC per il primo comando è SSC iniziale + 1, l'SSC per la prima risposta è SSC iniziale + 2).

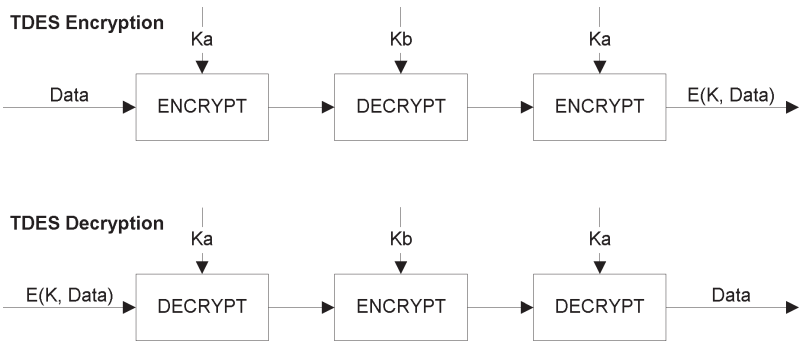
La figura seguente illustra il calcolo del retail MAC:



5.4. **Algoritmo per il calcolo di crittogrammi dei DO di riservatezza**

CSM_031 I crittogrammi sono calcolati utilizzando il TDEA nella modalità di funzionamento TCBC, secondo i riferimenti [TDES] e [TDES-OP] e con il vettore nullo come blocco valore iniziale.

La figura seguente illustra l'applicazione di chiavi in TDES:



▼B

6. MECCANISMI DI FIRMA DIGITALE PER IL TRASFERIMENTO DEI DATI

CSM_032 L'apparecchio intelligente dedicato (Intelligent dedicated equipment — IDE) memorizza in un file di dati fisico i dati ricevuti da un apparecchio (VU o carta) durante una sessione di trasferimento. Tale file deve contenere i certificati MS_i.C e EQT.C. Il file contiene firme digitali dei blocchi di dati secondo quanto specificato nell'appendice 7 «Protocolli di trasferimento dei dati».

CSM_033 Per le firme digitali dei dati trasferiti occorre adoperare uno schema di firma digitale con appendice tale che i dati trasferiti possano, se del caso, essere letti senza necessità di decifrazione.

6.1. **Generazione della firma**

CSM_034 La generazione di firme dei dati da parte dell'apparecchio deve seguire lo schema di firma con appendice definito nel riferimento [PKCS1] con la funzione di hash SHA-1:

Firma = EQT.SK[‘00’ || ‘01’ || *PS* || ‘00’ || DER(SHA-1(Data))]

PS = stringa di riempimento di ottetti con valore ‘FF’ in modo che la lunghezza sia 128.

DER(SHA-1(*M*)) è la codifica dell'algoritmo ID per la funzione di hash e il valore di hash in un valore ASN.1 di tipo DigestInfo (regole di codifica distinte):

‘30’||‘21’||‘30’||‘09’||‘06’||‘05’||‘2B’||‘0E’||‘03’||‘02’||‘1A’||
‘05’||‘00’ ‘04’||‘14’||valore di hash.

6.2. **Verifica della firma**

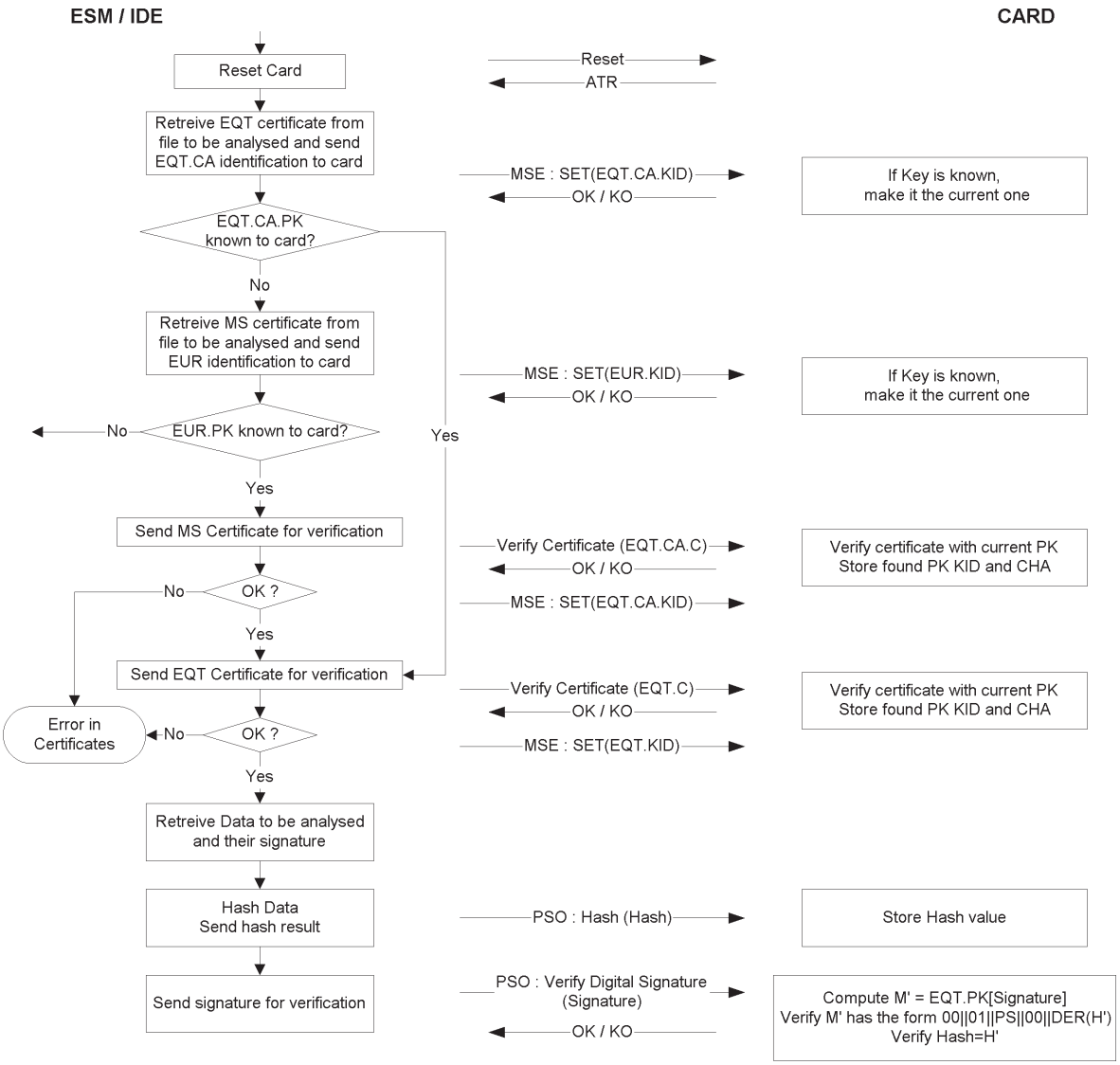
CSM_035 La verifica della firma dei dati sui dati trasferiti deve seguire lo schema di firma con appendice definito nel riferimento [PKCS1] con la funzione di hash SHA-1.

La chiave pubblica europea EUR.PK deve essere nota al verificatore in modo indipendente (e attendibile).

La tabella seguente illustra il protocollo che può seguire un IDE in cui sia stata inserita una carta di controllo per verificare l'integrità dei dati trasferiti e memorizzati nell'ESM (external storage media — dispositivo di memorizzazione esterno). La carta di controllo è usata per la decifrazione delle firme digitali. In questo caso, tale funzione può non essere implementata nell'IDE.

L'apparecchio che ha trasferito e firmato i dati da analizzare è indicato con EQT.

▼B



PARTE B

SISTEMA TACHIGRAFICO DI SECONDA GENERAZIONE

7. INTRODUZIONE

7.1. **Riferimenti**

In questa parte della presente appendice si rimanda alle seguenti norme.

AES	National Institute of Standards and Technology (NIST), FIPS PUB 197: Advanced Encryption Standard (AES), November 26, 2001
DSS	National Institute of Standards and Technology (NIST), FIPS PUB 186-4: Digital Signature Standard (DSS), July 2013
ISO 7816-4	ISO/IEC 7816-4, Identification cards — Integrated circuit cards — Part 4: Organization, security and commands for interchange. Third edition 2013-04-15 (ISO/IEC 7816-4, Carte di identificazione — Carte a circuito/i integrato/i — Parte 4: Organizzazione, sicurezza e comandi per l'interscambio. Terza edizione 2013-04-15).
ISO 7816-8	ISO/IEC 7816-8, Identification cards — Integrated circuit cards — Part 8: Commands for security operations. Second edition 2004-06-01 (ISO/IEC 7816-8, Carte di identificazione — Carte a circuito/i integrato/i — Parte 8: Comandi per le operazioni di sicurezza. Seconda edizione 2004-06-01).

▼B

ISO 8825-1	ISO/IEC 8825-1, Information technology — ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER). Fourth edition, 2008-12-15 [ISO/IEC 8825-1, Tecnologie dell'informazione — Regole di codifica ASN.1: specifiche delle regole di codifica di base (BER), regole di codifica canonica (CER) e regole di codifica distinta (DER). Quarta edizione 2008-12-15].
ISO 9797-1	ISO/IEC 9797-1, Information technology — Security techniques — Message Authentication Codes (MACs) — Part 1: Mechanisms using a block cipher. Second edition, 2011-03-01 [ISO/IEC 9797-1, Tecnologie dell'informazione — Tecniche di sicurezza — Codici di autenticazione del messaggio (MAC) — Parte 1: Meccanismi che usano una cifratura a blocchi. Seconda edizione 2011-03-01].
ISO 10116	ISO/IEC 10116, Information technology — Security techniques — Modes of operation of an *n*-bit block cipher. Third edition, 2006-02-01 (ISO/IEC 10116, Tecnologie dell'informazione — Tecniche di sicurezza — Modalità di funzionamento di una cifratura a blocchi a *n*-bit. Terza edizione 2006-02-01)
ISO 16844-3	ISO/IEC 16844-3, Road vehicles — Tachograph systems — Part 3: Motion sensor interface. First edition 2004, including Technical Corrigendum 1 2006 ((ISO/IEC 16844-3, Veicoli stradali — Sistemi tachigrafici — Parte 3: Interfaccia del sensore di movimento. Prima edizione 2004, compresa rettifica tecnica 1 2006).
RFC 5480	Elliptic Curve Cryptography Subject Public Key Information, March 2009
RFC 5639	Elliptic Curve Cryptography (ECC) — Brainpool Standard Curves and Curve Generation, 2010
RFC 5869	HMAC-based Extract-and-Expand Key Derivation Function (HKDF), May 2010
SHS	National Institute of Standards and Technology (NIST), FIPS PUB 180-4: Secure Hash Standard, March 2012
SP 800-38B	National Institute of Standards and Technology (NIST), Special Publication 800-38B: Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication, 2005
TR-03111	BSI Technical Guideline TR-03111, Elliptic Curve Cryptography, version 2.00, 2012-06-28

7.2. **Simboli e abbreviazioni**

Nella presente appendice sono stati usati i seguenti simboli e abbreviazioni:

AES	algoritmo di cifratura Advanced Encryption Standard
CA	autorità di certificazione
CAR	riferimento dell'autorità di certificazione
CBC	modalità di funzionamento a blocchi incatenati (Chipher Block Chaining)
CH	intestazione comando
CHA	autorizzazione del titolare del certificato
CHR	riferimento del titolare del certificato
CV	vettore costante
DER	regole di codifica distinte (Distinguished Encoding Rules)
DO	oggetto di dati (Data Object)
DSRC	comunicazione dedicata a corto raggio
ECC	crittografia a curve ellittiche
ECDSA	algoritmo di firma digitale su curva ellittica
ECDH	curva ellittica Diffie-Hellman [algoritmo di accordo sulla chiave (key agreement algorithm)]
EGF	dispositivo GNSS esterno
EQT	apparecchio

▼B

IDE	apparecchio intelligente dedicato (Intelligent Dedicated Equipment):
K_M	chiave master del sensore di movimento che consente l'abbinamento (pairing) di un'unità elettronica di bordo (VU) a un sensore di movimento
$K_{M\text{-}VU}$	chiave inserita nelle VU che consente a una VU di ricavare la chiave master del sensore di movimento se una carta dell'officina è inserita nella VU
$K_{M\text{-}WC}$	chiave inserita nelle carte dell'officina che consente a una VU di ricavare la chiave master del sensore di movimento se una carta dell'officina è inserita nella VU
MAC	codice di autenticazione del messaggio
MoS	sensore di movimento
MSB	bit più significativo
PKI	infrastruttura a chiave pubblica
RCF	dispositivo di comunicazione remota
SSC	contatore sequenza di invio
SM	messaggistica sicura
TDES	standard di cifratura Triple Date (Triple Data Encryption Standard)
TLV	valore lunghezza tag (Tag Length Value)
VU	unità elettronica di bordo
X.C	certificato di chiave pubblica dell'utente X
X.CA	autorità di certificazione che ha rilasciato il certificato dell'utente X
X.CAR	riferimento dell'autorità di certificazione citata nel certificato dell'utente X
X.CHR	riferimento del titolare del certificato citato nel certificato dell'utente X
X.PK	chiave pubblica dell'utente X
X.SK	chiave privata dell'utente X
$X.PK_{eph}$	chiave pubblica temporanea (ephemeral public key) dell'utente X
$X.SK_{eph}$	chiave privata temporanea (ephemeral private key) dell'utente X
'xx'	valore esadecimale
||	operatore di concatenamento

7.3. **Definizioni**

Le definizioni dei termini usati nella presente appendice sono riportate nella sezione I dell'allegato 1C.

8. SISTEMI E ALGORITMI CRITTOGRAFICI

8.1. **Sistemi crittografici**

CSM_38 Le unità elettroniche di bordo e le carte tachigrafiche devono utilizzare un sistema crittografico a chiave pubblica basato su curve ellittiche per fornire i seguenti servizi di sicurezza:

— autenticazione reciproca tra un'unità elettronica di bordo e una carta,

▼B

— accordo di chiavi di sessione AES tra un'unità elettronica di bordo e una carta,

— garantire l'autenticità, l'integrità e la non disconoscibilità dei dati trasferiti dalle unità elettroniche di bordo o dalle carte tachigrafiche a dispositivi esterni.

CSM_39 Le unità elettroniche di bordo e i dispositivi GNSS esterni devono utilizzare un sistema crittografico a chiave pubblica basato su curve ellittiche per fornire i seguenti servizi di sicurezza:

— accoppiamento di un'unità elettronica di bordo a un dispositivo GNSS esterno,

— autenticazione reciproca tra un'unità elettronica di bordo a un dispositivo GNSS esterno,

— accordo di una chiave di sessione AES tra un'unità elettronica di bordo e un dispositivo GNSS esterno,

CSM_40 Le unità elettroniche di bordo e le carte tachigrafiche devono utilizzare un sistema crittografico simmetrico basato su AES per fornire i seguenti servizi di sicurezza:

— garantire l'autenticità e l'integrità dei dati scambiati tra un'unità elettronica di bordo e una carta tachigrafica,

— se del caso, garantire la riservatezza dei dati scambiati tra un'unità elettronica di bordo e una carta tachigrafica.

CSM_41 Le unità elettroniche di bordo e i dispositivi GNSS esterni devono utilizzare un sistema crittografico simmetrico basato su AES per fornire i seguenti servizi di sicurezza:

— garantire l'autenticità e l'integrità dei dati scambiati tra un'unità elettronica di bordo e una dispositivo GNSS esterno.

CSM_42 Le unità elettroniche di bordo e i sensori di movimento devono utilizzare un sistema crittografico simmetrico basato su AES per fornire i seguenti servizi di sicurezza:

— abbinamento di un'unità elettronica di bordo a un sensore di movimento,

— autenticazione reciproca tra un'unità elettronica di bordo e un sensore di movimento,

— garantire la riservatezza dei dati scambiati tra un'unità elettronica di bordo e un sensore di movimento.

CSM_43 Le unità elettroniche di bordo e le carte di controllo devono utilizzare un sistema crittografico simmetrico basato su AES per fornire i seguenti servizi di sicurezza sull'interfaccia di comunicazione remota:

— garantire la riservatezza, l'autenticità e l'integrità dei dati trasmessi da un'unità elettronica di bordo a una carta di controllo.

Note:

— in realtà i dati sono trasmessi da una unità elettronica di bordo (VU) a un interrogatore remoto, sotto il controllo di un agente incaricato, che utilizza un dispositivo di comunicazione remota che può essere interno o

▼B

esterno alla VU, cfr. appendice 14. L'interrogatore remoto tuttavia invia i dati ricevuti a una carta di controllo per la decifrazione e la convalida dell'autenticità. Dal punto di vista della sicurezza, il dispositivo di comunicazione remota e l'interrogatore remoto sono completamente trasparenti.

— Per l'interfaccia DSRC una carta dell'officina offre gli stessi servizi di sicurezza di una carta di controllo. Ciò consente all'officina di convalidare il corretto funzionamento dell'interfaccia di comunicazione remota della VU, sicurezza inclusa. Per maggiori informazioni si veda la sezione 9.2.2.

8.2. **Algoritmi crittografici**

8.2.1 *Algoritmi simmetrici*

CSM_44 Le unità elettroniche di bordo, le carte tachigrafiche, i sensori di movimento e i dispositivi GNSS esterni devono essere compatibili con l'algoritmo AES, come definito nel riferimento [AES], con chiavi lunghe 128, 192 e 256 bit.

8.2.2 *Algoritmi asimmetrici e parametri di dominio standardizzati (standardized domain parameters)*

CSM_45 Le unità elettroniche di bordo, le carte tachigrafiche e i dispositivi GNSS esterni devono essere compatibili con la crittografia a curve ellittiche con chiavi lunghe 256, 384 e 512/521 bit.

CSM_46 Le unità elettroniche di bordo, le carte tachigrafiche e i dispositivi GNSS esterni devono essere compatibili con l'algoritmo di firma ECDSA, come specificato in [DSS].

CSM_47 Le unità elettroniche di bordo, le carte tachigrafiche e i dispositivi GNSS esterni devono essere compatibili con l'algoritmo di accordo sulla chiave (key agreement algorithm) ECKA-EG, come specificato in [TR 03111].

CSM_48 Le unità elettroniche di bordo, le carte tachigrafiche e i dispositivi GNSS esterni devono essere compatibili con tutti i parametri di dominio standardizzati specificati nella Tabella 1 seguente per la crittografia a curve ellittiche.

Tabella 1

Parametri di dominio standardizzati

Nome	Dimensioni (bit)	Riferimento	Identificativo di oggetto
NIST P-256	256	[DSS], [RFC 5480]	`secp256r1`
BrainpoolP256r1	256	[RFC 5639]	`brainpoolP256r1`
NIST P-384	384	[DSS], [RFC 5480]	`secp384r1`
BrainpoolP384r1	384	[RFC 5639]	`brainpoolP384r1`
BrainpoolP512r1	512	[RFC 5639]	`brainpoolP512r1`
NIST P-521	521	[DSS], [RFC 5480]	`secp521r1`

▼B

Nota: gli identificativi di oggetto (object identifiers) nell'ultima colonna della Tabella 1 sono specificati in [RFC 5639] per le curve Brainpool e in [RFC 5480] per le curve NIST.

Esempio 1: l'identificativo di oggetto per la curva BrainpoolP256r1 è `{iso(1) identified-organization(3) teletrust(36) algorithm(3) signaturealgorithm(3) ecSign(2) ecStdCurvesAndGeneration (8) ellipticCurve(1) versionOne(1) 7}`.

Oppure nella dot notation (notazione col punto): 1.3.36.3.3.2.8.1.1.7.

Esempio 2: l'identificativo di oggetto della curva NIST P-384 è

`{iso(1) identified-organization(3) certicom(132) curve(0) 34}`.

Oppure nella dot notation (notazione col punto):

8.2.3 *Algoritmi di hash*

CSM_49 Le unità elettroniche di bordo e le carte tachigrafiche devono essere compatibili con gli algoritmi SHA-256, SHA-384 e SHA-512 specificati nel riferimento [SHS].

8.2.4 *Suite crittografiche (cipher suites)*

CSM_50 Nel caso un algoritmo simmetrico, un algoritmo asimmetrico e/o un algoritmo di hash siano usati insieme per costituire un protocollo di sicurezza, le lunghezze delle rispettive chiavi e le dimensioni degli hash devono avere (approssimativamente) la stessa forza. Tabella 2 indica le suite crittografiche consentite:

Tabella 2

Suite crittografiche consentite

Id della suite crittografica	Dimensioni della chiave ECC (in bit)	Lunghezza della chiave AES (in bit)	Algoritmo di hash	Lunghezza MAC (in byte)
CS#1	256	128	SHA-256	8
CS#2	384	192	SHA-384	12
CS#3	512/521	256	SHA-512	16

Nota: le chiavi ECC delle dimensioni di 512 bit e 521 bit sono considerate di pari forza per tutti gli scopi previsti nella presente appendice.

9. CHIAVI E CERTIFICATI

9.1. **Coppie di chiavi asimmetriche e certificati delle chiavi pubbliche**

9.1.1 *Principi generali*

Nota: le chiavi descritte nella presente sezione sono usate per l'autenticazione reciproca e la messaggistica sicura tra unità elettroniche di bordo e carte tachigrafiche e tra unità elettroniche di bordo e dispositivi GNSS esterni. Queste procedure sono descritte in dettaglio nei capitoli 10 e 11 della presente appendice.

CSM_51 Nell'ambito del sistema tachigrafico intelligente europeo, le coppie di chiavi ECC e i certificati corrispondenti devono essere creati e gestiti in base a tre livelli gerarchici funzionali:

— livello europeo,

— livello di Stato membro,

— livello di apparecchio.

▼B

CSM_52 Nell'ambito del sistema tachigrafico intelligente europeo, le chiavi pubbliche e private e i certificati devono essere generati, gestiti e comunicati usando metodi standardizzati e sicuri.

9.1.2 *Livello europeo*

CSM_53 A livello europeo, deve essere generata una sola coppia di chiavi uniche ECC designata come EUR che si compone di una chiave privata (EUR.SK) e di una chiave pubblica EUR.PK. Questa coppia di chiavi deve costituire la coppia di chiavi radice (root) dell'intero del tachigrafo intelligente europeo PKI. Queste funzioni devono essere espletate dall'Autorità europea di certificazione primaria (European Root Certificate Authority — ERCA), sotto l'autorità e la responsabilità della Commissione europea.

CSM_54 La ERCA deve usare la chiave privata europea per firmare un certificato radice (autofirmato) della chiave pubblica europea e deve comunicare tale certificato radice a tutti gli Stati membri.

CSM_55 La ERCA deve usare la chiave privata europea per firmare, su richiesta, i certificati delle chiavi pubbliche degli Stati membri. La ERCA deve registrare tutti i certificati firmati delle chiavi pubbliche di uno Stato membro.

CSM_56 Come indicato nella Figura 1, sezione 9.1.7, la ERCA deve generare una nuova coppia di chiavi radice europee ogni 17 anni. Ogni volta che ciò accade, la ERCA deve creare un nuovo certificato radice autofirmato per la nuova chiave pubblica europea. Il periodo di validità di un certificato radice europeo deve essere di 34 anni più 3 mesi.

Nota: l'introduzione di una nuova coppia di chiavi radice implica inoltre che la ERCA genererà una nuova chiave master del sensore di movimento e una nuova chiave master DSRC, cfr. le sezioni 9.2.1.2 e 9.2.2.2.

CSM_57 Prima di generare una nuova coppia di chiavi radice europee, la ERCA deve effettuare un'analisi della forza crittografica necessaria per la nuova coppia di chiavi, dato che essa dovrebbe restare sicura per i successivi 34 anni. Se ritenuto necessario, la ERCA deve passare a una suite crittografica più forte di quella attuale, come specificato in CSM_50.

CSM_58 Ogni volta che si crea una nuova coppia di chiavi radice europee, la ERCA deve creare un certificato di collegamento (link certificate) per la nuova chiave pubblica europea e deve firmarlo con la precedente chiave privata europea. Il periodo di validità di un certificato di collegamento (link certificate) deve essere di 17 anni. Anch'esso è indicato nella Figura 1, sezione 9.1.7.

Nota: poiché un certificato di collegamento contiene la chiave pubblica ERCA della generazione *X* ed è firmato con la chiave privata ERCA della generazione *X-1*, un certificato di collegamento consente agli apparecchi della generazione *X-1* di considerare sicuri gli apparecchi della generazione *X*.

CSM_59 Non appena un nuovo certificato di chiavi radice diventa valido, la ERCA non deve usare la chiave privata di una coppia di chiavi radice per nessuno scopo.

▼B

CSM_60 In qualsiasi momento, la ERCA deve disporre dei seguenti certificati e chiavi crittografiche:

— la coppia di chiavi EUR attuale e il certificato corrispondente;

— tutti i precedenti certificati EUR da usare per la verifica dei certificati MSCA che sono ancora validi;

— i certificati di collegamento per tutte le generazioni di certificati EUR, eccetto la prima.

9.1.3 *Livello di Stato membro*

CSM_61 A livello di Stato membro, tutti gli Stati membri tenuti a firmare i certificati della carta tachigrafica devono generare una o più coppie di chiavi uniche ECC designate come MSCA_card. Tutti gli Stati membri tenuti a firmare i certificati per le unità elettroniche di bordo o i dispositivi GNSS esterni devono inoltre generare una o più coppie di chiavi uniche ECC designate come MSCA_VU-EGF.

CSM_62 Il compito di generare le coppie di chiavi dello Stato membro spetta all'autorità di certificazione dello Stato membro (Member State Certificate Authority — MSCA). Ogni volta che genera una coppia di chiavi dello Stato membro, la MSCA è tenuta a inviare la chiave pubblica alla ERCA in modo che quest'ultima possa firmare un corrispondente certificato dello Stato membro.

CSM_63 La forza di una coppia di chiavi dello Stato membro è scelta dalla MSCA e deve essere uguale alla forza della coppia di chiavi radice europee usate per firmare il corrispondente certificato dello Stato membro.

CSM_64 Una coppia di chiavi MSCA_VU-EGF, se presente, deve comporsi di una chiave privata MSCA_VU-EGF.SK e di una chiave pubblica MSCA_VU-EGF.PK. La MSCA deve usare la chiave privata MSCA_VU-EGF.SK solo per firmare i certificati della chiave pubblica delle unità elettroniche di bordo e dei dispositivi GNSS esterni.

CSM_65 Una coppia di chiavi MSCA_Card deve comporsi di una chiave privata MSCA_Card.SK e di una chiave pubblica MSCA_Card.PK. La MSCA deve usare la chiave privata MSCA_Card.SK esclusivamente per firmare i certificati della chiave pubblica delle carte tachigrafiche.

CSM_66 La MSCA deve registrare tutti i certificati firmati della VU, del dispositivo GNSS esterno e della carta tachigrafica, insieme all'identificazione dell'apparecchio cui è destinato ciascun certificato.

CSM_67 Il periodo di validità di un certificato MSCA_VU-EGF deve essere di 17 anni più 3 mesi. Il periodo di validità di un certificato MSCA_Card deve essere di 7 anni più 1 mese.

CSM_68 Come indicato nella Figura 1, sezione 9.1.7, la chiave privata di una coppia di chiavi MSCA_VU-EGF e la chiave privata di una coppia di chiavi MSCA_Card devono avere un periodo di utilizzo di due anni.

▼B

CSM_69 Dopo la fine del periodo di utilizzo, la MSCA non deve usare la chiave privata di una coppia di chiavi MSCA_VU-EGF per nessuno scopo. Allo stesso modo, dopo la fine del periodo di utilizzo, la MSCA non deve usare la chiave privata di una coppia di chiavi MSCA_Card per nessuno scopo.

CSM_70 In qualsiasi momento, la MSCA deve disporre dei seguenti certificati e chiavi crittografiche:

— la coppia di chiavi MSCA_Card attuale e il certificato corrispondente;

— tutti i precedenti certificati MSCA_Card da usare per la verifica dei certificati delle carte tachigrafiche che sono ancora validi;

— il certificato EUR attuale necessario alla verifica del certificato MSCA attuale;

— tutti i precedenti certificati EUR necessari alla verifica dei certificati MSCA che sono ancora validi;

CSM_71 Se una MSCA deve firmare certificati per VU o per dispositivi GNSS esterni, essa deve inoltre disporre dei seguenti certificati e chiavi:

— la coppia di chiavi MSCA_VU-EGF attuali e il certificato corrispondente;

— tutte le precedenti chiavi pubbliche MSCA_VU-EGF da usare per la verifica dei certificati delle VU o dei dispositivi GNSS esterni che sono ancora validi.

9.1.4 *Livello di apparecchio: unità elettroniche di bordo (VU)*

CSM_72 Due coppie di chiavi uniche ECC devono essere generate per ciascuna unità elettronica di bordo, designate come VU_MA e VU_sign. Questo compito spetta ai fabbricanti di VU. Ogniqualvolta si genera una coppia di chiavi della VU, la parte che genera la chiave deve inviare la chiave pubblica alla MSCA del paese in cui si risiede, in modo da ottenere un corrispondente certificato VU firmato dalla MSCA. La chiave privata deve essere usata solo dall'unità elettronica di bordo.

CSM_73 I certificati VU_MA e VU_Sign di una determinata unità elettronica di bordo devono avere la stessa data di efficacia (Certificate Effective Date).

CSM_74 La forza di una coppia di chiavi della VU è scelta dal fabbricante della VU e deve essere uguale alla forza della coppia di chiavi MSCA usate per firmare il corrispondente certificato della VU.

CSM_75 Una unità elettronica di bordo deve usare la propria coppia di chiavi VU_MA, composta da una chiave privata VU_MA.SK e da una chiave pubblica VU_MA.PK, esclusivamente per l'autenticazione della VU rispetto alle carte tachigrafiche e ai dispositivi GNSS esterni, come specificato nelle sezioni 10.3 e 11.4 della presente appendice.

CSM_76 Una unità elettronica di bordo deve essere in grado di generare coppie di chiavi ECC temporanee e deve utilizzare una coppia di chiavi temporanee esclusivamente per eseguire l'accordo sulla chiave di sessione con una carta tachigrafica o con un dispositivo GNSS esterno, come specificato nelle sezioni 10.4 e 11.4 della presente appendice.

▼B

CSM_77 Una unità elettronica di bordo deve usare la chiave privata VU_Sign.SK della coppia di chiavi VU_Sign esclusivamente per firmare i file di dati trasferiti, come specificato nel capitolo 14 della presente appendice. La corrispondente chiave pubblica VU_Sign.PK deve essere usata esclusivamente per verificare le firme create dall'unità elettronica di bordo.

CSM_78 Come mostrato in Figura 1, sezione 9.1.7, il periodo di validità di un certificato VU_MA deve essere di 15 anni più 3 mesi. Anche il periodo di validità di un certificato VU_Sign deve essere di 15 anni e 3 mesi.

Note:

— l'estensione del periodo di validità di un certificato VU_sign consente a una VU di creare firme valide per i dati trasferiti nel corso dei primi tre mesi dopo la sua scadenza, come previsto nel regolamento (UE) n. 581/2010.

— L'estensione del periodo di validità di un certificato VU_MA è necessaria per consentire alla VU di autenticare una carta di controllo o una carta dell'azienda durante i primi tre mesi dopo la sua scadenza, in modo che sia possibile effettuare un trasferimento di dati.

CSM_79 Dopo la scadenza del certificato corrispondente, l'unità elettronica di bordo non deve usare la chiave privata di una coppia di chiavi della VU per nessuno scopo.

CSM_80 Le coppie di chiavi della VU (eccetto le coppie di chiavi temporanee) e i certificati corrispondenti di una determinata unità elettronica di bordo non devono essere sostituiti o rinnovati sul campo una volta che l'unità elettronica di bordo è stata messa in funzione.

Note:

— Le coppie di chiavi temporanee non sono interessate da questo requisito, poiché a ogni esecuzione della autenticazione del chip (Chip Authentication) e dell'accordo sulla chiave di sessione (session key agreement) la VU genera una nuova coppia di chiavi temporanee, cfr. sezione 10.4. Si segnala che le coppie di chiavi temporanee non hanno certificati corrispondenti.

— Tale requisito non impedisce la sostituzione delle coppie di chiavi statiche della VU nel corso di un ricondizionamento o di una riparazione in un ambiente sicuro, controllato dal fabbricante della VU.

CSM_81 Al momento della messa in funzione, le unità elettroniche di bordo devono contenere i seguenti certificati e chiavi crittografiche:

— la chiave privata VU_MA e il certificato corrispondente;

— la chiave privata VU_Sign e il certificato corrispondente;

— il certificato MSCA_VU-EGF contenente la chiave pubblica MSCA_VU-EGF.PK da usare per la verifica del certificato VU_MA e del certificato VU_Sign;

▼B

— il certificato EUR contenente la chiave pubblica EUR.PK da usare per la verifica del certificato MSCA_VU-EGF;

— il certificato EUR il cui periodo di validità precede direttamente il periodo di validità del certificato EUR da usare per la verifica del certificato MSCA_VU-EGF, se presente;

— il certificato di collegamento che collega questi due certificati EUR, se presente.

CSM_82 In aggiunta alle chiavi crittografiche e ai certificati elencati in CSM_81, le unità elettroniche di bordo devono inoltre contenere le chiavi e i certificati specificati nella parte A della presente appendice, che consentono a una unità elettronica di bordo di interagire con le carte tachigrafiche di prima generazione.

9.1.5 *Livello di apparecchio: carte tachigrafiche*

CSM_83 Per ciascuna carta tachigrafica deve essere generata una coppia di chiavi uniche ECC, indicata come Card_MA. Inoltre, per ciascuna carta del conducente e per ciascuna carta dell'officina deve essere generata una seconda coppia di chiavi uniche ECC, indicata come Card_Sign. Questo compito può essere eseguito dai fabbricanti della carta o da chi personalizza la carta. Ogni volta che si genera una coppia di chiavi della carta, la parte che genera la chiave deve inviare la chiave pubblica alla MSCA del paese in cui si risiede, in modo da ottenere un corrispondente certificato della carta firmato dalla MSCA. La chiave privata deve essere usata solo dalla carta tachigrafica.

CSM_84 I certificati Card_MA e Card_Sign di una determinata carta del conducente o carta dell'officina devono avere la stessa data di efficacia (Certificate Effective Date).

CSM_85 La forza di una coppia di chiavi della carta deve essere scelta dal fabbricante della carta o da chi personalizza la carta e deve essere uguale alla forza della coppia di chiavi MSCA usate per firmare il corrispondente certificato della carta.

CSM_86 Una carta tachigrafica deve usare la propria coppia di chiavi Card_MA, composta da una chiave privata Card_MA.SK e da una chiave pubblica Card_MA.PK, esclusivamente per eseguire l'autenticazione reciproca e l'accordo sulle chiavi di sessione nei confronti delle unità elettroniche di bordo, come specificato nelle sezioni 10.3 e 10.4 della presente appendice.

CSM_87 Una carta del conducente o una carta dell'officina deve usare la chiave privata Card_Sign.SK della coppia di chiavi Card_Sign esclusivamente per firmare i file di dati trasferiti, come specificato nel capitolo 14 della presente appendice. La corrispondente chiave pubblica Card_Sign.PK deve essere usata esclusivamente per verificare le firme create dalla carta.

CSM_88 Il periodo di validità di un certificato Card_MA deve essere il seguente:

— per le carte del conducente: 5 anni;

— per le carte dell'azienda: 2 anni;

— per le carte di controllo: 2 anni;

— per le carte dell'officina: 1 anno.

▼B

CSM_89 Il periodo di validità di un certificato Card_Sign deve essere il seguente:

— per le carte del conducente: 5 anni e 1 mese;

— per le carte dell'officina: 1 anno e 1 mese.

Nota: l'estensione del periodo di validità di un certificato Card_Sign consente alla carta del conducente di creare firme valide per i dati trasferiti nel corso del primo mese dopo la sua scadenza. Ciò è necessario in ragione del Regolamento (UE) n. 581/2010 che impone che un trasferimento di dati da una carta del conducente deve essere possibile fino a 28 giorni dopo la registrazione dell'ultimo dato.

CSM_90 Le coppie di chiavi e i certificati corrispondenti di una determinata carta tachigrafica non devono essere sostituiti o rinnovati una volta che la carta è stata emessa.

CSM_91 Al momento del rilascio, le carte tachigrafiche devono contenere i seguenti certificati e chiavi crittografiche:

— la chiave privata Card_MA e il certificato corrispondente;

— per le carte del conducente e le carte dell'officina inoltre: la chiave privata Card_Sign e il certificato corrispondente;

— il certificato MSCA_Card contenente la chiave pubblica MSCA_Card.PK da usare per la verifica del certificato Card_MA e del certificato Card_Sign;

— il certificato EUR contenente la chiave pubblica EUR.PK da usare per la verifica del certificato MSCA_Card;

— il certificato EUR il cui periodo di validità precede direttamente il periodo di validità del certificato EUR da usare per la verifica del certificato MSCA_Card, se presente;

— il certificato di collegamento che collega questi due certificati EUR, se presente.

CSM_92 In aggiunta alle chiavi crittografiche e ai certificati elencati in CSM_91, le carte tachigrafiche devono inoltre contenere le chiavi e i certificati specificati nella parte A della presente appendice, che consentono a tali carte di interagire con le VU di prima generazione.

9.1.6 *Livello di apparecchio: dispositivi GNSS esterni*

CSM_93 Per ogni dispositivo GNSS esterno (EGF) deve essere generata una coppia di chiavi uniche ECC, indicata come EGF_MA. Questo compito spetta ai fabbricanti di dispositivi GNSS esterni. Ogniqualvolta si genera una coppia di chiavi EGF_MA, la chiave pubblica deve essere inviata alla MSCA del paese in cui si risiede, in modo da ottenere un corrispondente certificato EGF_MA firmato dalla MSCA. La chiave privata deve essere usata solo dal dispositivo GNSS esterno.

CSM_94 La forza di una coppia di chiavi EGF_MA deve essere scelta dal fabbricante dell'EGF e deve essere uguale alla forza della coppia di chiavi MSCA usate per firmare il corrispondente certificato EGF_MA.

▼B

CSM_95 Un dispositivo GNSS esterno deve usare la propria coppia di chiavi EGF_MA, composta da una chiave privata EGF_MA.SK e da una chiave pubblica EGF_MA.PK, esclusivamente per eseguire l'autenticazione reciproca e l'accordo sulle chiavi di sessione nei confronti delle unità elettroniche di bordo, come specificato nelle sezioni 11.4 e 11.4 della presente appendice.

CSM_96 Il periodo di validità di un certificato EGF_MA deve essere di 15 anni.

CSM_97 Dopo la scadenza del certificato corrispondente, il dispositivo GNSS esterno non deve usare la chiave privata della sua coppia di chiavi EGF_MA per l'accoppiamento con un'unità elettronica di bordo.

Nota: come spiegato nella sezione 11.3.3, un EGF può potenzialmente usare la sua chiave privata per l'autenticazione reciproca con la VU cui è già accoppiato, anche dopo la scadenza del certificato corrispondente.

CSM_98 La coppia di chiavi EGF_MA e il certificato corrispondente di un determinato dispositivo GNSS esterno non devono essere sostituiti o rinnovati sul campo una volta che l'EGF è stato messo in funzione.

Nota: tale requisito non impedisce la sostituzione delle coppie di chiavi EGF nel corso di un ricondizionamento o di una riparazione in un ambiente sicuro, controllato dal fabbricante dell'EGF.

CSM_99 Al momento della messa in funzione, i dispositivi GNSS esterni devono contenere i seguenti certificati e chiavi crittografiche:

— la chiave privata EGF_MA e il certificato corrispondente;

— il certificato MSCA_VU-EGF contenente la chiave pubblica MSCA_VU-EGF.PK da usare per la verifica del certificato EGF_MA;

— il certificato EUR contenente la chiave pubblica EUR.PK da usare per la verifica del certificato MSCA_VU-EGF;

— il certificato EUR il cui periodo di validità precede direttamente il periodo di validità del certificato EUR da usare per la verifica del certificato MSCA_VU-EGF, se presente;

— il certificato di collegamento che collega questi due certificati EUR, se presente.

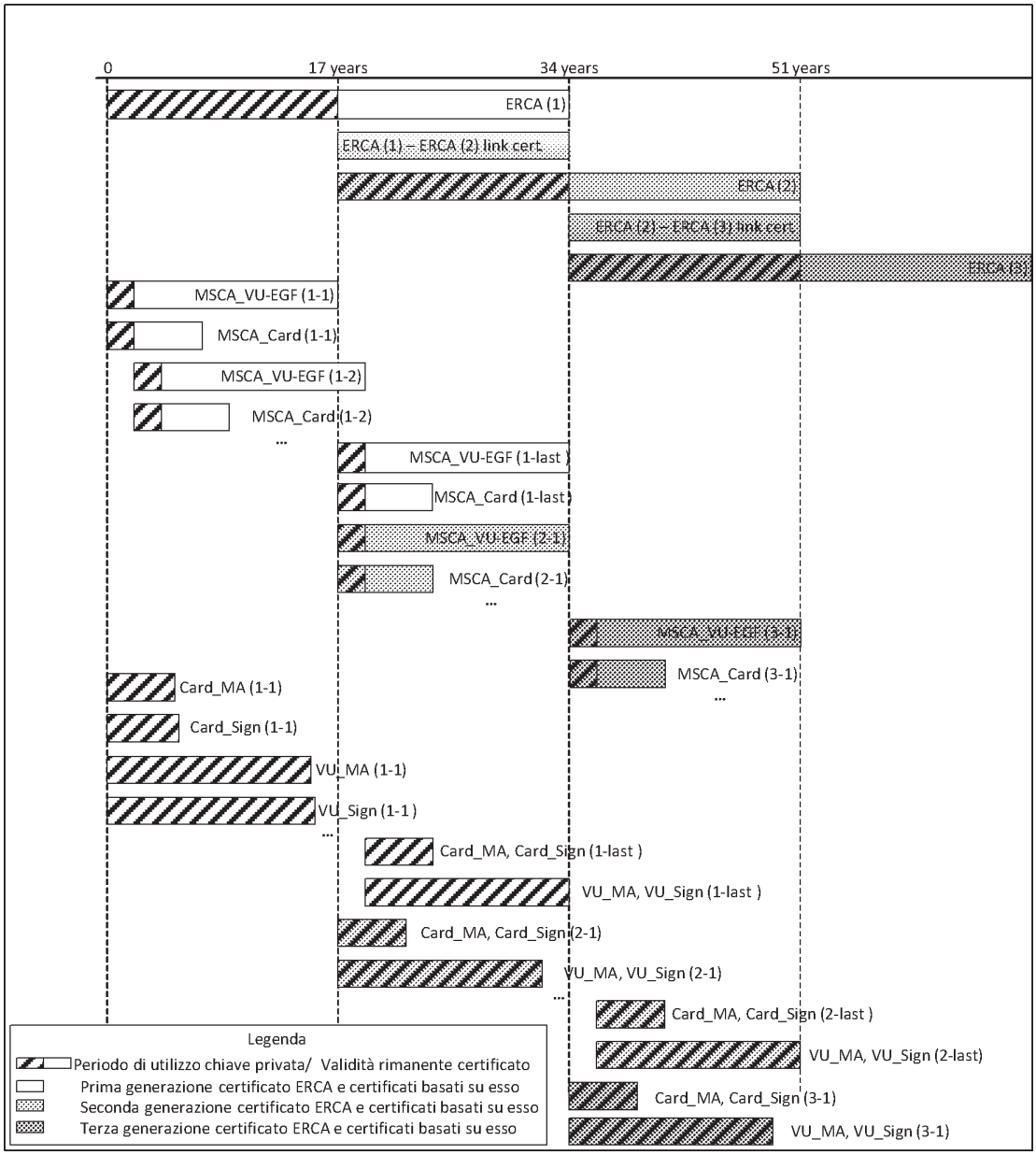
9.1.7 *Riepilogo: sostituzione dei certificati*

La Figura 1 di seguito mostra come diverse generazioni di certificati radice ERCA, di certificati di collegamento ERCA, di certificati MSCA e di certificati di dispositivo (VU o carta) siano rilasciati e usati nel tempo:

▼B

Figura 1

Rilascio e uso di diverse generazioni di certificati radice ERCA, certificati di collegamento ERCA, certificati MSCA e certificati di dispositivo



Note alla Figura 1:

1. Le diverse generazioni del certificato radice sono indicate con un numero tra parentesi. Ad esempio ERCA (1) è la prima generazione del certificato radice ERCA; ERCA (2) è la seconda generazione, ecc.

2. Altri certificati sono indicati da due numeri tra parentesi, di cui il primo indica la generazione del certificato radice in base al quale sono stati rilasciati e il secondo indica la generazione del certificato stesso. Ad esempio MSCA_Card (1-1) è il primo certificato MSCA_Card rilasciato in base a ERCA (1); MSCA_Card (2-1) è il primo certificato MSCA_Card rilasciato in base a ERCA (2); MSCA_Card (2-last) è l'ultimo certificato MSCA_Card rilasciato in base a ERCA (2); Card_MA (2-1) è il primo certificato della carta per l'autenticazione reciproca rilasciato in base a ERCA (2), ecc.

▼B

3. I certificati MSCA_Card (2-1) e MSCA_Card (1-last) sono rilasciati quasi, ma non esattamente, nella stessa data. MSCA_Card (2-1) è il primo certificato MSCA_Card rilasciato in base a ERCA (2) poco dopo MSCA_Card (1-last) che è l'ultimo certificato MSCA_Card rilasciato in base a ERCA (1).

4. Come indicato nella figura, i primi certificati della VU e della carta rilasciati in base a ERCA (2) compariranno quasi due anni prima degli ultimi certificati della VU e della carta rilasciati in base a ERCA (1). Ciò è dovuto al fatto che i certificati della VU e della carta sono rilasciati in base a un certificato MSCA e non direttamente in base al certificato ERCA. Il certificato MSCA (2-1) sarà rilasciato subito dopo l'inizio della validità di ERCA (2), ma il certificato MSCA (1-last) sarà rilasciato solo poco prima, nell'ultimo momento in cui il certificato ERCA (1) è ancora valido. Questi due certificati MSCA avranno quindi quasi lo stesso periodo di validità, nonostante appartengano a due diverse generazioni.

5. Il periodo di validità indicato per le carte è lo stesso di quello delle carte del conducente (5 anni).

6. Per motivi di spazio, la differenza del periodo di validità tra i certificati Card_MA e Card_Sign e tra i certificati VU_MA e VU_Sign è indicata solo per la prima generazione.

9.2. **Chiavi simmetriche**

9.2.1 *Chiavi per la sicurezza della comunicazione tra VU e sensore di movimento*

9.2.1.1 *Principi generali*

Nota: si presume che i lettori della presente sezione conoscano il contenuto della norma [ISO 16844-3] che descrive l'interfaccia tra una VU e un sensore di movimento. La procedura di abbinamento tra una VU e un sensore di movimento è descritta in dettaglio nel capitolo 12 della presente appendice.

CSM_100 L'abbinamento delle VU ai sensori di movimento, l'autenticazione reciproca tra le VU e i sensori di movimento e la cifratura della comunicazione tra le VU e i sensori di movimento necessitano di un certo numero di chiavi simmetriche, come indicato in Tabella 3. Tutte queste chiavi devono essere chiavi AES, di lunghezza uguale alla lunghezza della chiave master del sensore di movimento, che deve essere legata alla lunghezza della coppia di chiavi radice europee (prevista) come descritto in CSM_50.

Tabella 3

Chiavi per la sicurezza della comunicazione VU — sensore di movimento

Chiave	Simbolo	Generata da	Metodo di generazione	Memorizzata da
Chiave master del sensore di movimento — parte della VU	$K_{M\text{-}VU}$	ERCA	Casuale	ERCA, MSCA coinvolte nel rilascio dei certificati delle VU, fabbricanti di VU, unità elettroniche di bordo (VU)
Chiave master del sensore di movimento — parte dell'officina	$K_{M\text{-}WC}$	ERCA	Casuale	ERCA, MSCA, fabbricanti di carte, carte dell'officina

▼B

Chiave	Simbolo	Generata da	Metodo di generazione	Memorizzata da
Chiave master del sensore di movimento	K_M	Non generata in modo indipendente	Calcolata come $K_M = K_{M\text{-}VU}$ XOR $K_{M\text{-}WC}$	ERCA, MSCA coinvolte nel rilascio delle chiavi dei sensori di movimento (facoltativamente) (*)
Chiave di identificazione	K_{ID}	Non generata in modo indipendente	Calcolata come $K_{ID} = K_M$ XOR CV, dove CV è specificato in CSM_106	ERCA, MSCA coinvolte nel rilascio delle chiavi dei sensori di movimento (facoltativamente) (*)
Chiave di abbinamento	K_P	Fabbricante del sensore di movimento	Casuale	Un sensore di movimento
Chiave di sessione	K_S	VU (durante l'abbinamento tra VU e sensore di movimento)	Casuale	Una VU e un sensore di movimento

(*) La memorizzazione di K_M e K_{ID} è facoltativa, poiché queste chiavi possono essere calcolate da $K_{M\text{-}VU}$, $K_{M\text{-}WC}$ e CV.

CSM_101 L'Autorità europea di certificazione primaria (ERCA) deve generare $K_{M\text{-}VU}$ e $K_{M\text{-}WC}$, che sono due chiavi AES uniche e casuali con cui è possibile calcolare la chiave master del sensore di movimento K_M come $K_{M\text{-}VU}$ XOR $K_{M\text{-}WC}$. La ERCA deve comunicare, su richiesta, K_M, $K_{M\text{-}VU}$ e $K_{M\text{-}WC}$ alle autorità di certificazione degli Stati membri.

CSM_102 La ERCA deve assegnare a ciascuna chiave master del sensore di movimento K_M un numero di versione unico, applicabile anche alle chiavi $K_{M\text{-}VU}$ e $K_{M\text{-}WC}$ di cui si compone e alla relativa chiave di identificazione K_{ID}. Quando la ERCA trasmette alle MSCA le chiavi $K_{M\text{-}VU}$ e $K_{M\text{-}WC}$ deve anche comunicare il numero di versione.

Nota: il numero di versione è usato per distinguere le diverse generazioni di tali chiavi, come spiegato in dettaglio nella sezione 9.2.1.2.

CSM_103 Un'autorità di certificazione dello Stato membro (MSCA) deve trasmettere la $K_{M\text{-}VU}$, insieme al numero di versione, ai fabbricanti di VU che ne facciano richiesta. I fabbricanti di VU devono inserire la chiave $K_{M\text{-}VU}$ e il relativo numero di versione in tutte le VU fabbricate.

CSM_104 Un'autorità di certificazione dello Stato membro (MSCA) deve garantire che la chiave $K_{M\text{-}WC}$ e il rispettivo numero di versione siano inseriti in ogni carta dell'officina rilasciata sotto la sua responsabilità.

Note:

— cfr. la descrizione del tipo di dati `SensorInstallationSecData` nell'appendice 2.

— Come spiegato nella sezione 9.2.1.2, più generazioni di $K_{M\text{-}WC}$ possono in realtà essere inserite in un'unica carta dell'officina.

▼B

CSM_105 Oltre alle chiavi AES specificate in CSM_104, una MSCA deve garantire che la chiave in TDES Km_{WC}, specificata nel requisito CSM_ 037 nella parte A della presente appendice, sia inserita in ogni carta dell'officina rilasciata sotto la propria responsabilità.

Note:

— ciò consente di usare una carta dell'officina di seconda generazione per l'accoppiamento con una VU di prima generazione.

— Una carta dell'officina di seconda generazione conterrà due distinte applicazioni, una conforme alla parte B della presente appendice e l'altra conforme alla parte A. Quest'ultima conterrà la chiave in TDES Km_{WC}.

CSM_106 Una MSCA che partecipa al rilascio dei sensori di movimento deve calcolare la chiave di identificazione mediante una operazione XOR tra la chiave master del sensore di movimento e un vettore costante CV. Il valore di CV deve essere il seguente:

— Per le chiavi master dei sensori di movimento a 128 bit: CV = ‘B6 44 2C 45 0E F8 D3 62 0B 7A 8A 97 91 E4 5E 83’

— Per le chiavi master dei sensori di movimento a 192 bit: CV = ‘72 AD EA FA 00 BB F4 EE F4 99 15 70 5B 7E EE BB 1C 54 ED 46 8B 0E F8 25’

— Per le chiavi master dei sensori di movimento a 256 bit: CV = ‘1D 74 DB F0 34 C7 37 2F 65 55 DE D5 DC D1 9A C3 23 D6 A6 25 64 CD BE 2D 42 0D 85 D2 32 63 AD 60’

Nota: i vettori costanti sono stati generati come segue:

Pi_10 = primi 10 byte della parte decimale della costante matematica π = ‘24 3F 6A 88 85 A3 08 D3 13 19’

CV_128-bits = primi 16 byte di SHA-256(Pi_10)

CV_192-bits = primi 24 byte di SHA-384(Pi_10)

CV_256-bits = primi 32 byte di SHA-512(Pi_10)

CSM_107 I fabbricanti di sensori di movimento devono generare una chiave di abbinamento K_P unica e casuale per ciascun sensore di movimento e devono inviare ciascuna chiave di accoppiamento a un'autorità di certificazione dello Stato membro (MSCA). La MSCA deve criptare separatamente ciascuna chiave di abbinamento con la chiave master del sensore di movimento K_M e deve restituire la chiave criptata al fabbricante del sensore di movimento. Per ciascuna chiave criptata, la MSCA deve comunicare al fabbricante del sensore di movimento il numero di versione della K_M associata.

Nota: come spiegato nella sezione 9.2.1.2, un fabbricante di sensori di movimento può in realtà dover generare molteplici chiavi di abbinamento uniche per un singolo sensore di movimento.

▼B

CSM_108 I fabbricanti di sensori di movimento devono generare un numero di serie unico per ciascun sensore di movimento e devono inviare tutti i numeri di serie a un'autorità di certificazione dello Stato membro (MSCA). La MSCA deve criptare separatamente ciascun numero di serie con la chiave di identificazione del sensore di movimento K_{ID} e deve restituire il numero di serie criptato al fabbricante del sensore di movimento. Per ciascun numero di serie criptato, la MSCA deve comunicare al fabbricante del sensore di movimento il numero di versione della K_{ID} associata.

CSM_109 Per i requisiti CSM_107 e CSM_108, la MSCA deve usare l'algoritmo AES nella modalità di funzionamento a blocchi incatenati (Chipher Block Chaining), come definito nella norma [ISO 10116], con un parametro di interleave (interleave parameter) $m = 1$ e un vettore di inizializzazione SV = '00' {16}, cioè sedici byte con valore binario 0. Quando necessario, la MSCA deve usare il metodo di riempimento 2 definito nella norma [ISO 9797-1].

CSM_110 Il fabbricante del sensore di movimento deve memorizzare nel sensore di movimento la chiave di abbinamento criptata e il numero di serie criptato, insieme ai corrispondenti valori in formato di testo in chiaro (plain text) e al numero di versione di K_M e K_{ID} usati per la cifratura.

Nota: come spiegato nella sezione 9.2.1.2, un fabbricante di sensori di movimento può in realtà dover inserire molteplici chiavi di abbinamento criptate e molteplici numeri di serie criptati in un singolo sensore di movimento.

CSM_111 Oltre al materiale crittografico basato su AES specificato in CSM_110, un fabbricante di sensori di movimento può inoltre memorizzare in ciascun sensore di movimento il materiale crittografico basato su TDES specificato nel requisito CSM_037 nella parte A della presente appendice.

Nota: ciò consentirà l'accoppiamento di un sensore di movimento di seconda generazione con una VU di prima generazione.

CSM_112 La lunghezza della chiave di sessione K_S generata da una VU durante l'abbinamento a un sensore di movimento deve essere collegata alla lunghezza della sua chiave $K_{M\text{-}VU}$, come descritto in CSM_50.

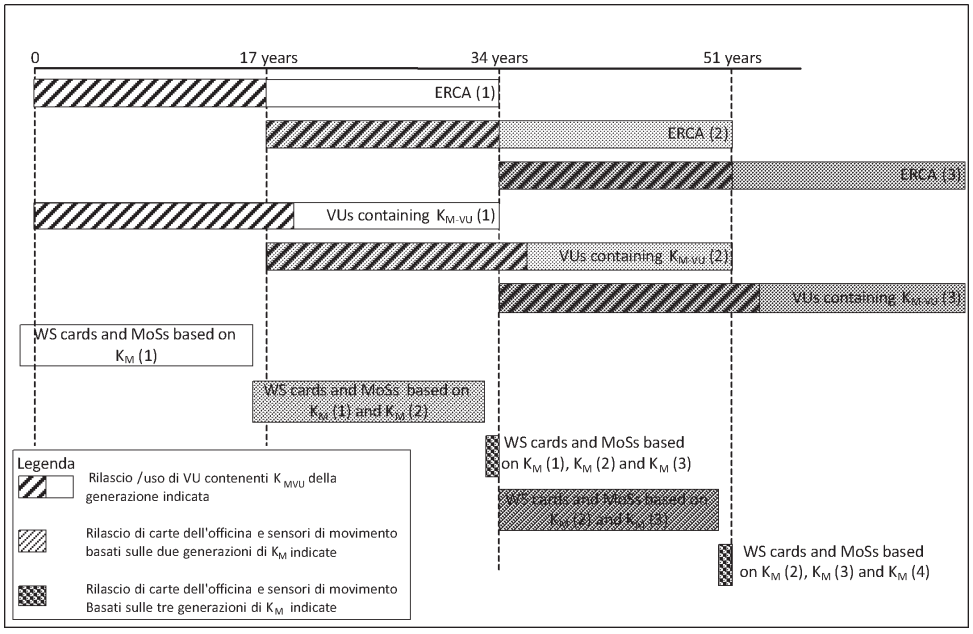
9.2.1.2 *Sostituzione della chiave master del sensore di movimento in apparecchi di seconda generazione*

CSM_113 Ciascuna chiave master del sensore di movimento e tutte le relative chiavi (cfr. Tabella 3) sono associate a una particolare generazione della coppia di chiavi radice ERCA. Tali chiavi devono pertanto essere sostituite ogni 17 anni. Il periodo di validità di ciascuna generazione di chiavi master del sensore di movimento deve iniziare un anno prima che la coppia di chiavi radice ERCA associata diventi valida e terminare alla scadenza della coppia di chiavi radice ERCA associata, come illustrato nella Figura 2.

▼B

Figura 2

Rilascio e uso di diverse generazioni della chiave master del sensore di movimento nelle VU, nei sensori di movimento e nelle carte dell'officina



CSM_114 Almeno un anno prima della generazione di una nuova coppia di chiavi radice europee, come descritto in CSM_56, la ERCA deve generare una nuova chiave master del sensore di movimento, generando una nuova chiave K_{M-VU} e una nuova chiave K_{M-WC}. La lunghezza della chiave master del sensore di movimento deve essere collegata alla forza prevista della nuova coppia di chiavi radice europee, conformemente a CSM_50. La ERCA deve comunicare le nuove chiavi K_M, K_{M-VU} e K_{M-WC} alle MSCA che ne facciano richiesta, insieme al rispettivo numero di versione.

CSM_115 Una MSCA deve garantire che tutte le generazioni valide di K_{M-WC} siano memorizzate in ogni carta dell'officina rilasciata sotto la sua autorità, insieme ai rispettivi numeri di versione, come illustrato in Figura 2.

Nota: ciò implica che nell'ultimo anno del periodo di validità di un certificato ERCA le carte dell'officina saranno rilasciate con tre diverse generazioni di K_{M-WC}, come illustrato in Figura 2.

CSM_116 Relativamente alla procedura descritta in CSM_107 e CSM_108: la MSCA deve criptare separatamente ciascuna chiave di abbinamento K_P che riceve dal fabbricante del sensore di movimento con ogni generazione valida della chiave master del sensore di movimento K_M. la MSCA deve inoltre criptare separatamente ciascun numero di serie che riceve dal fabbricante del sensore di movimento con ogni generazione valida della chiave di identificazione K_{ID}. Il fabbricante del sensore di movimento deve memorizzare nel sensore di movimento tutte le cifrature della chiave di abbinamento e del numero di serie, insieme ai corrispondenti valori in formato di testo semplice e ai numeri di versione di K_M e K_{ID} usati per la cifratura.

▼B

Nota: ciò implica che nell'ultimo anno del periodo di validità di un certificato ERCA i sensori di movimento saranno rilasciati con dati criptati in base a tre diverse generazioni di K_M, come illustrato in Figura 2.

CSM_117 Relativamente alla procedura descritta in CSM_107: poiché la lunghezza della chiave di abbinamento K_P deve essere collegata alla lunghezza di K_M (cfr. CSM_100), un fabbricante di sensori di movimento può dover generare fino a tre diverse chiavi di abbinamento (di lunghezze diverse) per un sensore di movimento, nel caso le successive generazioni K_M abbiano lunghezze diverse. In tal caso, il fabbricante deve inviare ciascuna chiave di abbinamento alla MSCA. Le MSCA deve garantire che ciascuna chiave di abbinamento sia criptata con la generazione corretta della chiave master del sensore di movimento, ossia quella avente la stessa lunghezza.

Nota: nel caso in cui scelga di generare una chiave di abbinamento basata su TDES per un sensore di movimento di seconda generazione (cfr. CSM_111), il fabbricante di sensori di movimento deve indicare alla MSCA che la chiave master del sensore di movimento basata su TDES deve essere usata per criptare questa chiave di accoppiamento. Ciò è dovuto al fatto che la lunghezza della chiave in TDES può essere pari a quella di una chiave AES, per cui la MSCA non può giudicare a partire dalla sola lunghezza della chiave.

CSM_118 I fabbricanti di VU devono inserire solo una generazione di $K_{M\text{-}VU}$ in ciascuna VU, insieme al suo numero di versione. La generazione della $K_{M\text{-}VU}$ deve essere correlata al certificato ERCA su cui si basano i certificati della VU.

Note:

— una VU basata sulla generazione *X* del certificato ERCA deve contenere solo la generazione *X* della chiave $K_{M\text{-}VU}$, anche se è stata rilasciata dopo l'inizio del periodo di validità della generazione *X+1* del certificato ERCA. Ciò è illustrato nella Figura 2.

— Una generazione di VU *X* non può essere abbinata a un sensore di movimento di generazione *X-1*.

— Poiché le carte dell'officina hanno un periodo di validità di un anno, il risultato di CSM_113 — CSM_118 sarà che tutte le carte di officina conterranno la nuova chiave $K_{M\text{-}WC}$ al momento del rilascio della prima VU contenente la nuova chiave $K_{M\text{-}VU}$. Tale VU sarà quindi sempre in grado di calcolare la nuova chiave K_M. In quel momento inoltre la maggior parte dei nuovi sensori di movimento conterrà dati criptati basati anche sulla nuova chiave K_M.

9.2.2 *Chiavi per la sicurezza della comunicazione DSRC*

9.2.2.1 *Principi generali*

CSM_119 L'autenticità e la riservatezza dei dati comunicati da una VU a un'autorità di controllo su un canale di comunicazione remota DSRC devono essere garantite mediante un insieme di chiavi AES specifiche della VU derivate da una singola chiave master DSRC, KM_{DSRC}.

▼B

CSM_120 La chiave master DSRC KM_{DSRC} deve essere una chiave AES generata, memorizzata e distribuita in modo sicuro dalla ERCA. La lunghezza della chiave può essere di 128, 192 o 256 bit e deve essere legata alla lunghezza della coppia di chiavi radice europee, come descritto in CSM_50.

CSM_121 La ERCA deve comunicare in modo sicuro la chiave master DSRC alle autorità di certificazione degli Stati membri (MSCA) che ne facciano richiesta, per consentire loro di calcolare le chiavi DSRC specifiche della VU e di garantire che la chiave master DSRC sia inserita in tutte le carte di controllo e le carte dell'officina rilasciate sotto la loro responsabilità.

CSM_122 La ERCA deve assegnare a ciascuna chiave master DSRC un numero di versione unico. Quando la ERCA trasmette alle MSCA le chiavi master DSRC deve anche comunicare loro il numero di versione.

Nota: il numero di versione è usato per distinguere le diverse generazioni di chiavi master DSRC, come spiegato in dettaglio nella sezione 9.2.2.2.

CSM_123 Per ciascuna VU, il fabbricante di VU deve generare un numero di serie unico della VU e deve inviare tale numero alla rispettiva MSCA in una richiesta volta ad ottenere un insieme di due chiavi DSRC specifiche della VU. Il numero di serie della VU deve essere di tipo di dati `VuSerialNumber` e per la codifica devono essere usate le regole di codifica distinte (DER) conformemente allo standard [ISO 8825-1].

CSM_124 Dopo aver ricevuto una richiesta di chiavi DSRC specifiche della VU, la MSCA deve calcolare due chiavi AES per la VU, denominate K_VU_{DSRC}_ENC e K_VU_{DSRC}_MAC. Tali chiavi specifiche della VU devono avere la stessa lunghezza della chiave master DSRC. La MSCA deve usare la funzione di derivazione della chiave definita in [RFC 5869]. La funzione di hash necessaria per istanziare la funzione HMAC-Hash deve essere collegata alla lunghezza della chiave master DSRC, come descritto in CSM_50. La funzione di derivazione della chiave in [RFC 5869] deve essere usata come segue:

Fase 1 (estrazione):

— *PRK* = HMAC-Hash (*salt, IKM*) dove *salt* è una stringa vuota ‘’ e *IKM* è KM_{DSRC}.

Fase 2 (espansione):

— *OKM* = *T(1)*, dove

T(1) = HMAC-Hash (*PRK*, *T(0)* || *info* || “01”) con

▼B

— *T(0)* = una stringa vuota (‘ ’)

— *info* = numero di serie della VU come specificato in CSM_123

— K_VU_{DSRC}_ENC = primi *L* ottetti di *OKM* e

K_VU_{DSRC}_MAC = ultimi *L* ottetti di *OKM*

dove *L* è la lunghezza richiesta di K_VU_{DSRC}_ENC e K_VU_{DSRC}_MAC in ottetti.

CSM_125 La MSCA deve distribuire K_VU_{DSRC}_ENC e K_VU_{DSRC}_MAC in modo sicuro al fabbricante della VU perché le inserisca nella VU cui sono destinate.

CSM_126 Al momento del rilascio una VU deve contenere nella memoria sicura le chiavi K_VU_{DSRC}_ENC e K_VU_{DSRC}_MAC, in modo da poter garantire l'integrità, l'autenticità e la riservatezza dei dati trasmessi attraverso il canale di comunicazione remota. Una VU deve inoltre avere in memoria il numero della versione della chiave master DSRC usata per calcolare tali chiavi specifiche della VU.

CSM_127 Al momento del rilascio, le carte di controllo e le carte dell'officina devono contenere KM_{DSRC} nella loro memoria sicura, in modo da essere in grado di verificare l'integrità e l'autenticità dei dati trasmessi da una VU sul canale di comunicazione remota e di decriptare tali dati. Le carte di controllo e le carte dell'officina deve inoltre avere in memoria il numero di versione della chiave master DSRC.

Nota: come spiegato nella sezione 9.2.2.2, più generazioni di K_{DSRC} possono in realtà essere inserite in un'unica carta dell'officina o carta di controllo.

CSM_128 La MSCA deve registrare tutte le chiavi DSRC specifiche della VU che ha generato, il loro numero di versione e l'identificazione della VU cui è destinata ciascuna serie di chiavi.

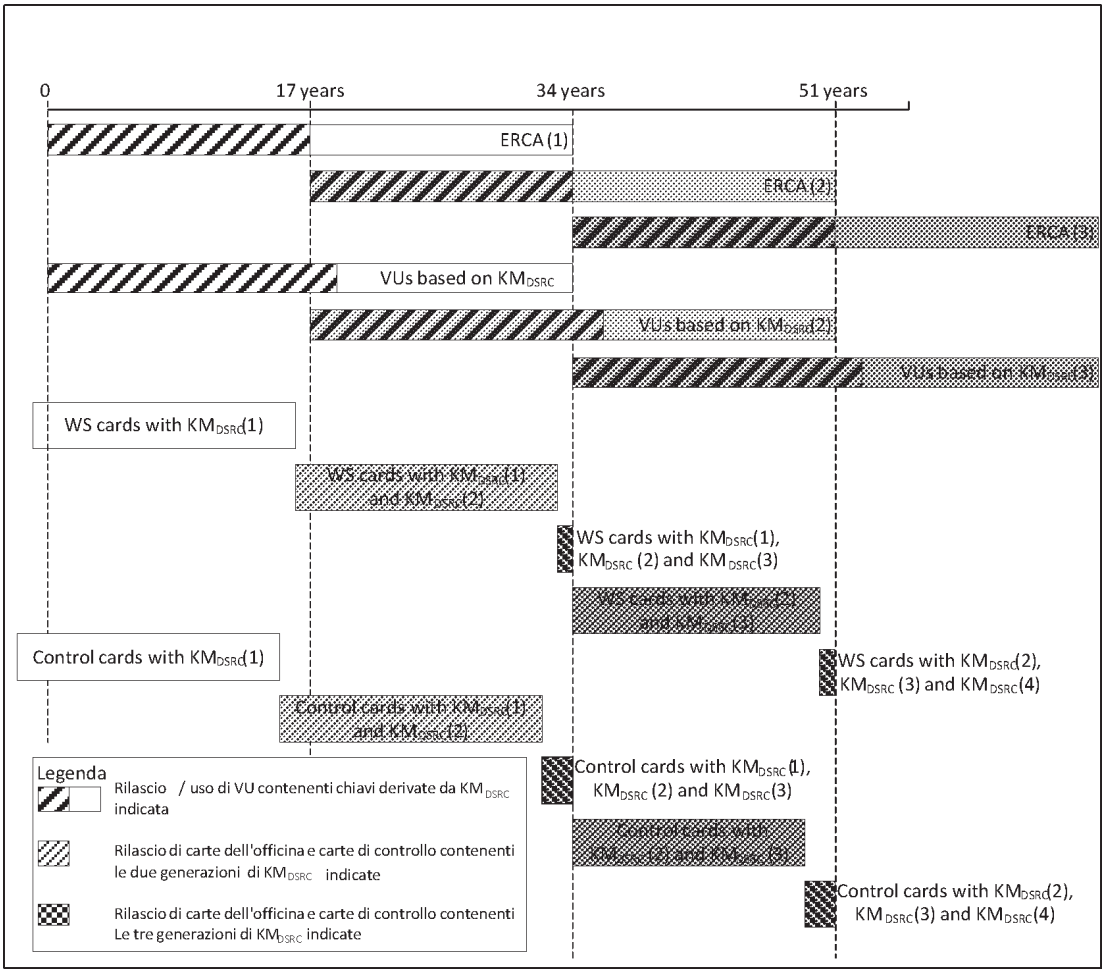
9.2.2.2 *Sostituzione della chiave master DSRC*

CSM_129 Ciascuna chiave master DSRC è associata a una particolare generazione della coppia di chiavi radice ERCA. La ERCA deve quindi sostituire la chiave master DSRC ogni 17 anni. Il periodo di validità di ciascuna generazione di chiavi master DSRC deve iniziare due anni prima che la coppia di chiavi radice ERCA associata diventi valida e terminare alla scadenza della coppia di chiavi radice ERCA associata, come illustrato nella Figura 3.

▼B

Figura 3

Rilascio e uso di diverse generazioni della chiave master DSRC nelle VU, nelle carte dell'officina e nelle carte di controllo



CSM_130 Almeno due anni prima della generazione di una nuova coppia di chiavi radice europee, come descritto in CSM_56, la ERCA deve generare una nuova chiave master DSRC. La lunghezza della chiave master DSRC deve essere collegata alla forza prevista della nuova coppia di chiavi radice europee, conformemente a CSM_50. La ERCA deve comunicare la nuova chiave master DSRC alle MSCA che ne facciano richiesta, insieme al rispettivo numero di versione.

CSM_131 La MSCA deve garantire che tutte le generazioni valide di KM_{DSRC} siano memorizzate in ogni carta di controllo rilasciata sotto la sua autorità, insieme ai rispettivi numeri di versione, come illustrato in Figura 3.

Nota: ciò implica che degli ultimi due anni del periodo di validità di un certificato ERCA le carte di controllo saranno rilasciate con tre diverse generazioni di KM_{DSRC}, come illustrato in Figura 3.

CSM_132 La MSCA deve garantire che tutte le generazioni di KM_{DSRC} che sono state valide per almeno un anno e sono ancora valide, siano memorizzate in ogni carta di controllo rilasciata sotto la sua autorità, insieme ai rispettivi numeri di versione, come illustrato in Figura 3.

▼B

Nota: ciò implica che nell'ultimo anno del periodo di validità di un certificato ERCA le carte dell'officina saranno rilasciate con tre diverse generazioni di K_{DSRC}, come illustrato in Figura 3.

CSM_133 I fabbricanti di VU devono inserire solo una serie di chiavi DSRC specifiche della VU in ciascuna VU, insieme al suo numero di versione. Questa serie di chiavi deve essere calcolata dalla generazione di KM_{DSRC} collegata al certificato ERCA su cui si basano i certificati della VU.

Note:

— ciò implica che una VU basata sulla generazione *X* del certificato ERCA deve contenere solo la generazione *X* K_VU_{DSRC}_ENC e K_VU_{DSRC}_MAC, anche se la VU è stata rilasciata dopo l'inizio del periodo di validità della generazione *X + 1* del certificato ERCA. Ciò è illustrato in Figura 3.

— Poiché le carte dell'officina hanno una validità di un anno e le carte di controllo di due anni, il risultato di CSM_131 — CSM_133 sarà che tutte le carte dell'officina e le carte di controllo conterranno la nuova chiave master DSRC al momento del rilascio della prima VU contenente le chiavi specifiche della VU basata su tale chiave master.

9.3. **Certificati**

9.3.1 *Principi generali*

CSM_134 Tutti i certificati nell'ambito del sistema tachigrafico intelligente europeo devono essere verificabili mediante carta (card verifiable — CV) e autodescrittivi (self-descriptive), conformemente alle norme [ISO 7816-4] e [ISO 7816-8].

CSM_135 Le regole di codifica distinte (DER) conformemente alla norma [ISO 8825-1] devono essere usate sia per la codifica delle strutture di dati ASN.1 che degli oggetti di dati (specifici dell'applicazione) all'interno dei certificati.

Nota: questa codifica genera una struttura Tag-Lunghezza-Valore (TLV) come segue:

Tag: il tag è codificato in uno o due ottetti e indica il contenuto.

Lunghezza: la lunghezza è codificata come un numero intero senza segno in uno, due o tre ottetti, fino a una lunghezza massima di 65 535 ottetti. Deve essere usato il numero minimo di ottetti.

Valore: il valore è codificato come zero o più ottetti.

9.3.2 *Contenuto del certificato*

CSM_136 Tutti i certificati devono avere la struttura indicata nel profilo del certificato nella Tabella 4.

Tabella 4

Profilo del certificato versione 1

Campo	ID campo	Tag	Lunghezza (byte)	Tipo di dati ASN. 1 (cfr. appendice 1)
Certificato ECC	C	'7F 21'	var	
Corpo del certificato ECC	B	'7F 4E'	var	

▼B

Campo	ID campo	Tag	Lunghezza (byte)	Tipo di dati ASN. 1 (cfr. appendice 1)
Identificativo del profilo del certificato (Certificate Profile Identifier)	CPI	‘5F 29’	‘01’	`INTEGER(0..255)`
Riferimento dell'autorità di certificazione	CAR	‘42’	‘08’	`KeyIdentifier`
Autorizzazione del titolare del certificato	CHA	‘5F 4C’	‘07’	`CertificateHolder Authorisation`
Chiave pubblica	PK	‘7F 49’	var	
Parametri di dominio	DP	‘06’	var	`OBJECT IDENTIFIER`
Punto pubblico (public point)	PP	‘86’	var	`OCTET STRING`
Riferimento del titolare del certificato	CHR	‘5F 20’	‘08’	`KeyIdentifier`
Data di efficacia del certificato	CEfD	‘5F 25’	‘04’	`TimeReal`
Data di scadenza del certificato	CExD	‘5F 24’	‘04’	`TimeReal`
Firma del certificato ECC	S	‘5F 37’	var	`OCTET STRING`

Nota: ID campo sarà usato in sezioni successive della presente appendice per indicare i singoli campi di un certificato, ad esempio X.CAR è il riferimento all'autorità di certificazione (Certificate Authority Reference — CAR) citata nel certificato dell'utente X.

9.3.2.1 Identificativo del profilo del certificato (Certificate Profile Identifier)

CSM_137 I certificati devono usare un identificativo del profilo del certificato (Certificate Profile Identifier) per indicare il profilo del certificato usato. Come specificato nella Tabella 4, la versione 1 deve essere indicata col valore “00”.

9.3.2.2 Riferimento dell'autorità di certificazione

CSM_138 Il riferimento dell'autorità di certificazione deve essere usato per identificare la chiave pubblica da usare per la verifica della firma del certificato. Il riferimento dell'autorità di certificazione deve quindi essere uguale al riferimento del titolare del certificato (Certificate Holder Reference — CHR) nel certificato della corrispondente autorità di certificazione.

CSM_139 Un certificato radice ERCA deve essere autofirmato, vale a dire che nel certificato il riferimento dell'autorità di certificazione e il riferimento del titolare del certificato devono essere uguali.

▼B

CSM_140 Per un certificato di collegamento ERCA, il riferimento del titolare del certificato deve essere uguale al CHR del nuovo certificato radice ERCA. Il riferimento dell'autorità di certificazione per un certificato di collegamento deve essere uguale al CHR del precedente certificato radice ERCA.

9.3.2.3 Autorizzazione del titolare del certificato.

CSM_141 L'autorizzazione del titolare del certificato deve essere usata per identificare il tipo di certificato. Si compone dei sei byte più significativi dell'ID dell'applicazione tachigrafica, concatenati con il tipo di apparecchio cui è destinato il certificato.

9.3.2.4 Chiave pubblica

La chiave pubblica contiene due elementi di dati: i parametri di dominio standardizzati da usare con la chiave pubblica nel certificato e il valore del punto pubblico.

CSM_142 L'elemento di dati «parametri di dominio» (Domain Parameters) deve contenere uno degli identificativi di oggetto specificati nella Tabella 1 in riferimento a un insieme di parametri di dominio standardizzati.

CSM_143 L'elemento di dati «punto pubblico» (Public Point) deve contenere il punto pubblico. I punti pubblici della curva ellittica devono essere convertiti in stringhe di ottetti, come specificato in [TR-03111]. Deve essere usato il formato di codifica non compresso. Al momento del ripristino di un punto di una curva ellittica dal formato codificato, devono essere sempre eseguite le convalide descritte in [TR-03111].

9.3.2.5 Riferimento del titolare del certificato

CSM_144 Il riferimento del titolare del certificato (Certificate Holder Reference) è un identificativo della chiave pubblica contenuta nel certificato. Deve essere usato per fare riferimento a tale chiave pubblica in altri certificati.

CSM_145 Per i certificati della carta e dei dispositivi GNSS esterni, il riferimento del titolare del certificato deve avere il tipo di dati `ExtendedSerialNumber` specificato nell'appendice 1.

CSM_146 Per le VU, il fabbricante, quando richiede un certificato, può conoscere o può non conoscere il numero di serie specifico del fabbricante della VU cui tale certificato e la chiave privata associata sono destinati. Nel primo caso, il riferimento del titolare del certificato deve avere il tipo di dati `ExtendedSerialNumber` specificato nell'appendice 1. Nel secondo caso, il riferimento del titolare del certificato deve avere il tipo di dati `CertificateRequestID` specificato nell'appendice 1.

CSM_147 Per i certificati ERCA e MSCA, il riferimento del titolare del certificato deve avere il tipo di dati `CertificationAuthorityKID` specificato nell'appendice 1.

▼B

9.3.2.6 Data di efficacia del certificato

CSM_148 La data di efficacia del certificato deve indicare la data e l'ora di inizio del periodo di validità del certificato. La data di efficacia del certificato deve essere la data della generazione del certificato.

9.3.2.7 Data di scadenza del certificato

CSM_149 La data di scadenza del certificato deve indicare la data e l'ora di fine del periodo di validità del certificato.

9.3.2.8 Firma del certificato

CSM_150 La firma sul certificato deve essere creata sul corpo del certificato codificato, compresi il tag e la lunghezza del corpo del certificato. L'algoritmo di firma deve essere ECDSA, come specificato in [DSS], usando l'algoritmo di hash collegato alle dimensioni della chiave dell'autorità che firma, come specificato in CSM_50. Il formato della firma deve essere in chiaro, come specificato in [TR-03111].

9.3.3 *Richiesta di certificati*

CSM_151 Per la richiesta di un certificato, il richiedente deve inviare i seguenti dati alla sua autorità di certificazione:

— l'identificativo del profilo del certificato richiesto;

— il riferimento dell'autorità di certificazione che si prevede di usare per la firma del certificato;

— la chiave pubblica da firmare.

CSM_152 Oltre ai dati in CSM_151, una MSCA deve inviare i seguenti dati in una richiesta di certificato alla ERCA, consentendo a quest'ultima di creare il riferimento del titolare del certificato del nuovo certificato MSCA:

— il codice numerico del paese dell'autorità di certificazione (tipo di dati `NationNumeric` definito nell'appendice 1);

— il codice alfanumerico del paese dell'autorità di certificazione (tipo di dati `NationAlpha` definito nell'appendice 1);

— il numero di serie a 1 byte usato per distinguere le diverse chiavi dell'autorità di certificazione in caso di cambio di chiavi;

— il campo a due byte contenente specifiche informazioni supplementari dell'autorità di certificazione.

CSM_153 Oltre ai dati in CSM_151, una fabbricante dell'apparecchiatura deve inviare i seguenti dati in una richiesta di certificato alla MSCA, consentendole di creare il riferimento del titolare del certificato del nuovo certificato dell'apparecchiatura:

— un identificativo del tipo di apparecchiatura specifico del fabbricante;

— se noto (cfr. CSM_154), un numero di serie per l'apparecchio, univocamente associato al fabbricante, al tipo di apparecchio e al mese di fabbricazione. In caso contrario, un identificativo unico della richiesta di certificato;

▼B

— il mese e l'anno di fabbricazione dell'apparecchio o della richiesta di certificato.

Il fabbricante deve garantire che tali dati siano corretti e che il certificato restituito dalla MSCA sia inserito nell'apparecchio cui è destinato.

CSM_154 Nel caso di una VU, il fabbricante, quando richiede un certificato, può conoscere o può non conoscere il numero di serie specifico del fabbricante della VU cui tale certificato e la chiave privata associata sono destinati. Nel primo caso, il fabbricante della VU deve inviare il numero di serie alla MSCA. Nel secondo caso, il fabbricante deve identificare univocamente ciascuna richiesta di certificato e inviare tale numero di serie della richiesta di certificato alla MSCA. Il certificato che ne risulta conterrà quindi il numero di serie della richiesta di certificato. Dopo aver inserito il certificato in una specifica VU, il fabbricante deve comunicare alla MSCA il collegamento tra il numero di serie della richiesta di certificato e l'identificazione della VU.

10. AUTENTICAZIONE RECIPROCA E MESSAGGISTICA SICURA TRA VU E CARTA

10.1. **Principi generali**

CSM_155 Ad alto livello, la comunicazione sicura tra una VU e una carta tachigrafica deve avvenire secondo le seguenti fasi:

— prima fase: ciascuna parte deve dimostrare all'altra di essere in possesso di un certificato a chiave pubblica valido, firmato da un'autorità di certificazione di uno Stato membro (MSCA). Il certificato MSCA a chiave pubblica deve essere firmato dalla ERCA. Questa fase è denominata verifica della catena di certificati (certificate chain verification) ed è specificata in dettaglio nella sezione 10.2;

— seconda fase: la VU deve dimostrare alla carta di essere in possesso della chiave privata corrispondente alla chiave pubblica nel certificato presentato, firmando un numero casuale inviato dalla carta. La carta verifica la firma per questo numero casuale e, se la verifica ha esito positivo, la VU è autenticata. Questa fase è denominata autenticazione della VU (VU Authentication) ed è specificata in dettaglio nella sezione 10.3;

— terza fase: entrambe le parti calcolano in modo indipendente due chiavi di sessione AES usando un algoritmo di accordo sulla chiave asimmetrica. Usando una di queste chiavi di sessione, la carta crea un codice di autenticazione del messaggio (MAC) per alcuni dati trasmessi dalla VU. La VU verifica il MAC. Se la verifica ha esito positivo, la carta è autenticata. Questa fase è denominata autenticazione della carta (Card Authentication) ed è specificata in dettaglio nella sezione 10.4;

— quarta fase: la VU e la carta devono usare le chiavi di sessione su cui si sono accordate per garantire la riservatezza, l'integrità e l'autenticità di tutti i messaggi scambiati. Questa fase è denominata messaggistica sicura (Secure Messaging) ed è specificata in dettaglio nella sezione 10.5.

CSM_156 Il meccanismo descritto in CSM_155 deve essere attivato dalla VU ogni volta che una carta è inserita in una delle sue sedi (slot).

▼B

10.2. **Verifica reciproca della catena di certificati**

10.2.1 *Verifica della catena di certificati della carta da parte della VU*

CSM_157 Le VU devono usare il protocollo illustrato in Figura 4 per la verifica della catena di certificati di una carta tachigrafica.

Note alla Figura 4:

— i certificati e le chiavi pubbliche della carta citati nella figura sono quelli usati per l'autenticazione reciproca. Nella sezione 9.1.5 sono indicati come Card_MA.

— I certificati e le chiavi pubbliche Card.CA citati nella figura sono quelli usati per firmare i certificati della carta e sono indicati nel CAR del certificato della carta. Nella sezione 9.1.3 sono indicati come MSCA_Card.

— Il certificato Card.CA.EUR citato nella figura è il certificato radice europeo indicato nel CAR del certificato Card.CA.

— Il certificato Card.Link indicato nella figura è il certificato di collegamento della carta, se presente. Come specificato nella sezione 9.1.2, si tratta di un certificato di collegamento per una nuova coppia di chiavi radice europee creata dalla ERCA e firmata con la precedente chiave privata europea.

— Il certificato Card.Link.EUR è il certificato radice europeo indicato nel CAR del certificato Card.Link.

CSM_158 Come illustrato nella Figura 4, la verifica della catena di certificati della carta deve iniziare al momento dell'inserimento della carta. La VU deve leggere il riferimento del titolare della carta (`cardExtendedSerialNumber`) dall'EF ICC. La VU deve verificare se conosce la carta, vale a dire, se ha già verificato in passato la catena di certificati della carta con esito positivo e ha memorizzato questi dati per riferimento futuro. In caso affermativo, e se il certificato della carta è ancora valido, la procedura continua con la verifica della catena di certificati della VU. In caso contrario la VU deve leggere dalla carta, in successione, il certificato MSCA_Card da usare per la verifica del certificato della carta, il certificato Card.CA.EUR da usare per la verifica del certificato MSCA_Card e eventualmente il certificato di collegamento, fino a che non trova un certificato che conosce o che può verificare. Se tale certificato viene trovato, la VU lo usa per verificare i certificati della carta sottostanti che ha letto dalla carta. In caso di esito positivo, la procedura continua con la verifica della catena di certificati della VU. In caso di esito negativo, la VU deve ignorare la carta.

▼B

Nota: la VU può conoscere il certificato Card.CA.EUR in tre modi:

— il certificato Card.CA.EUR è uguale al certificato EUR della VU stessa;

— il certificato Card.CA.EUR è precedente al certificato EUR della VU stessa e la VU lo conteneva già al momento del rilascio (cfr. CSM_81);

— il certificato Card.CA.EUR è successivo al certificato EUR della VU stessa e la VU ha ricevuto un certificato di collegamento in passato da un'altra carta tachigrafica, lo ha verificato e lo ha memorizzato per riferimento futuro.

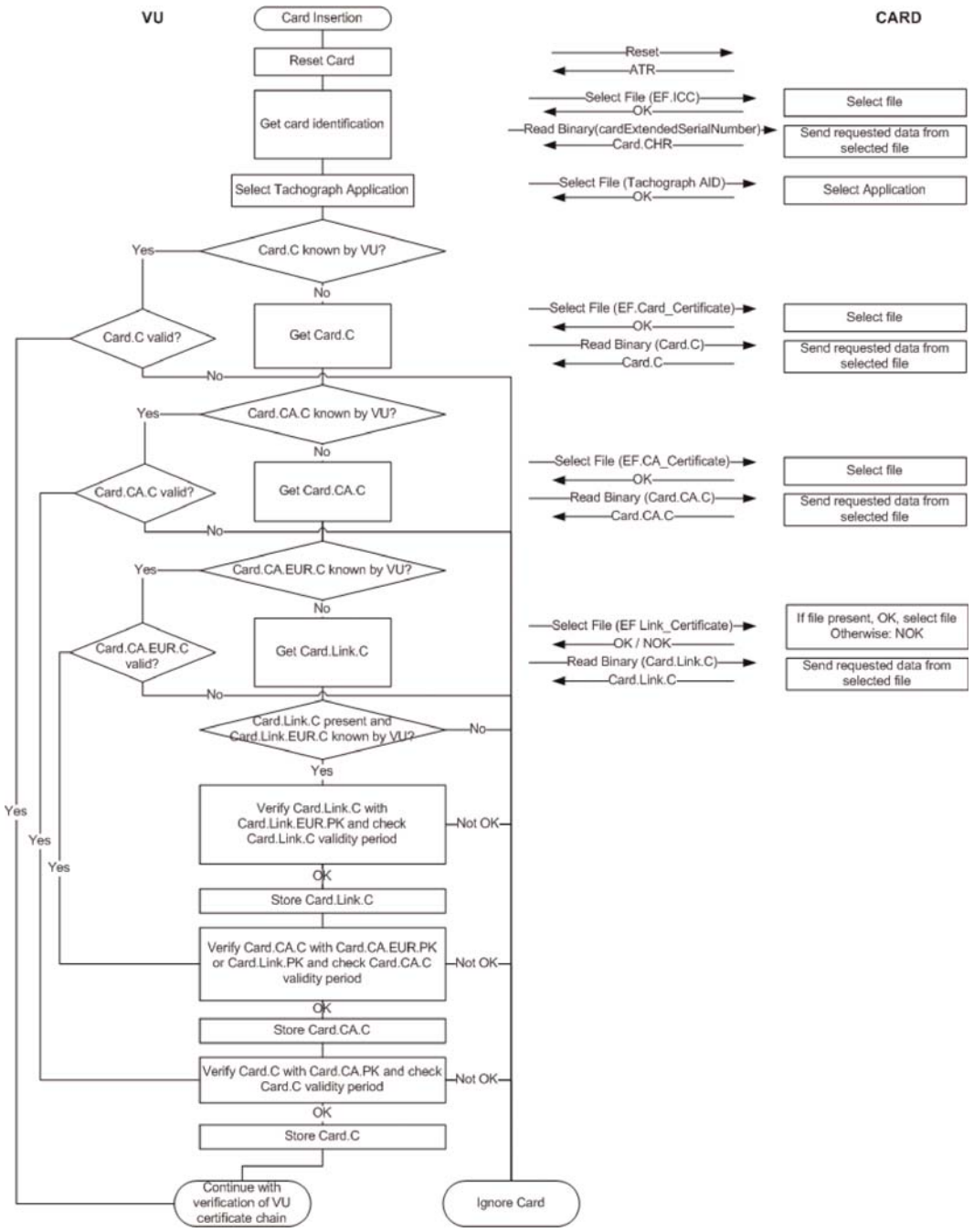
CSM_159 Come illustrato in Figura 4, una volta verificata l'autenticità e la validità di un certificato precedentemente sconosciuto, la VU può conservarlo per riferimento futuro, in modo da non doverne nuovamente verificare l'autenticità se viene nuovamente presentato alla VU. Invece di memorizzare l'intero certificato, una VU può scegliere di memorizzare solo il contenuto del corpo del certificato, come specificato nella sezione 9.3.2.

CSM_160 La VU deve verificare la validità temporale di qualsiasi certificato letto dalla carta o memorizzato nella sua memoria e respingere i certificati scaduti. Per verificare la validità temporale del certificato presentato dalla carta la VU deve usare il suo orologio interno.

▼B

Figura 4

Protocollo per la verifica della catena di certificati della carta da parte della VU



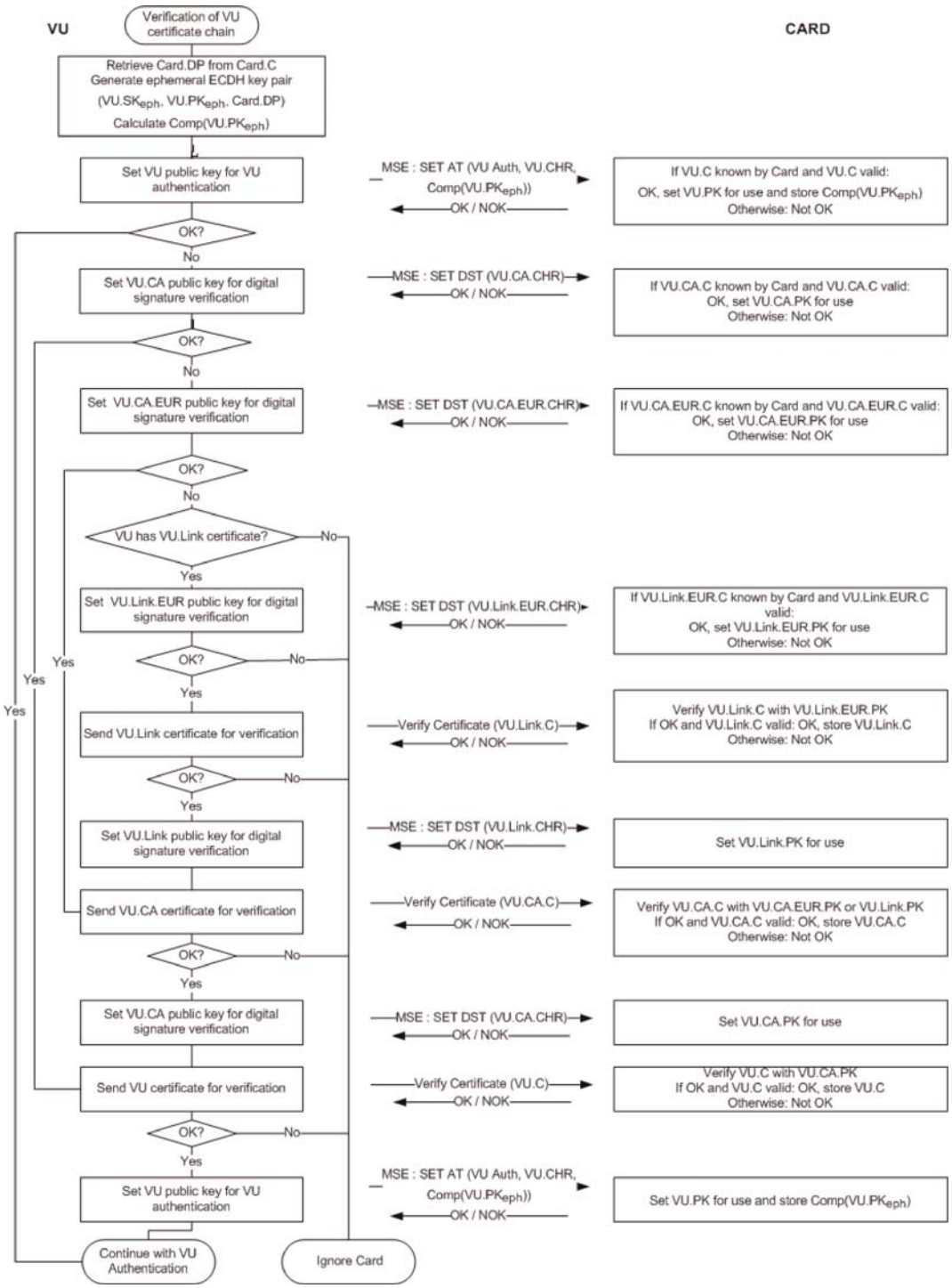
10.2.2 *Verifica della catena di certificati della VU da parte della carta*

CSM_161 Le carte tachigrafiche devono usare il protocollo illustrato nella Figura 5 per la verifica della catena di certificati di una VU.

▼B

Figura 5

Protocollo per la verifica della catena di certificati della VU da parte della carta



Note alla Figura 5:

— i certificati e le chiavi pubbliche della VU citati nella figura sono quelli usati per l'autenticazione reciproca. Nella sezione 9.1.4 sono indicati come VU_MA.

▼B

— I certificati e le chiavi pubbliche VU.CA citati nella figura sono quelli usati per firmare i certificati della VU e del dispositivo GNSS esterno. Nella sezione 9.1.3 sono indicati come MSCA_VU-EGF.

— Il certificato VU.CA.EUR citato nella figura è il certificato radice europeo indicato nel CAR del certificato VU.CA.

— Il certificato VU.Link indicato nella figura è il certificato di collegamento della VU, se presente. Come specificato nella sezione 9.1.2, si tratta di un certificato di collegamento per una nuova coppia di chiavi radice europee creata dalla ERCA e firmata con la precedente chiave privata europea.

— Il certificato VU.Link.EUR è il certificato radice europeo indicato nel CAR del certificato VU.Link.

CSM_162 Come illustrato in Figura 5, la verifica della catena di certificati della VU deve iniziare con il tentativo della VU di usare la propria chiave pubblica nella carta tachigrafica. Se questo tentativo ha esito positivo significa che in passato la carta aveva già verificato la catena di certificati della VU con esito positivo e aveva memorizzato il certificato della VU per riferimento futuro. In tal caso il certificato della VU è impostato per l'uso e la procedura continua con l'autenticazione della VU. Se il certificato della VU non è noto alla carta, la VU deve presentare, in successione, il certificato VU.CA da usare per verificare il suo certificato di VU, il certificato VU.CA.EUR da usare per verificare il certificato VU.CA e eventualmente il certificato di collegamento, in modo da trovare un certificato noto o verificabile dalla carta. Se tale certificato viene trovato, la carta deve farne uso per verificare i certificati della VU sottostanti che le sono stati presentati. In caso di esito positivo la VU deve impostare infine la sua chiave pubblica per l'uso nella carta tachigrafica. In caso di esito negativo, la VU deve ignorare la carta.

Nota: la carta può conoscere il certificato VU.CA.EUR in tre modi:

— il certificato VU.CA.EUR è uguale al certificato EUR della carta stessa;

— il certificato VU.CA.EUR è precedente al certificato EUR della carta stessa e la carta lo conteneva già al momento del rilascio (cfr. CSM_91);

— il certificato VU.CA.EUR è successivo al certificato EUR della carta stessa e la carta ha ricevuto un certificato di collegamento in passato da un'altra VU, lo ha verificato e lo ha memorizzato per riferimento futuro.

CSM_163 La VU deve usare il comando MSE: Set AT per impostare la sua chiave pubblica per l'uso nella carta tachigrafica. Come specificato nell'appendice 2, tale comando contiene un'indicazione del meccanismo di crittografia che sarà usato con la chiave impostata. Il meccanismo è «autenticazione della VU utilizzando l'algoritmo ECDSA, in combinazione con l'algoritmo di hash collegato alle dimensioni della coppia di chiavi VU_MA della VU, come specificato in CSM_50».

▼B

CSM_164 Il comando MSE: Set AT contiene inoltre un'indicazione della coppia di chiavi temporanee che la VU userà durante l'accordo sulla chiave di sessione (cfr. sezione 10.4). Pertanto prima di inviare il comando MSE: Set AT la VU deve generare una coppia di chiavi ECC temporanee. Per generare la coppia di chiavi temporanee, la VU deve usare i parametri di dominio standardizzati indicati nel certificato della carta. La coppia di chiavi temporanee è indicata come ($VU.SK_{eph}$, $VU.PK_{eph}$, Card.DP). La VU deve prendere la coordinata x del punto pubblico temporaneo ECDH come chiave di identificazione; ciò è denominato rappresentazione compressa della chiave pubblica ed indicato come $Comp(VU.PK_{eph})$.

CSM_165 Se il comando MSE: Set AT ha esito positivo, la carta deve impostare il VU.PK indicato per l'uso successivo durante l'autenticazione del veicolo e memorizzare temporaneamente il $Comp(VU.PK_{eph})$. Nel caso in cui due o più comandi MSE: Set AT siano inviati con esito positivo prima dell'accordo sulla chiave di sessione, la carta deve memorizzare solo l'ultimo $Comp(VU.PK_{eph})$ ricevuto.

CSM_166 La carta deve verificare la validità temporale di qualsiasi certificato presentato dalla VU o cui la VU si riferisce mentre è conservato nella memoria della carta e deve rifiutare i certificati scaduti.

CSM_167 Per verificare la validità temporale del certificato presentato dalla VU, ogni carta tachigrafica deve conservare in memoria dei dati che rappresentano l'ora corrente. Tali dati non devono essere direttamente aggiornabili da una VU. Al momento del rilascio, l'ora corrente di una carta deve essere impostata come uguale alla data di efficacia del certificato Card_MA della carta. Una carta deve aggiornare la sua ora corrente se la data di efficacia di un certificato «sorgente di tempo valida» autentico presentato da una VU è più recente dell'ora corrente della carta. In tal caso, la carta deve impostare la sua ora corrente come uguale alla data di efficacia di tale certificato. La carta deve accettare solo i seguenti certificati come sorgente di tempo valida:

— certificati di collegamento ERCA di seconda generazione;

— certificati MSCA di seconda generazione;

— certificati della VU di seconda generazione rilasciati dallo stesso paese del certificato o dei certificati della carta stessa.

Nota: quest'ultimo requisito implica che una carta sia in grado di riconoscere il CAR del certificato della VU, vale a dire il certificato MSCA_VU-EGF, che sarà diverso dal CAR del suo stesso certificato, che è il certificato MSCA_Card.

CSM_168 Come illustrato nella Figura 5, una volta verificata l'autenticità e la validità di un certificato precedentemente sconosciuto, la carta può conservarlo per riferimento futuro, in modo da non doverne nuovamente verificare l'autenticità se

▼B

viene nuovamente presentato alla carta. Invece di memorizzare l'intero certificato, una carta può scegliere di memorizzare solo il contenuto del corpo del certificato, come specificato nella sezione 9.3.2.

10.3. **Autenticazione della VU**

CSM_169 Le VU e le carte devono usare il protocollo di autenticazione della VU illustrato nella Figura 6 per autenticare la VU nei confonti della carta. L'autenticazione della VU consente alla carta tachigrafica di verificare esplicitamente che la VU sia autentica; quest'ultima deve usare la sua chiave privata per firmare una sfida (challenge) generata dalla carta.

CSM_170 Accanto alla sfida (challenge) della carta, la VU deve includere nella firma il riferimento al titolare della carta preso dal certificato della carta.

Nota: ciò garantisce che la carta nei confonti della quale la VU si sta autenticando sia la stessa carta di cui la VU ha precedentemente verificato la catena di certificati.

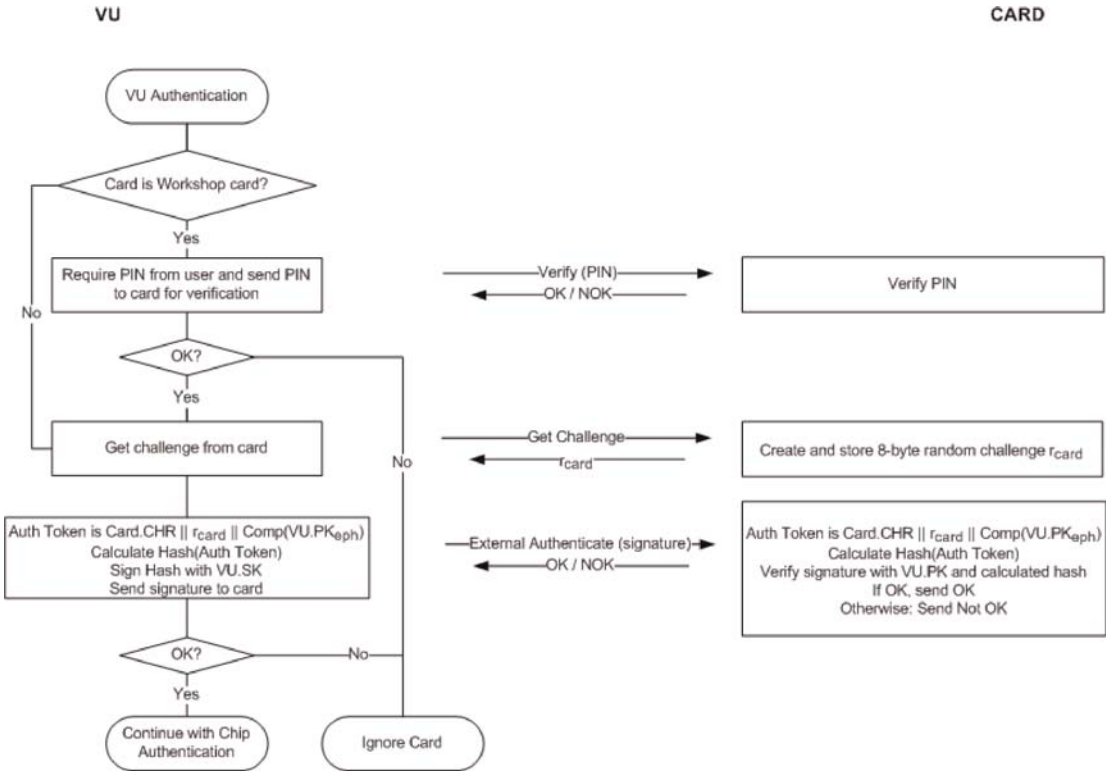
CSM_171 La VU deve inoltre includere nella firma l'identificativo della chiave pubblica temporanea Comp(VU.PK_{eph}) che la VU stessa userà per la messaggistica sicura durante la procedura di autenticazione del chip specificata nella sezione 10.4.

Nota: ciò garantisce che la VU con cui una carta comunica durante una sessione di messaggistica sicura sia la stessa VU che è stata autenticata dalla carta.

▼B

Figura 6

Protocollo di autenticazione della VU



CSM_172 Se la VU invia molteplici comandi GET CHALLENGE durante l'autenticazione, la carta deve restituire ogni volta una nuova sfida (challenge) casuale a 8 byte, ma deve memorizzare solo l'ultima sfida.

CSM_173 L'algoritmo di firma usato dalla VU per l'autenticazione della VU deve essere ECDSA, come specificato in [DSS], usando l'algoritmo di hash collegato alle dimensioni della coppia di chiavi VU_MA della VU, come specificato in CSM_50. Il formato della firma deve essere in chiaro, come specificato in [TR-03111]. La VU deve inviare alla carta la firma che ne risulta.

CSM_174 Al ricevimento della firma della VU in un comando EXTERNAL AUTHENTICATE, la carta deve:

— calcolare il token di autenticazione concatenando Card.CHR, la sfida (challenge) della carta r_{card} e l'identificativo della chiave pubblica temporanea della VU Comp($VU.PK_{eph}$),

— calcolare l'hash sul token di autenticazione usando l'algoritmo di hash collegato alle dimensioni della coppia di chiavi VU_MA della VU, come specificato in CSM_50,

— verificare la firma della VU usando l'algoritmo ECDSA in combinazione con VU.PK e l'hash calcolato.

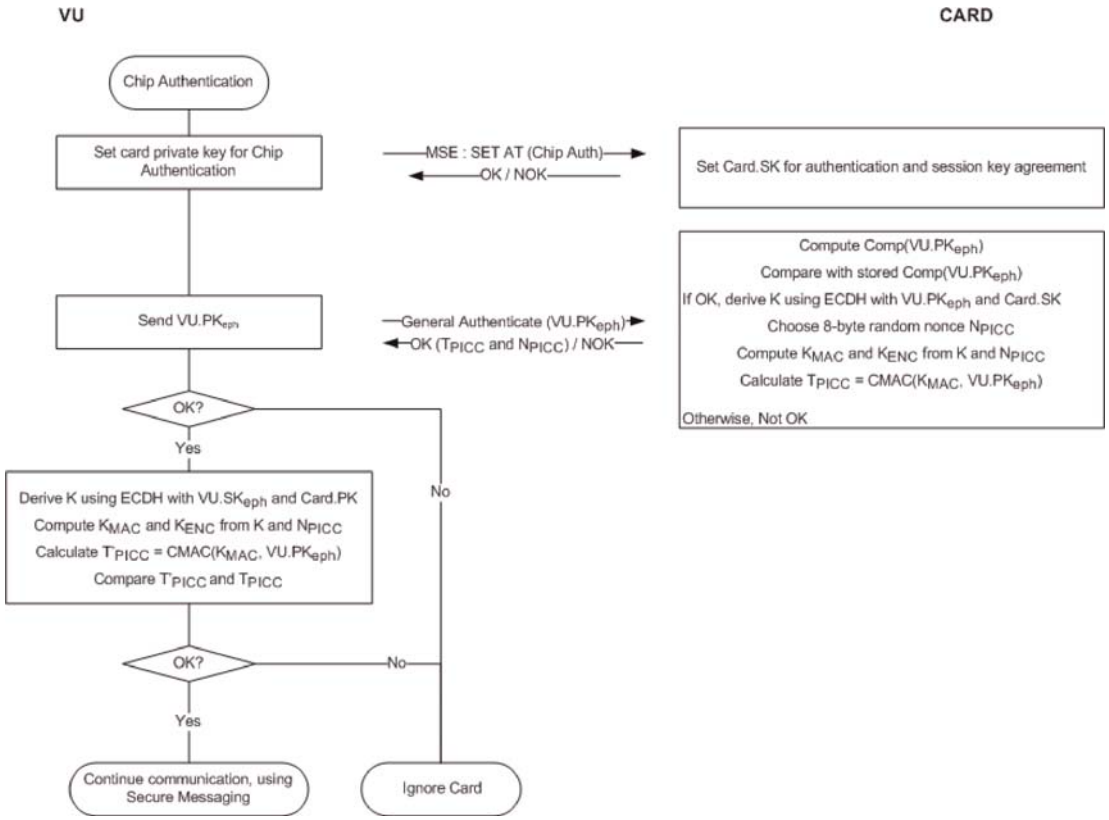
▼B

10.4. **Autenticazione del chip e accordo sulla chiave di sessione**

CSM_175 Le VU e le carte devono usare il protocollo di autenticazione del chip illustrato nella **Figura 7** per autenticare la carta verso la VU. L'autenticazione del chip consente alla VU di verificare esplicitamente che la carta sia autentica.

Figura 7

Autenticazione del chip e accordo sulla chiave di sessione



CSM_176 La VU e la carta devono eseguire la seguente procedura:

1. la VU avvia la procedura di autenticazione del chip inviando il comando MSE: Set AT con l'indicazione «Autenticazione del chip usando l'algoritmo ECDH che dà come risultato una lunghezza della chiave di sessione AES collegata alle dimensioni della coppia di chiavi Card_MA della carta, come specificato in CSM_50». La VU deve determinare le dimensioni della chiave della coppia di chiavi della carta dal certificato della stessa.

2. La VU invia alla carta il punto pubblico $VU.PK_{eph}$ della sua coppia di chiavi temporanee. Come spiegato in CSM_164, la VU ha generato questa coppia di chiavi temporanee prima della verifica della catena di certificati della VU. La VU ha inviato alla carta l'identificativo della chiave pubblica temporanea $Comp(VU.PK_{eph})$ e la carta lo ha memorizzato.

▼B

3. La carta calcola Comp(VU.PK_{eph}) da VU.PK_{eph} e lo confronta con il valore memorizzato di Comp(VU.PK_{eph}).

4. Usando l'algoritmo ECDH in combinazione con la chiave privata statica della carta e la chiave pubblica temporanea della VU, la carta calcola una chiave segreta K.

5. La carta sceglie un nonce casuale a 8 byte N_{PICC} e lo usa per calcolare due chiavi di sessione AES K_{MAC} e K_{ENC} da K. Cfr. CSM_179.

6. Usando K_{MAC}, la carta calcola un token di autenticazione sull'identificativo della chiave pubblica temporanea della VU: T_{PICC} = CMAC(K_{MAC}, VU.PK_{eph}). La Carta invia N_{PICC} e T_{PICC} alla VU.

7. Usando l'algoritmo ECDH in combinazione con la chiave pubblica statica della carta e la chiave privata temporanea della VU, la VU calcola la stessa chiave segreta K calcolata dalla carta nella fase 4.

8. La VU calcola le chiavi di sessione K_{MAC} e K_{ENC} da K e N_{PICC}; cfr. CSM_179.

9. La VU verifica il token di autenticazione T_{PICC}.

CSM_177 Nella precedente fase 3, la carta deve calcolare Comp(VU.PKeph) come la coordinata x del punto pubblico in VU.PKeph.

CSM_178 Nelle precedenti fasi 4 e 7, la carta e la VU devono usare l'algoritmo ECKA-EG come definito in [TR- 03111].

CSM_179 Nelle precedenti fasi 5 e 8, la carta e la VU devono usare la funzione di derivazione della chiave per le chiavi di sessione AES definita in [TR- 03111], tenendo conto delle seguenti precisazioni e modifiche:

— il valore del contatore deve essere ‘00 00 00 01’ per K_{ENC} e ‘00 00 00 02’ per K_{MAC};

— il nonce facoltativo *r* deve essere usato e deve essere uguale a N_{PICC};

— per il calcolo delle chiavi AES a 128 bit, l'algoritmo di hash da usare è SHA-256;

— per il calcolo delle chiavi AES a 192 bit, l'algoritmo di hash da usare è SHA-384;

— per il calcolo delle chiavi AES a 256 bit, l'algoritmo di hash da usare è SHA-512.

La lunghezza delle chiavi di sessione (vale a dire la lunghezza in corrispondenza della quale viene troncato l'hash) deve essere collegata alle dimensioni della coppia di chiavi Card_MA, come specificato in CSM_50.

▼B

CSM_180 Nelle precedenti fasi 6 e 9, la carta e la VU devono usare l'algoritmo AES in modalità CMAC, come definito in [SP 800-38B]. La lunghezza di T_{PICC} deve essere collegata alla lunghezza delle chiavi di sessione AES, come specificato in CSM_50.

10.5. **Messaggistica sicura (Secure Messaging)**

10.5.1 *Principi generali*

CSM_181 Tutti i comandi e le risposte scambiate tra una VU e una carta tachigrafica, dopo un'autenticazione del chip con esito positivo e fino alla fine della sessione, devono essere protette mediante messaggistica sicura.

CSM_182 La messaggistica sicura deve essere usata in modalità di sola autenticazione, ad eccezione della lettura da un file con condizioni di accesso SM-R-ENC-MAC-G2 (cfr. appendice 2, sezione 4). Nella modalità di sola autenticazione, un totale di controllo crittografico (alias MAC) è aggiunto a tutti i comandi e a tutte le risposte per garantire l'autenticità e l'integrità del messaggio.

CSM_183 Per la lettura di dati da un file con condizioni di accesso SM-R-ENC-MAC-G2, la messaggistica sicura deve essere usata in modalità cifratura seguita da autenticazione (encrypt-then-authenticate), vale a dire i dati della risposta sono in primo luogo criptati per garantire la riservatezza del messaggio e successivamente viene calcolato un MAC sui dati criptati formattati per garantirne l'autenticità e l'integrità.

CSM_184 La messaggistica sicura deve utilizzare AES come definito in [AES] con le chiavi di sessione K_{MAC} e K_{ENC} concordate durante l'autenticazione del chip.

CSM_185 Un numero intero senza segno deve essere usato come contatore sequenza di invio (SSC) per prevenire gli attacchi di tipo *replay attack*. Le dimensioni dell'SSC devono essere uguali alle dimensioni dei blocchi AES, vale a dire 128 bit. L'SSC deve essere in formato MSB-first. Il contatore sequenza di invio deve essere inizializzato a zero (vale a dire '00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00') all'inizio della messaggistica sicura. L'SSC deve essere aumentato ogni volta prima che sia generato un comando o una risposta APDU, vale a dire: poiché il valore di partenza dell'SSC in una sessione SM è 0, nel primo comando il valore dell'SSC sarà 1. Il valore dell'SSC per la prima risposta sarà 2.

CSM_186 Per criptare i messaggi, deve essere usata la chiave K_{ENC} con AES nella modalità di funzionamento a blocchi incatenati (CBC), come definito in [ISO 10116], con un parametro di interleave (interleave parameter) $m = 1$ e un vettore di inizializzazione $SV = E(K_{ENC}, SSC)$, vale a dire il valore corrente dell'SSC criptato con K_{ENC}.

CSM_187 Per l'autenticazione del messaggio, K_{MAC} deve essere usato con AES in modalità CMAC come specificato in [SP 800-38B]. La lunghezza del MAC deve essere collegata alla lunghezza delle chiavi di sessione AES, come specificato in CSM_50. Il contatore sequenza di invio deve essere incluso nel MAC, aggiungendolo prima del datagramma da autenticare.

▼B

10.5.2 *Struttura dei messaggi sicuri*

CSM_188 La messaggistica sicura deve avvalersi solo di oggetti di dati in messaggistica sicura (cfr. [ISO 7816-4]) elencati in Tabella 5. In tutti i messaggi tali oggetti di dati devono essere usati nell'ordine indicato nella seguente tabella.

Tabella 5

Oggetti di dati in messaggistica sicura

Nome dell'oggetto di dati (Data Object Name)	Tag	Presenza (O)bbligatoria, (C)ondizionata o (V)ietata in	
		Comandi	Risposte
Valore in chiaro, non codificato in BER-TLV	'81'	C	C
Valore in chiaro, non codificato in BER-TLV, ma che non include DO SM	'B3'	C	C
Indicatore di contenuto di riempimento seguito da crittogramma, valore in chiaro, non codificato in BER-TLV	'87'	C	C
Le protetto	'97'	C	V
Stato di elaborazione	'99'	V	O
Totale di controllo crittografico	'8E'	O	O

Nota: come specificato nell'appendice 2, le carte tachigrafiche possono essere compatibili con i comandi READ BINARY e UPDATE BINARY con un byte INS dispari ("B1" risp. "D7"). Tali varianti di comandi sono necessarie per leggere e aggiornare i file con più di 32 768 byte. Nel caso in cui si usi tale variante, deve essere usato un oggetto di dati con tag "B3" invece di uno con tag "81". Cfr. appendice 2 per ulteriori informazioni.

CSM_189 Tutti gli oggetti di dati SM devono essere codificati in DER TLV come specificato nella norma [ISO 8825-1]. Questa codifica genera una struttura Tag-Lunghezza-Valore (TLV) come segue:

Tag: il tag è codificato in uno o due ottetti e indica il contenuto.

Lunghezza: la lunghezza è codificata come un numero intero senza segno in uno, due o tre ottetti, fino a una lunghezza massima di 65 535 ottetti. Deve essere usato il numero minimo di ottetti.

Valore: il valore è codificato come zero o più ottetti.

CSM_190 Gli APDU protetti con messaggistica sicura devono essere creati come segue:

— l'intestazione del comando (command header) deve essere inclusa nel calcolo del MAC, pertanto per il byte classe CLA deve essere usato il valore '0C'.

▼B

— Come specificato nell'appendice 2, tutti i byte INS devono essere pari, con l'eventuale eccezione di byte INS dispari per i comandi READ BINARY e UPDATE BINARY.

— Il valore effettivo di Lc sarà modificato in Lc' dopo l'applicazione della messaggistica sicura.

— Il campo dati deve essere costituito da oggetti di dati SM.

— Nel comando protetto APDU il nuovo byte Le deve essere impostato a '00'. Se necessario, nel campo di dati deve essere incluso un oggetto di dati '97' per trasmettere il valore iniziale di Le.

CSM_191 Qualsiasi oggetto di dati da criptare deve essere riempito conformemente alla norma [ISO 7816-4] usando l'indicatore di contenuto di riempimento '01'. Per il calcolo del MAC, ciascun oggetto di dati nell'APDU deve inoltre essere riempito separatamente conformemente alla norma [ISO 7816-4].

Nota: il riempimento per la messaggistica sicura è sempre eseguito a livello di messaggistica sicura e non dagli algoritmi CMAC o CBC.

Riepilogo ed esempi

Un comando APDU con messaggistica sicura applicata avrà la seguente struttura, a seconda del caso del rispettivo comando non sicuro (DO corrisponde a oggetto di dati):

Caso 1:	CLA INS P1 P2 || Lc' || DO '8E' || Le
Caso 2:	CLA INS P1 P2 || Lc' || DO '97' || DO '8E' || Le
Caso 3 (byte INS pari):	CLA INS P1 P2 || Lc' || DO '81' || DO '8E' || Le
Caso 3 (byte INS dispari):	CLA INS P1 P2 || Lc' || DO 'B3' || DO '8E' || Le
Caso 4 (byte INS pari):	CLA INS P1 P2 || Lc' || DO '81' || DO '97' || DO '8E' || Le
Caso 4 (byte INS dispari):	CLA INS P1 P2 || Lc' || DO 'B3' || DO '97' || DO '8E' || Le

dove Le = '00' o '00 00' a seconda che siano usati campi di lunghezza breve o campi di lunghezza estesa; cfr. [ISO 7816-4].

Una risposta APDU con messaggistica sicura applicata avrà la seguente struttura, a seconda del caso della rispettiva risposta non sicura:

Caso 1 o 3:	DO '99' || DO '8E' || SW1SW2
Caso 2 o 4 (byte INS pari) criptato:	DO '81' || DO '99' || DO '8E' || SW1SW2
Caso 2 o 4 (byte INS pari) non criptato:	DO '87' || DO '99' || DO '8E' || SW1SW2
Caso 2 o 4 (byte INS dispari) non criptato:	DO 'B3' || DO '99' || DO '8E' || SW1SW2

Nota: il caso 2 o 4 (byte INS dispari) criptato non è mai usato nella comunicazione tra una VU e una carta.

▼B

Di seguito tre esempi di trasformazioni APDU per comandi con codice INS pari. La Figura 8 mostra un comando APDU caso 4 autenticato, la Figura 9 una risposta APDU caso 2/caso 4 autenticata e la Figura 10 una risposta APDU, caso 2/caso 4 autenticata e criptata.

Figura 8

Transformation of an authenticated Case 4 Command APDU

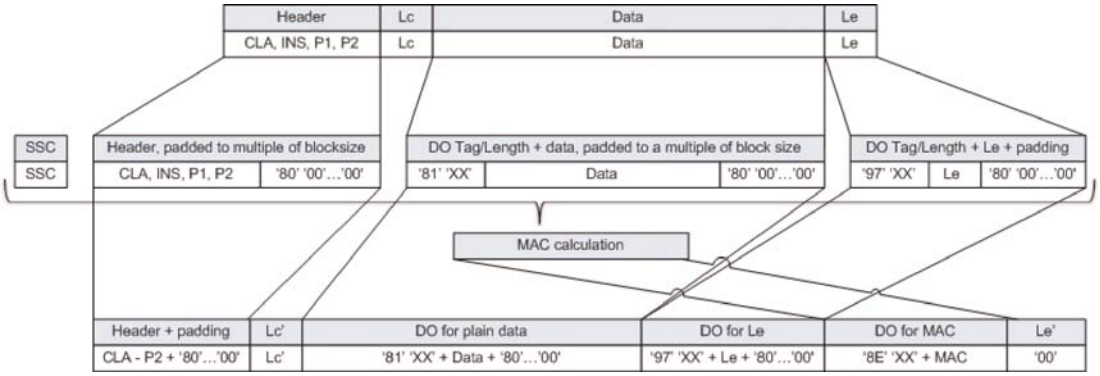
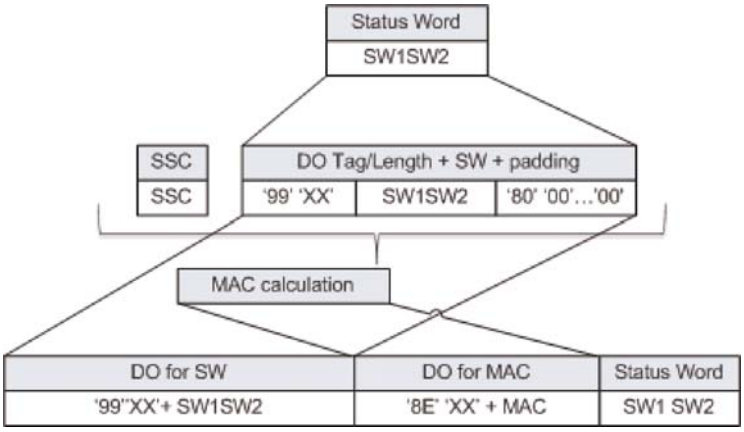


Figura 9

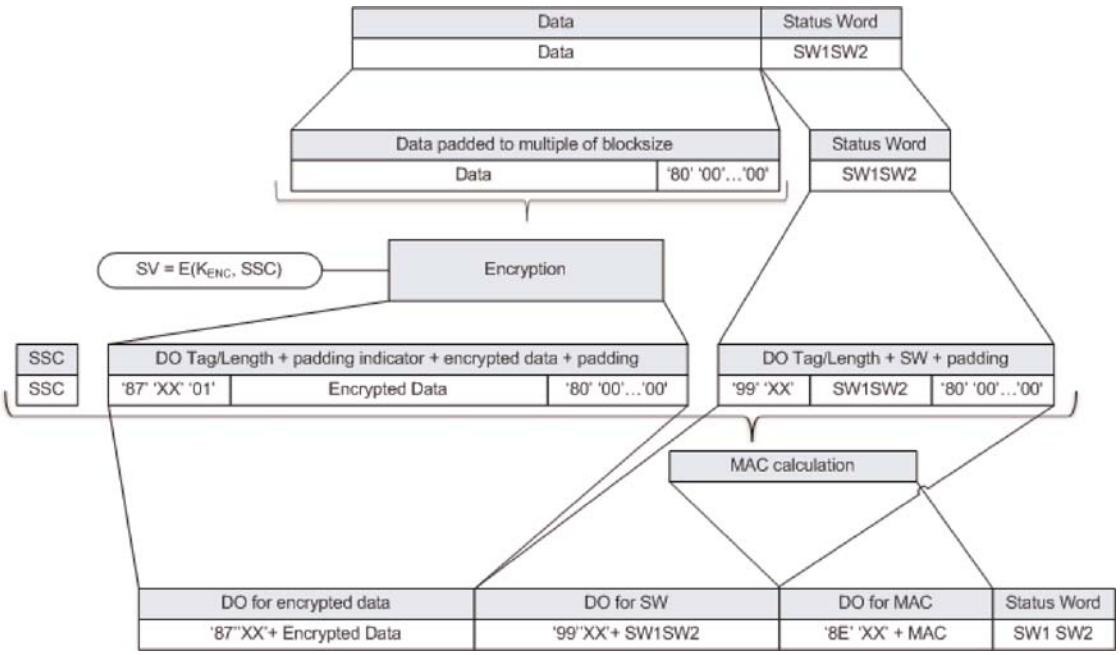
Transformation of an authenticated Case 1 / Case 3 Response APDU



▼B

Figura 10

Transformation of an encrypted and authenticated Case 2/Case 4 Response APDU



10.5.3 *Interruzione di una sessione di messaggistica sicura*

CSM_192 Una VU deve interrompere una sessione di messaggistica sicura (SM) in corso se e solo se si verifica una delle seguenti condizioni:

— la VU riceve una risposta APDU in chiaro;

— la VU individua un errore di messaggistica sicura in una risposta APDU:

  — manca un oggetto di dati atteso in messaggistica sicura, l'ordine degli oggetti di dati è errato o è incluso un oggetto di dati sconosciuto,

  — un oggetto di dati in messaggistica sicura non è corretto, ad esempio il valore MAC non è corretto, la struttura TLV non è corretta, o l'indicatore di riempimento nel tag ‘87’ non è uguale a ‘01’;

— la carta invia un byte di status che indica che ha riscontrato un errore di SM (cfr. CSM_194);

— si è raggiunto il limite per il numero di comandi e di risposte associate all'interno della sessione corrente. Per una data VU, tale limite deve essere definito dal suo fabbricante, tenendo conto dei requisiti di sicurezza dell'hardware usato, con un valore massimo di 240 comandi di SM e risposte associate per sessione.

▼B

CSM_193 Una carta tachigrafica deve interrompere una sessione di messaggistica sicura in corso se e solo se si verifica una delle seguenti condizioni:

— la carta tachigrafica riceve un comando APDU in chiaro;

— la carta tachigrafica individua un errore di messaggistica sicura in un comando APDU:

— manca un oggetto di dati atteso in messaggistica sicura, l'ordine degli oggetti di dati è errato o è incluso un oggetto di dati sconosciuto,

— un oggetto di dati in messaggistica sicura non è corretto, ad esempio il valore MAC non è corretto o la struttura TLV non è corretta;

— la carta non è più alimentata o viene reinizializzata;

— la VU seleziona una applicazione sulla carta;

— la VU inizia la procedura di autenticazione della VU;

— si è raggiunto il limite per il numero di comandi e di risposte associate all'interno della sessione corrente. Per una data carta, tale limite deve essere definito dal suo fabbricante, tenendo conto dei requisiti di sicurezza dell'hardware usato, con un valore massimo di 240 comandi di SM e risposte associate per sessione.

CSM_194 Per quanto riguarda l'errore di SM gestito da una carta tachigrafica:

— se in un comando APDU mancano alcuni oggetti di dati in messaggistica sicura attesi, l'ordine degli oggetti di dati non è corretto o sono inclusi oggetti di dati sconosciuti, una carta tachigrafica deve rispondere con i byte di stato ‘69 87’;

— se un oggetto di dati in messaggistica sicura in un comando APDU non è corretto, una carta tachigrafica deve rispondere con i byte di stato ‘69 88’.

In tal caso i byte di stato devono essere restituiti senza usare SM.

CSM_195 Se una sessione di messaggistica sicura tra una VU e una carta tachigrafica viene interrotta, la VU e le carte tachigrafiche devono:

— distruggere in modo sicuro le chiavi di sessione memorizzate;

— stabilire immediatamente una nuova sessione di messaggistica sicura, come descritto nelle sezioni 10.2 — 10.5.

CSM_196 Se per qualsiasi motivo la VU decide di riavviare l'autenticazione reciproca nei confronti di una carta inserita, la procedura deve riprendere con la verifica della catena di certificati della carta, come descritto nella sezione 10.2, e poi continuare come descritto nelle sezioni 10.2 — 10.5.

▼B

11. ACCOPPIAMENTO, AUTENTICAZIONE RECIPROCA E MESSAGGISTICA SICURA TRA VU E DISPOSITIVO GNSS ESTERNO

11.1. **Principi generali**

CSM_197 Il dispositivo GNSS usato da una VU per determinare la sua posizione può essere interno (ossia costruito all'interno dell'involucro della VU e non amovibile) o può essere un modulo esterno. Nel primo caso non vi è alcuna necessità di standardizzare la comunicazione interna tra il dispositivo GNSS e la VU, pertanto i requisiti di cui al presente capitolo non si applicano. Nel secondo caso, la comunicazione tra la VU e il dispositivo GNSS esterno deve essere standardizzata e protetta come indicato al presente capitolo.

CSM_198 La comunicazione sicura tra l'unità elettronica di bordo e un dispositivo GNSS esterno deve avvenire nello stesso modo della comunicazione sicura tra una VU e una carta tachigrafica, con il dispositivo GNSS esterno (EGF) nel ruolo della carta. Tutti i requisiti di cui al capitolo 10 per le carte tachigrafiche devono essere soddisfatti da un EGF, tenuto conto delle variazioni, dei chiarimenti e delle integrazioni di cui al presente capitolo. In particolare la verifica reciproca della catena di certificati, dell'autenticazione della VU e dell'autenticazione del chip deve essere effettuata come descritto nelle sezioni 11.3 e 11.4.

CSM_199 La comunicazione tra la VU e un EGF differisce dalla comunicazione tra una VU e una carta nel fatto che è necessario che una VU e un EGF siano stati accoppiati una volta in officina prima di potersi scambiarsi dati basati su GNSS durante il funzionamento normale. La procedura di accoppiamento è descritta nella sezione 11.2.

CSM_200 Per la comunicazione tra una VU e un EGF devono essere usati i comandi e le risposte APDU basati sulle norme [ISO 7816-4] e [ISO 7816-8]. La struttura esatta di tali APDU è definita nell'appendice 2 del presente allegato.

11.2. **Accoppiamento tra VU e dispositivo GNSS esterno**

CSM_201 L'accoppiamento tra una VU e un EGF di un veicolo deve essere eseguito in officina. Solo una VU e un EGF che sono stati accoppiati sono in grado di comunicare durante il funzionamento normale.

CSM_202 L'accoppiamento tra una VU e un EGF è possibile solo se la VU è in modalità taratura. L'accoppiamento deve essere avviato dalla VU.

CSM_203 Un'officina può riaccoppiare una VU con un altro o con lo stesso EGF in qualsiasi momento. Durante il riaccoppiamento la VU deve cancellare dalla sua memoria in modo sicuro il certificato EGF_MA esistente e memorizzare il certificato EGF_MA dell'EGF a cui viene accoppiata.

CSM_204 Un'officina può riaccoppiare un dispositivo GNSS esterno con un'altra o con la stessa VU in qualsiasi momento. Durante il riaccoppiamento l'EGF deve cancellare dalla sua memoria in modo sicuro il certificato VU_MA esistente e memorizzare il certificato VU_MA della VU a cui viene accoppiato.

▼B

11.3. **Verifica reciproca della catena di certificati**

11.3.1 *Principi generali*

CSM_205 La verifica reciproca della catena di certificati tra una VU e un EGF deve avvenire solo durante l'accoppiamento della VU con l'EGF in officina. Durante il funzionamento normale di una VU e un EGF accoppiati, nessun certificato deve essere verificato, poiché la VU e l'EGF devono fidarsi dei certificati che hanno memorizzato durante l'accoppiamento, dopo averne verificato la validità temporale. Per proteggere la comunicazione tra la VU e l'EFG, questi ultimi non devono fidarsi di nessun altro certificato.

11.3.2 *Durante l'accoppiamento tra VU e EFG*

CSM_206 Durante l'accoppiamento con un EFG, una VU deve usare il protocollo illustrato nella Figura 4 (sezione 10.2.1) per verificare la catena di certificati del dispositivo GNSS esterno.

Note alla Figura 4 in questo contesto:

— il controllo della comunicazione non rientra nel campo di applicazione della presente appendice. L'EGF non è tuttavia una carta intelligente (smart card), per cui la VU probabilmente non invierà un comando di reinizializzazione (Reset) per avviare la comunicazione e non riceverà un ATR.

— I certificati e le chiavi pubbliche della carta citati nella figura devono essere interpretati come i certificati e le chiavi pubbliche dell'EGF per l'autenticazione reciproca. Nella sezione 9.1.6 sono indicati come EGF_MA.

— I certificati Card.CA e le chiavi pubbliche citati nella figura devono essere interpretati come i certificati e le chiavi pubbliche dell'MSCA per la firma dei certificati EGF. Nella sezione 9.1.3 sono indicati come MSCA_VU-EGF.

— Il certificato Card.CA.EUR citato nella figura deve essere interpretato come il certificato radice europeo indicato nel CAR del certificato MSCA_VU-EGF.

— Il certificato Card.Link citato nella figura deve essere interpretato come il certificato di collegamento dell'EGF, se presente. Come specificato nella sezione 9.1.2, si tratta di un certificato di collegamento per una nuova coppia di chiavi radice europee creata dalla ERCA e firmata con la precedente chiave privata europea.

— Il certificato Card.Link.EUR è il certificato radice europeo indicato nel CAR del certificato Card.Link.

— Invece del `cardExtendedSerialNumber`, la VU deve leggere il `sensorGNSSserialNumber` dall'EF ICC.

— Invece di selezionare Tachograph AID, la VU deve selezionare EGF AID.

— ‘Ignore Card’ (Ignora Carta) deve essere interpretato come ‘Ignore EGF’ (Ignora EGF).

▼B

CSM_207 Dopo la verifica del certificato EGF_MA, la VU deve memorizzare tale certificato da usare durante il funzionamento normale; cfr. sezione 11.3.3.

CSM_208 Durante l'accoppiamento a una VU, un dispositivo GNSS esterno deve usare il protocollo illustrato in Figura 5 (sezione 10.2.2) per verificare la catena di certificati della VU.

Note alla Figura 5 in questo contesto:

— la VU deve generare una nuova coppia di chiavi temporanee usando i parametri di dominio nel certificato EGF.

— I certificati e le chiavi pubbliche della VU citati nella figura sono quelli usati per l'autenticazione reciproca. Nella sezione 9.1.4 sono indicati come VU_MA.

— I certificati e le chiavi pubbliche VU.CA citati nella figura sono quelli usati per firmare i certificati della VU e del dispositivo GNSS esterno. Nella sezione 9.1.3 sono indicati come MSCA_VU-EGF.

— Il certificato VU.CA.EUR citato nella figura è il certificato radice europeo indicato nel CAR del certificato VU.CA.

— Il certificato VU.Link indicato nella figura è il certificato di collegamento della VU, se presente. Come specificato nella sezione 9.1.2, si tratta di un certificato di collegamento per una nuova coppia di chiavi radice europee creata dalla ERCA e firmata con la precedente chiave privata europea.

— Il certificato VU.Link.EUR è il certificato radice europeo indicato nel CAR del certificato VU.Link.

CSM_209 A differenza di quanto previsto nel requisito CSM_167, un EGF deve usare l'ora del GNSS per verificare la validità temporale di qualsiasi certificato presentato.

CSM_210 Dopo la verifica del certificato VU_MA, il dispositivo GNSS esterno deve memorizzare tale certificato da usare durante il funzionamento normale; cfr. sezione 11.3.3.

11.3.3 *Durante il funzionamento normale*

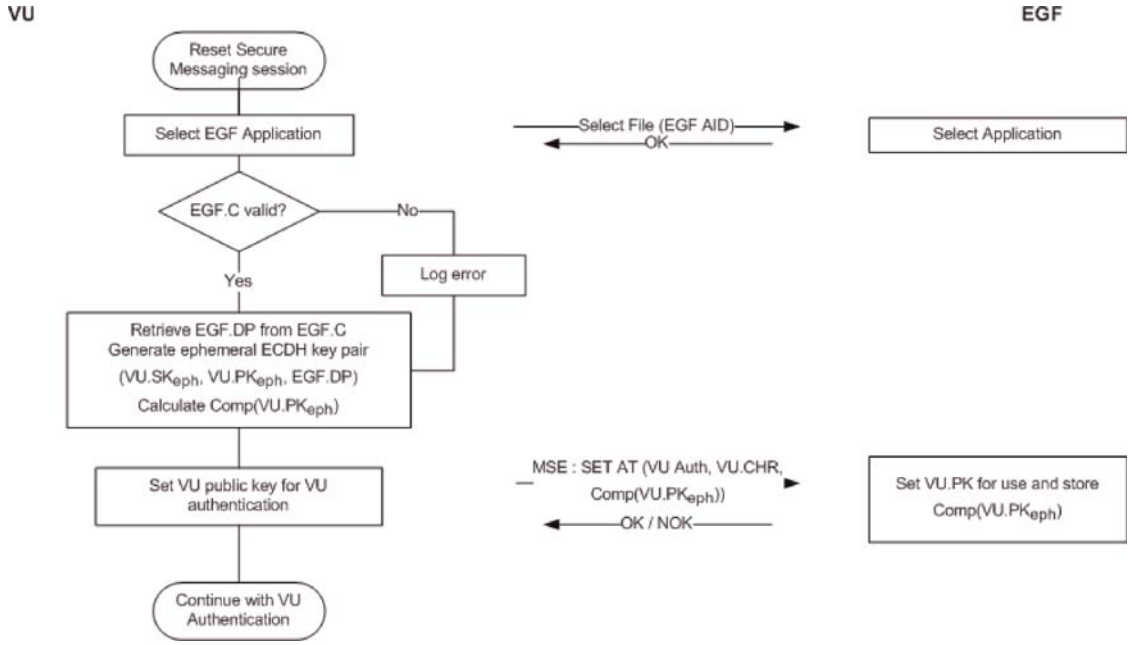
CSM_211 Durante il funzionamento normale, una VU e un EGF devono usare il protocollo della Figura 11 per verificare la validità temporale dei certificati EGF_MA e VU_MA memorizzati e per impostare la chiave pubblica VU_MA per la successiva autenticazione della VU. Durante il normale funzionamento non deve aver luogo nessun'altra verifica reciproca delle catene di certificati.

Da notare che la Figura 11 è costituita sostanzialmente dalle prime fasi illustrate nella Figura 4 e nella Figura 5. Si noti inoltre che un EGF non è una carta intelligente (smart card), per cui la VU probabilmente non invierà un comando di reinizializzazione (Reset) per avviare la comunicazione e non riceverà un ATR. In ogni caso ciò non rientra nel campo di applicazione della presente appendice.

▼B

Figura 11

Verifica reciproca della validità temporale dei certificati durante un funzionamento normale VU — EGF



CSM_212 Come illustrato nella Figura 11, la VU deve registrare un errore se il certificato EGF_MA non è più valido. L'autenticazione reciproca, l'accordo sulla chiave e la successiva comunicazione mediante messaggistica sicura devono tuttavia proseguire normalmente.

11.4. **Autenticazione della VU, autenticazione del chip e accordo sulla chiave di sessione**

CSM_213 L'autenticazione della VU, l'autenticazione del chip e l'accordo sulla chiave di sessione tra una VU e un EGF devono avere luogo nel corso delle operazioni di accoppiamento e ogniqualvolta si ripristini una sessione di messaggistica sicura durante il funzionamento normale. La VU e l'EFG devono eseguire le procedure descritte nelle sezioni 10.3 e 10.4. Si applicano tutti i requisiti di tali sezioni.

11.5. **Messaggistica sicura**

CSM_214 Tutti i comandi e le risposte scambiate tra una VU e un dispositivo GNSS esterno, dopo un'autenticazione del chip con esito positivo e fino alla fine della sessione, devono essere protette mediante messaggistica sicura in modalità di sola autenticazione. Si applicano tutti i requisiti della sezione 10.5.

CSM_215 Se si interrompe una sessione di messaggistica sicura tra una VU e un EFG, la VU deve stabilire immediatamente una nuova sessione di messaggistica sicura, come descritto nelle sezioni 11.3.3 e 11.4.

12. ABBINAMENTO E COMUNICAZIONE TRA VU E SENSORE DI MOVIMENTO

12.1. **Principi generali**

CSM_216 La VU e il sensore di movimento devono comunicare usando il protocollo di interfaccia specificato nella norma [ISO 16844-3] durante l'abbinamento e in condizioni di funzionamento normale, con le modifiche descritte nel presente capitolo e nella sezione 9.2.1.

▼B

Nota: si presume che i lettori del presente capitolo conoscano il contenuto della norma [ISO 16844-3].

12.2. **Abbinamento tra VU e sensore di movimento usando diverse generazioni di chiavi**

Come spiegato nella sezione 9.2.1, la chiave master del sensore di movimento e tutte le chiavi associate vengono periodicamente sostituite. Ciò fa sì che le carte dell'officina possano contenere fino a tre chiavi AES relative al sensore di movimento $K_{M\text{-}WC}$ (di generazioni consecutive). Analogamente i sensori di movimento possono contenere fino a tre diverse cifrature di dati basate su AES (basate su generazioni consecutive della chiave master del sensore di movimento K_M). Una VU contiene una sola chiave relativa al sensore di movimento $K_{M\text{-}VU}$.

CSM_217 Una VU di seconda generazione e un sensore di movimento di seconda generazione devono essere abbinati come segue (cfr. tabella 6 nella norma [ISO 16844-3]):

1. si inserisce una carta dell'officina di seconda generazione nella VU e si collega quest'ultima al sensore di movimento.

2. La VU legge tutte le chiavi $K_{M\text{-}WC}$ disponibili dalla carta dell'officina, controlla i rispettivi numeri di versione e sceglie quella il cui numero di versione corrisponde alla chiave $K_{M\text{-}VU}$ della VU. Se nella carta dell'officina non è presente la corrispondente chiave $K_{M\text{-}WC}$, la VU interrompe la procedura di abbinamento e mostra un messaggio di errore apposito al titolare della carta dell'officina.

3. La VU calcola la chiave master del sensore di movimento K_M da $K_{M\text{-}VU}$ e $K_{M\text{-}WC}$ e la chiave di identificazione K_{ID} da K_M, come specificato nella sezione 9.2.1.

4. La VU invia l'istruzione di avviare la procedura di abbinamento con il sensore di movimento, come descritto nella norma [ISO 16844-3], e cripta il numero di serie che riceve dal sensore di movimento con la chiave di identificazione K_{ID}. La VU restituisce il numero di serie criptato al sensore di movimento.

5. Il sensore di movimento confronta il numero di serie criptato con ciascuna delle cifrature del numero di serie che contiene, in successione. Se ne trova una che corrisponde, la VU viene autenticata. Il sensore di movimento nota la generazione della K_{ID} usata dalla VU e restituisce la corrispondente versione criptata della sua chiave di abbinamento; vale a dire la cifratura creata usando la stessa generazione di K_M.

6. La VU decripta la chiave di accoppiamento usando K_M, genera una chiave di sessione K_S, la cripta con la chiave di abbinamento e invia il risultato al sensore di movimento. Il sensore di movimento decripta K_S.

7. La VU assembla le informazioni di accoppiamento come definito nella norma [ISO 16844-3], cripta le informazioni con la chiave di abbinamento e invia il risultato al sensore di movimento. Il sensore di movimento decripta le informazioni di abbinamento.

8. Il sensore di movimento cripta le informazioni di abbinamento con la chiave K_S che ha ricevuto e le restituisce alla VU. La VU verifica che le informazioni di abbinamento siano le stesse informazioni inviate dalla VU al sensore di movimento nella fase precedente. Se sì, il sensore di movimento ha usato la stessa K_S della VU

▼B

e pertanto nella fase 5 ha inviato la chiave di abbinamento cifrata con la generazione corretta di K_M. Il sensore di movimento viene quindi autenticato.

Da notare che le fasi 2 e 5 sono diverse dalla procedura standard della norma [ISO 16844-3]; le altre fasi sono standard.

Esempio: supponiamo che un abbinamento abbia luogo nel corso del primo anno di validità del certificato ERCA (3); cfr. la Figura 2 nella sezione 9.2.1.2. Inoltre

— supponiamo che il sensore di movimento sia stato rilasciato nell'ultimo anno di validità del certificato ERCA (1). Esso conterrà quindi i seguenti dati e chiavi:

  — $N_s[1]$: numero di serie criptato con la generazione 1 della chiave K_{ID},

  — $N_s[2]$: numero di serie criptato con la generazione 2 della chiave K_{ID},

  — $N_s[3]$: numero di serie criptato con la generazione 3 della chiave K_{ID},

  — $K_P[1]$: chiave di abbinamento della generazione 1 ([1]), criptata con la generazione 1 della chiave K_M,

  — $K_P[2]$: chiave di abbinamento di seconda generazione, criptata con la generazione 2 della chiave K_M,

  — $K_P[3]$: chiave di abbinamento di terza generazione, criptata con la generazione 3 della chiave K_M,

— supponiamo che la carta dell'officina sia stata rilasciata nel primo anno di validità del certificato ERCA (3). Essa conterrà pertanto la seconda e la terza generazione della chiave $K_{M\text{-}WC}$.

— Supponiamo che la VU sia di seconda generazione e che contenga la chiave $K_{M\text{-}VU}$ di seconda generazione.

In tal caso nelle fasi da 2 a 5 si verificherà quanto segue:

— Fase 2: la VU legge la generazione 2 e la generazione 3 della chiave $K_{M\text{-}WC}$ dalla carta dell'officina e controlla il loro numero di versione.

— Fase 3: la VU combina la chiave $K_{M\text{-}WC}$ di seconda generazione con la sua chiave $K_{M\text{-}VU}$ per calcolare K_M e K_{ID}.

— Fase 4: la VU cripta il numero di serie che riceve dal sensore di movimento con la chiave K_{ID}.

— Fase 5: il sensore di movimento confronta i dati ricevuti con $N_s[1]$ e non trova corrispondenze. Successivamente confronta i dati con $N_s[2]$ e trova una corrispondenza. Il sensore di movimento conclude che la VU è di seconda generazione e quindi restituisce $K_P[2]$.

([1]) Da notare che le chiavi di abbinamento di prima, seconda e terza generazione possono in realtà essere la stessa chiave o possono essere tre chiavi diverse con diverse lunghezze, come spiegato in CSM_117.

▼B

12.3. **Abbinamento e comunicazione tra VU e sensore di movimento usando AES**

CSM_218 Come specificato nella Tabella 3 della sezione 9.2.1, tutte le chiavi coinvolte nell'abbinamento di una VU (di seconda generazione) con un sensore di movimento (MoS) e nelle successive comunicazioni devono essere chiavi AES, invece di chiavi in TDES a doppia lunghezza come specificato nella norma [ISO 16844-3]. Tali chiavi AES possono avere una lunghezza di 128, 192 o 256 bit. Poiché le dimensioni dei blocchi AES sono di 16 byte, la lunghezza di un messaggio criptato deve essere un multiplo di 16 byte, rispetto agli 8 byte per il TDES. Alcuni di questi messaggi saranno inoltre usati per trasportare le chiavi AES, la cui lunghezza può essere di 128, 192 o 256 bit. Il numero di byte di dati per ciascuna istruzione nella tabella 5 della norma [ISO 16844-3] deve pertanto essere modificato come indicato nella Tabella 6:

Tabella 6

Numero di byte di dati di testo in chiaro (plaintext) e criptati per istruzione definiti in [ISO 16844-3]

Istruzione	Richiesta / risposta	Descrizione dei dati	# di byte di dati di testo in chiaro (plaintext) secondo [ISO 16844-3]	# di byte di dati di testo in chiaro (plaintext) usando chiavi AES	# di byte di dati criptati usando chiavi AES di lunghezza (in bit)		
					128	192	256
10	richiesta	Dati di autenticazione + numero del file	8	8	16	16	16
11	risposta	Dati di autenticazione + contenuto del file	16 o 32 a seconda del file	16 o 32 a seconda del file	16 / 32	16 / 32	16 / 32
41	richiesta	Numero di serie MoS	8	8	16	16	16
41	risposta	Chiave di abbinamento	16	16 / 24 / 32	16	32	32
42	richiesta	Chiave di sessione	16	16 / 24 / 32	16	32	32
43	richiesta	Informazioni di abbinamento	24	24	32	32	32
50	risposta	Informazioni di abbinamento	24	24	32	32	32
70	richiesta	Dati di autenticazione	8	8	16	16	16
80	risposta	Valore del contatore del MoS + dati di autenticazione	8	8	16	16	16

CSM_219 Le informazioni di abbinamento inviate nell'istruzione 43 (richiesta della VU) e 50 (risposta del MoS) devono essere assemblate come specificato nella sezione 7.6.10 della norma [ISO 16844-3], con la differenza che deve essere usato l'algoritmo AES invece dell'algoritmo TDES nello schema di cifratura dei dati di abbinamento, generando quindi due cifrature AES e adottando il riempimento specificato in CSM_220 per rispettare le dimensioni del blocco AES. La chiave K'_P usata per tale cifratura deve essere generata come segue:

— nel caso in cui la chiave di abbinamento K_P sia lunga 16 byte: $K'_P = K_P \text{ XOR } (N_s||N_s)$;

▼B

— nel caso in cui la chiave di abbinamento K_P sia lunga 24 byte: $K'_p = K_P$ XOR $(N_s||N_s||N_s)$;

— nel caso in cui la chiave di abbinamento K_P sia lunga 32 byte: $K'_p = K_P$ XOR $(N_s||N_s||N_s||N_s)$;

dove N_S è il numero di serie a 8 byte del sensore di movimento.

CSM_220 Nel caso in cui la lunghezza dei dati di testo in chiaro (usando le chiavi AES) non sia un multiplo di 16 byte, deve essere usato il metodo di riempimento 2 definito nella norma [ISO 9797-1].

Nota: nella norma [ISO 16844-3], il numero di byte di dati di testo in chiaro è sempre un multiplo di 8, in modo che non sia necessario alcun riempimento quando si usa TDES. La definizione dei dati e dei messaggi della norma [ISO 16844-3] non è modificata da questa parte della presente appendice, che quindi richiede l'uso del riempimento.

CSM_221 Per l'istruzione 11 e nel caso sia necessario criptare più di un blocco di dati, deve essere usata la modalità di funzionamento a blocchi incatenati (CBC) come definito nella norma [ISO 10116], con un parametro di interleave *m* = 1. L'IV da usare è

— per l'istruzione 11: il blocco di autenticazione a 8 byte indicato alla sezione 7.6.3.3 della norma [ISO 16844-3], riempito usando il metodo di riempimento 2 definito nella norma [ISO 9797-1]; cfr. anche le sezioni 7.6.5 e 7.6.6 della norma [ISO 16844-3].

— Per tutte le altre istruzioni in cui sono trasferiti più di 16 byte come specificato nella Tabella 6: '00' {16}, vale a dire sedici byte con valore binario 0.

Nota: come indicato nelle sezioni 7.6.5 e 7.6.6 della norma [ISO 16844-3], quando il MoS cripta i file di dati per l'inclusione nell'istruzione 11, il blocco di autenticazione è sia:

— usato come vettore di inizializzazione per la cifratura dei file di dati in modalità CBC, che

— criptato e incluso come primo blocco nei dati inviati alla VU.

12.4. **Abbinamento tra VU e sensore di movimento per diverse generazioni di apparecchi**

CSM_222 Come spiegato nella sezione 9.2.1, un sensore di movimento di seconda generazione può contenere la cifratura basata su TDES dei dati di abbinamento (come definito nella parte A della presente appendice), che gli permette di essere abbinato a una VU di prima generazione. In tal caso, una VU di prima generazione e un sensore di movimento di seconda generazione devono essere abbinati come descritto nella parte A della presente appendice e nella norma [ISO 16844-3]. Per l'abbinamento è possibile usare sia una carta dell'officina di prima generazione che una di seconda generazione.

Note:

— Non è possibile accoppiare una VU di seconda generazione a un sensore di movimento di prima generazione.

▼B

— Non è possibile usare una carta dell'officina di prima generazione per l'accoppiamento di una VU di seconda generazione a un sensore di movimento.

13. SICUREZZA PER LA COMUNICAZIONE REMOTA ATTRAVERSO DSRC

13.1. **Principi generali**

Come specificato nell'appendice 14, la VU genera periodicamente dati di monitoraggio del tachigrafo a distanza (Remote Tachograph Monitoring — RTM) e li trasmette al dispositivo (interno o esterno) di comunicazione remota (Remote Communication Facility — RCF). Il dispositivo di comunicazione remota è responsabile dell'invio di tali dati all'interrogatore remoto attraverso l'interfaccia DSRC descritta nell'appendice 14. L'appendice 1 specifica che i dati RTM sono la concatenazione di:

payload (dati utili trasmessi) criptato del tachigrafo cifratura del payload del tachigrafo;

dati di sicurezza DSRC come da descrizione che segue

Il formato in chiaro dei dati payload del tachigrafo è specificato nell'appendice 1 ed ulteriormente descritto nell'appendice 14. La presente sezione descrive la struttura dei dati di sicurezza DSRC; la specifica formale è descritto nell'appendice 1.

CSM_223 I dati di testo in chiaro `tachographPayload` trasmessi da una VU a un dispositivo di comunicazione remota (se l'RCF è esterno alla VU) o dalla VU all'interrogatore remoto tramite l'interfaccia DSRC (se l'RCF è interno alla VU) devono essere protetti in modalità cifratura seguita da autenticazione (encrypt-then-authenticate), cioè in primo luogo si criptano i dati payload del tachigrafo per garantire la riservatezza del messaggio e successivamente si calcola un MAC per garantire l'autenticità e l'integrità dei dati.

CSM_224 I dati di sicurezza DSRC devono essere costituiti dalla concatenazione dei seguenti elementi di dati nell'ordine seguente; cfr. anche Figura 12:

data e ora correnti	la data e l'ora correnti della VU (tipo di dati `TimeReal`);
contatore	un contatore da 3 byte, cfr. CSM_225;
numero di serie della VU	il numero di serie della VU (tipo di dati `VuSerialNumber`);
numero di versione della chiave master DSRC	il numero di versione da un byte della chiave master DSRC da cui sono calcolate le chiavi DSRC specifiche della VU, cfr. sezione 9.2.2;
MAC	il MAC calcolato su tutti i byte precedenti dei dati RTM.

CSM_225 Il contatore da 3 byte nei dati di sicurezza DSRC deve essere in formato MSB-first. La prima volta che una VU calcola una serie di dati RTM dopo essere stata messa in produzione, il valore del contatore deve essere impostato a 0. La VU deve aumentare di 1 il valore del contatore di dati ogni volta che si appresta a calcolare una nuova serie di dati RTM.

▼B

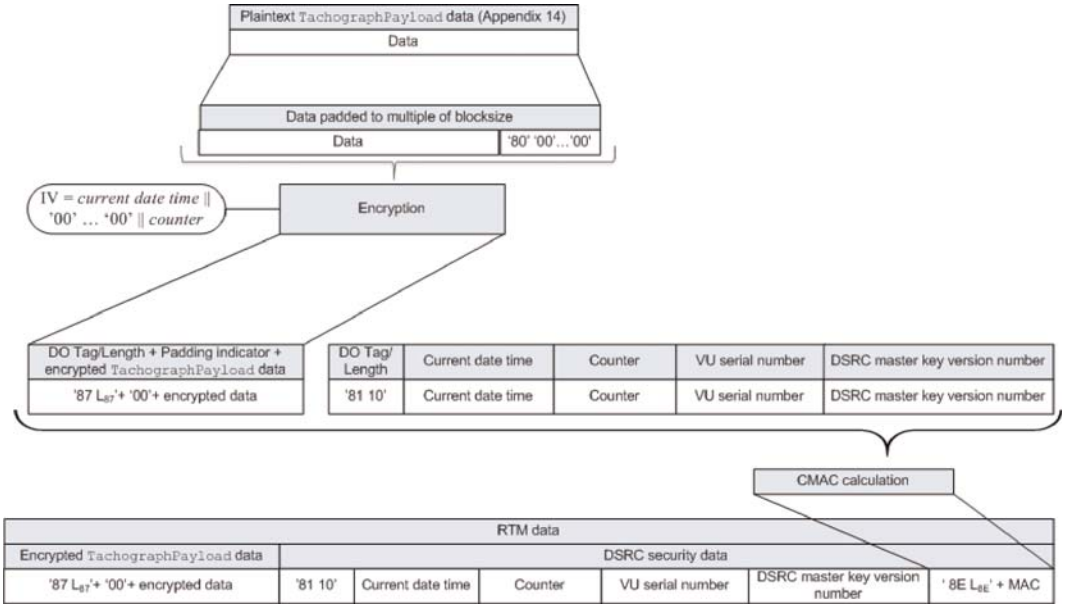
13.2. **Cifratura del payload del tachigrafo e generazione del MAC**

CSM_226 Dato un elemento di dati in chiaro con tipo di dati `TachographPayload` come descritto nell'appendice 14, la VU deve criptare tali dati come illustrato nella Figura 12: deve essere usata la chiave DSRC per la cifratura $K_VU_{DSRC}_ENC$ (cfr. sezione 9.2.2) con AES modalità di funzionamento a blocchi incatenati (CBC), come definito nella norma [ISO 10116], con un parametro di interleave $m = 1$. Il vettore di inizializzazione deve essere uguale a *IV = data e ora correnti* || '*00 00 00 00 00 00 00 00*' || *contatore*, dove *data e ora correnti* e *contatore* sono specificati in CSM_224. I dati da criptare devono essere riempiti usando il metodo 2 definito nella norma [ISO 9797-1].

CSM_227 La VU deve calcolare il MAC nei dati di sicurezza DSRC come indicato nella Figura 12: il MAC deve essere calcolato su tutti i byte precedenti nei dati RTM, fino al numero di versione della chiave master DSRC incluso, includendo i tag e le lunghezze degli oggetti di dati. La VU deve usare la sua chiave DSRC per autenticità $K_VU_{DSRC}_MAC$ (cfr. sezione 9.2.2) con l'algoritmo AES in modalità CMAC come specificato in [SP 800-38B]. La lunghezza del MAC deve essere collegata alla lunghezza delle chiavi DSRC specifiche della VU, come specificato in CSM_50.

Figura 12

Cifratura del payload del tachigrafo e generazione del MAC



13.3. **Verifica e decifratura del payload del tachigrafo**

CSM_228 Quando un interrogatore remoto riceve dati RTM da una VU, esso deve inviare l'intero pacchetto di dati RTM a una carta di controllo nel campo dati di un comando PROCESS DSRC MESSAGE, come descritto nell'appendice 2. Successivamente:

▼B

1. la carta di controllo deve verificare il numero di versione della chiave master DSRC nei dati di sicurezza DSRC. Se non conosce la chiave master DSRC indicata, la carta di controllo deve restituire un errore specificato nell'appendice 2 e interrompere la procedura.

2. La carta di controllo deve usare la chiave master DSRC in combinazione con il numero di serie della VU nei dati di sicurezza DSRC per calcolare le chiavi DSRC specifiche della VU K_VU_{DSRC}_ENC e K_VU_{DSRC}_MAC, come specificato in CSM_124.

3. La carta di controllo deve usare K_VU_{DSRC}_MAC per verificare il MAC nei dati di sicurezza DSRC, come specificato in CSM_227. Se il MAC non è corretto, la carta di controllo deve restituire un errore specificato nell'appendice 2 e interrompere la procedura.

4. La carta di controllo deve usare K_VU_{DSRC}_ENC per decriptare il payload criptato del tachigrafo, come specificato in CSM_226. La carta di controllo deve eliminare il riempimento e restituire i dati payload decriptati del tachigrafo all'interrogatore remoto.

CSM_229 Al fine di impedire attacchi di tipo replay attack, l'interrogatore remoto deve verificare l'attualità dei dati RTM verificando che *data e ora correnti* nei dati di sicurezza DSRC non si discostino eccessivamente dall'ora corrente dell'interrogatore remoto.

Note:

— ciò implica che l'interrogatore remoto usi una sorgente oraria precisa e affidabile.

— Poiché secondo l'appendice 14 la VU calcola una nuova serie di dati RTM ogni 60 secondi e l'orologio della VU può discostarsi di 1 minuto dall'ora effettiva, il limite inferiore per l'attualità dei dati RTM è di 2 minuti. L'attualità effettiva necessaria dipende anche dalla precisione dell'orologio dell'interrogatore remoto.

CSM_230 Quando verifica il corretto funzionamento della funzionalità DSRC di una VU, l'officina deve inviare l'intero pacchetto di dati RTM ricevuti dalla VU a una carta dell'officina nel campo dati di un comando PROCESS DSRC MESSAGE, come descritto nell'appendice 2. La carta dell'officina deve effettuare tutti i controlli e le azioni specificati in CSM_228.

14. FIRMA DEL TRASFERIMENTO DEI DATI E VERIFICA DELLE FIRME

14.1. **Principi generali**

CSM_231 L'apparecchio intelligente dedicato (Intelligent Dedicated Equipment — IDE) deve memorizzare in un file di dati fisico i dati ricevuti da una VU o da una carta durante una sessione di trasferimento. I dati possono essere memorizzati in un dispositivo di memorizzazione esterno (ESM). Tale file contiene firme digitali su blocchi di dati, come specificato nell'appendice 7, e deve contenere inoltre i seguenti certificati (cfr. sezione 9.1):

▼B

— in caso di trasferimento dei dati su VU:

— il certificato VU_Sign,

— il certificato MSCA_VU-EGF contenente la chiave pubblica da usare per la verifica del certificato VU_Sign;

— in caso di trasferimento dei dati su carta:

— il certificato Card_Sign,

— il certificato MSCA_Card contenente la chiave pubblica da usare per la verifica del certificato Card_Sign.

CSM_232 L'IDE deve anche disporre di:

— nel caso usi una carta di controllo per verificare la firma, come illustrato nella Figura 13: il certificato di collegamento che collega l'ultimo certificato EUR al certificato EUR il cui periodo di validità è immediatamente precedente, se esistenti;

— nel caso verifichi esso stesso la firma: tutti i certificati radice europei validi.

Nota: il metodo usato dall'IDE per recuperare tali certificati non è specificato nella presente appendice.

14.2. **Generazione della firma**

CSM_233 L'algoritmo di firma usato per creare le firme digitali sui dati trasferiti deve essere ECDSA, come specificato in [DSS], usando l'algoritmo di hash collegato alle dimensioni della chiave della VU o della carta, come specificato in CSM_50. Il formato della firma deve essere in chiaro, come specificato in [TR-03111].

14.3. **Verifica della firma**

CSM_234 Un IDE può verificare la firma sui dati trasferiti oppure può usare una carta di controllo per questo scopo. Nel caso usi una carta di controllo, la verifica della firma può avvenire come illustrato in Figura 13. Nel caso verifichi esso stesso la firma, l'IDE deve verificare l'autenticità e la validità di tutti i certificati della catena di certificati nel file di dati e la firma sui dati che seguono lo schema di firma definito in [DSS].

Note alla Figura 13:

— l'apparecchio che ha firmato i dati da analizzare è indicato con EQT.

— I certificati e le chiavi pubbliche EQT citati nella figura sono quelli usati per la firma, cioè VU_Sign o Card_Sign.

— I certificati e le chiavi pubbliche EQT.CA citati nella figura sono quelli usati per firmare i certificati della VU o della carta, a seconda del caso.

— Il certificato EQT.CA.EUR citato nella figura è il certificato radice europeo indicato nel CAR del certificato EQT.CA.

▼B

— Il certificato EQT.Link indicato nella figura è il certificato di collegamento dell'EQT, se presente. Come specificato nella sezione 9.1.2, si tratta di un certificato di collegamento per una nuova coppia di chiavi radice europee creata dalla ERCA e firmate con la precedente chiave privata europea.

— Il certificato EQT.Link.EUR è il certificato radice europeo indicato nel CAR del certificato ETQ.Link.

CSM_235 Per calcolare l'hash M inviato alla carta di controllo nel comando PSO:Hash, l'IDE deve usare l'algoritmo di hash collegato alle dimensioni della chiave della VU o della carta da cui sono trasferiti i dati, come specificato in CSM_50.

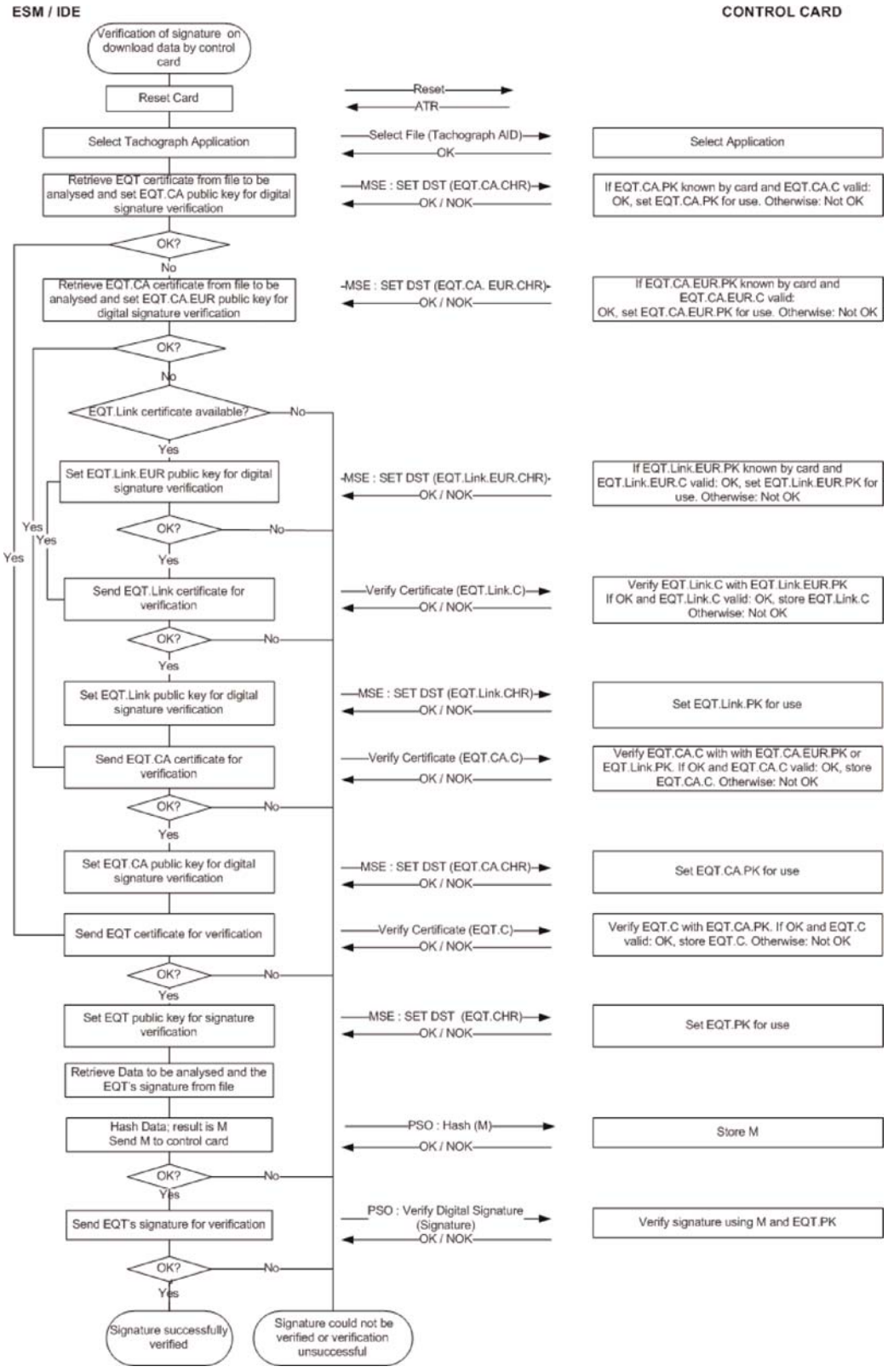
CSM_236 Per verificare la firma dell'EQT, la carta di controllo deve seguire lo schema di firma definito in [DSS].

Nota: il presente documento non specifica alcuna azione da intraprendere se la firma su un file di dati trasferito non può essere verificata o se la verifica non va a buon fine.

▼B

Figura 13

Protocollo di verifica della firma su un file di dati trasferiti



▼B

Appendice 12

POSIZIONAMENTO BASATO SUL SISTEMA GLOBALE DI NAVIGAZIONE SATELLITARE (GNSS)

INDICE

1. INTRODUZIONE

1.1. Campo di applicazione

1.2. Acronimi e simboli

2. SPECIFICHE DEL RICEVITORE GNSS

3. FRASI NMEA

4. UNITÀ ELETTRONICA DI BORDO CON DISPOSITIVO GNSS ESTERNO

4.1. Configurazione

4.1.1 Componenti principali e interfacce

4.1.2 Stato del dispositivo GNSS esterno alla fine della produzione

4.2. Comunicazione tra il dispositivo GNSS esterno e l'unità elettronica di bordo

4.2.1 Protocollo di comunicazione

4.2.2 Trasferimento sicuro di dati GNSS

4.2.3 Struttura del comando Read Record

4.3. Accoppiamento, autenticazione reciproca e accordo sulla chiave di sessione del dispositivo GNSS esterno con l'unità elettronica di bordo

4.4. Gestione degli errori

4.4.1 Errore di comunicazione con il dispositivo GNSS esterno

4.4.2 Violazione dell'integrità fisica del dispositivo GNSS esterno

4.4.3 Assenza di informazioni sulla posizione provenienti dal ricevitore GNSS

4.4.4 Certificato del dispositivo GNSS esterno scaduto

5. UNITÀ ELETTRONICA DI BORDO SENZA DISPOSITIVO GNSS ESTERNO

5.1. Configurazione

5.2. Gestione degli errori

5.2.1 Assenza di informazioni sulla posizione provenienti dal ricevitore GNSS

6. CONFLITTO DI ORARI DEL GNSS

7. CONFLITTO SUL MOVIMENTO DEL VEICOLO

1. INTRODUZIONE

La presente appendice stabilisce i requisiti tecnici per i dati GNSS usati dalle unità elettroniche di bordo, compresi i protocolli che devono essere implementati per garantire la sicura e corretta trasmissione dei dati relativi alle informazioni sul posizionamento.

Gli articoli principali del regolamento (UE) n. 165/2014 alla base di tali requisiti sono: «Articolo 8 Registrazione della posizione del veicolo in determinati punti nel corso del periodo di lavoro giornaliero», «Articolo 10 Interfaccia coi sistemi di trasporto intelligenti» e «Articolo 11 Norme dettagliate per i tachigrafi intelligenti».

▼B

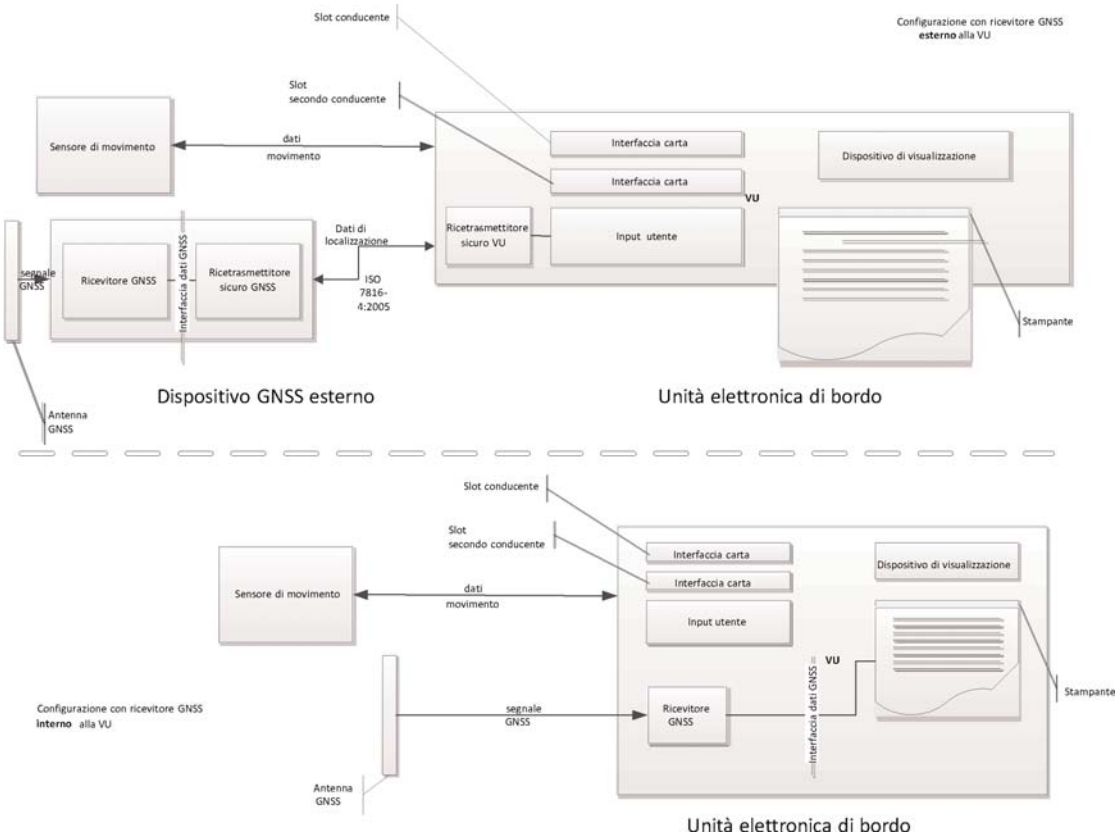
1.1. **Campo di applicazione**

GNS_1 L'unità elettronica di bordo deve raccogliere i dati di localizzazione da almeno un dispositivo GNSS a supporto dell'attuazione dell'articolo 8.

L'unità elettronica di bordo può comprendere o non comprendere un dispositivo GNSS esterno come illustrato nella Figure 1:

Figura 1

Configurazioni diverse per il ricevitore GNSS.



1.2. **Acronimi e simboli**

Nella presente appendice sono utilizzati i seguenti acronimi:

DOP	Diluizione della precisione
EGF	File elementare dispositivo GNSS
EGNOS	Servizio europeo di copertura per la navigazione geostazionaria
GNSS	Sistema globale di navigazione satellitare
GSA	GPS DOP e satelliti attivi
HDOP	Diluizione della precisione in orizzontale
ICD	Documento di controllo dell'interfaccia
NMEA	National Marine Electronics Association

▼B

PDOP Diluizione della precisione della posizione

RMC Recommended Minimum Specific (minimo specifico raccomandato)

SIS Segnale nello spazio

VDOP Diluizione della precisione in verticale

VU Unità elettronica di bordo

2. SPECIFICHE DEL RICEVITORE GNSS

Indipendentemente dalla configurazione del tachigrafo intelligente con o senza un dispositivo GNSS esterno, la trasmissione di informazioni precise e affidabili sul posizionamento è un elemento essenziale dell'efficacia di funzionamento del tachigrafo intelligente. È quindi opportuno prescriverne la compatibilità con i servizi forniti dai programmi Galileo e EGNOS (servizio europeo di copertura per la navigazione geostazionaria), come da regolamento (UE) n. 1285/2013 del Parlamento europeo e del Consiglio ([1]). Il sistema realizzato nel quadro del programma Galileo è un sistema globale indipendente di navigazione satellitare, mentre quello realizzato nel quadro del programma EGNOS è un sistema regionale di navigazione satellitare volto a migliorare la qualità del segnale del sistema di posizionamento globale (Global Positioning System — GPS).

GNS_2 I fabbricanti devono garantire che i ricevitori GNSS dei tachigrafi intelligenti siano compatibili con i servizi di posizionamento forniti dai sistemi Galileo e EGNOS. I fabbricanti possono inoltre optare per la compatibilità anche con ulteriori sistemi di navigazione satellitare.

GNS_3 Il ricevitore GNSS deve poter supportare l'autenticazione sul servizio aperto (Open Service) di Galileo quando tale servizio sarà fornito dal sistema Galileo col sostegno dei fabbricanti di ricevitori GNSS. Ai tachigrafi intelligenti immessi sul mercato prima che siano soddisfatte le precedenti condizioni e che non supportano l'autenticazione sul servizio aperto (Open Service) di Galileo non sarà tuttavia richiesto un adeguamento successivo (retrofitting).

3. FRASI NMEA

La presente sezione descrive le frasi NMEA usate nel funzionamento del tachigrafo intelligente. La presente sezione è valida per la configurazione del tachigrafo intelligente sia con che senza dispositivo GNSS esterno.

GNS_4 I dati di localizzazione si basano sulla frase NMEA *Recommended Minimum Specific (RMC) GNSS Data*, che contiene le informazioni sulla posizione (latitudine, longitudine), l'ora in formato UTC (oommss.ss) e la velocità al suolo in nodi, più altri valori.

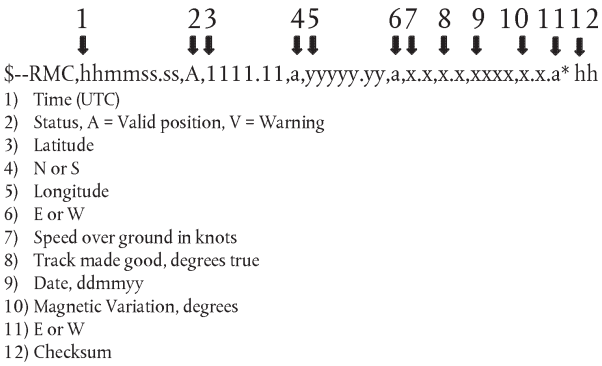
Il formato della frase RMC è il seguente (come da norma NMEA V4.1):

([1]) Regolamento (UE) n. 1285/2013 del Parlamento europeo e del Consiglio, dell'11 dicembre 2013, relativo all'attuazione e all'esercizio dei sistemi europei di radionavigazione via satellite e che abroga il regolamento (CE) n. 876/2002 del Consiglio e il regolamento (CE) n. 683/2008 del Parlamento europeo e del Consiglio (GU L 347 del 20.12.2013, pag. 1).

▼B

Figura 2

Struttura della frase RMC



Lo stato indica se il segnale GNSS è disponibile. Fino a che il valore dello stato non è impostato su A, i dati ricevuti (ad esempio sull'ora o sulla latitudine/longitudine) non possono essere usati per registrare la posizione del veicolo nella VU.

La risoluzione della posizione è basata sul formato della frase RMC di cui sopra. La prima parte dei campi 3) e 5) (i primi due numeri) è usata per rappresentare i gradi. La parte restante è usata per rappresentare i minuti con tre decimali. La risoluzione è quindi 1/1000 di minuto o 1/60000 di grado (poiché un minuto è 1/60 di un grado).

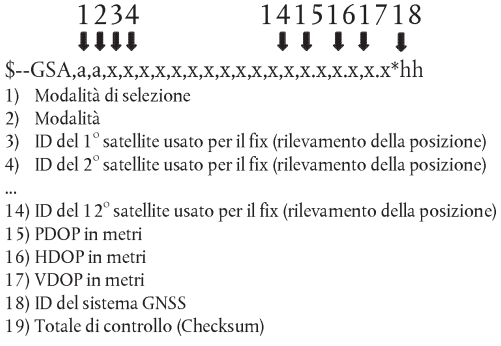
GNS_5 L'unità elettronica di bordo deve conservare nella propria banca dati le informazioni sulla posizione per latitudine e longitudine con una risoluzione di 1/10 di min o 1/600 di grado, come descritto nell'appendice 1 per il tipo GeoCoordinates.

Il comando GPS DOP e satelliti attivi (GSA) può essere usato dalla VU per determinare e registrare la disponibilità e la precisione del segnale. In particolare HDOP è usato per fornire un'indicazione circa il livello di precisione dei dati di localizzazione registrati (cfr. 4.2.2). La VU memorizzerà il valore dell'HDOP (Horizontal Dilution of Precision), calcolato come il valore HDOP minimo tra quelli raccolti sui sistemi GNSS disponibili.

L'identificativo del sistema GNSS (GNSS System Id) indica GPS, Glonass, Galileo, Beidou o il sistema di potenziamento basato su satelliti (Satellite-Based Augmentation System — SBAS).

Figura 3

Struttura della frase GSA



▼B

Dove la modalità 2) fornisce un'indicazione sulla disponibilità del fix: non disponibile (modalità=1) o disponibile in 2D (modalità=2) o disponibile in 3D (modalità=3).

GNS_6 La frase *GSA* deve essere memorizzata con il numero di registrazione '06'.

GNS_7 La dimensione massima delle frasi NMEA (ad esempio RMC, GSA o altre) che può essere usata per la definizione delle dimensioni del comando «read record» (leggi registrazione) è di 85 byte (cfr. Table 1).

4. UNITÀ ELETTRONICA DI BORDO CON DISPOSITIVO GNSS ESTERNO

4.1. **Configurazione**

4.1.1 *Componenti principali e interfacce*

In tale configurazione, il ricevitore GNSS è parte del dispositivo GNSS esterno.

GNS_8 Il dispositivo GNSS esterno deve essere alimentato con una specifica interfaccia del veicolo.

GNS_9 Il dispositivo GNSS esterno deve essere costituito dai seguenti elementi (cfr. Figure 4):

a) un ricevitore GNSS commerciale per fornire i dati sulla posizione attraverso l'interfaccia dati GNSS. Ad esempio l'interfaccia dati GNSS può essere conforme alla norma NMEA V4.10, con il ricevitore GNSS che funge da sorgente e trasmette frasi NMEA al ricetrasmettitore sicuro GNSS con una frequenza di 1 Hz per l'insieme predefinito di frasi NMEA, che devono comprendere almeno le frasi RMC e GSA. L'implementazione dell'interfaccia dati GNSS è una scelta dei fabbricanti dei dispositivi GNSS esterni;

b) una unità ricetrasmittente (ricetrasmettitore sicuro GNSS) compatibile con la norma ISO/IEC 7816-4:2013 (cfr. 4.2.1) per comunicare con l'unità elettronica di bordo e essere compatibile con l'interfaccia dati GNSS per il ricevitore GNSS. Tale unità è dotata di memoria per conservare i dati di identificazione del ricevitore GNSS e del dispositivo GNSS esterno;

c) un contenitore, con funzione di rilevamento delle manomissioni, che contenga sia il ricevitore GNSS che il ricetrasmettitore sicuro GNSS. La funzione di rilevamento delle manomissioni deve attuare le misure di protezione della sicurezza come richiesto nel profilo di protezione del tachigrafo intelligente;

d) un'antenna GNSS installata sul veicolo e collegata al ricevitore GNSS tramite il contenitore.

GNS_10 Il dispositivo GNSS esterno è dotato almeno delle seguenti interfacce esterne:

a) l'interfaccia per l'antenna GNSS installata sull'autocarro, se si utilizza un'antenna esterna;

b) l'interfaccia per l'unità elettronica di bordo.

GNS_11 Il ricetrasmettitore sicuro della VU è all'altro capo della comunicazione sicura con il ricetrasmettitore sicuro GNSS e deve essere compatibile con la norma ISO/IEC 7816-4:2013 per il collegamento al dispositivo GNSS esterno.

▼B

GNS_12 Per il livello fisico della comunicazione con il dispositivo GNSS esterno, l'unità elettronica di bordo deve essere compatibile con la norma ISO/IEC 7816-12:2005 o un'altra norma compatibile con ISO/IEC 7816-4:2013 (cfr. 4.2.1).

4.1.2 *Stato del dispositivo GNSS esterno alla fine della produzione*

GNS_13 All'uscita dalla fabbrica il dispositivo GNSS esterno deve conservare nella memoria non volatile del ricetrasmettitore sicuro GNSS i seguenti valori:

— la coppia di chiavi EGF_MA e il certificato corrispondente,

— il certificato MSCA_VU-EGF contenente la chiave pubblica MSCA_VU-EGF.PK da usare per la verifica del certificato EGF_MA,

— il certificato EUR contenente la chiave pubblica EUR.PK da usare per la verifica del certificato MSCA_VU-EGF,

— il certificato EUR il cui periodo di validità precede direttamente il periodo di validità del certificato EUR da usare per la verifica del certificato MSCA_VU-EGF, se presente,

— il certificato di collegamento che collega questi due certificati EUR, se presente,

— il numero di serie completo del dispositivo GNSS esterno,

— l'identificativo del sistema operativo del dispositivo GNSS,

— il numero di omologazione del dispositivo GNSS esterno,

— l'identificativo del componente di sicurezza del dispositivo GNSS esterno.

4.2. **Comunicazione tra il dispositivo GNSS esterno e l'unità elettronica di bordo**

4.2.1 *Protocollo di comunicazione*

GNS_14 Il protocollo di comunicazione tra il dispositivo GNSS esterno e l'unità elettronica di bordo deve essere compatibile con tre funzioni:

1. la raccolta e la distribuzione di dati GNSS (ad esempio posizione, ora, velocità),

2. la raccolta dei dati di configurazione del dispositivo GNSS esterno,

3. il protocollo di gestione a supporto di accoppiamento, autenticazione reciproca e accordo sulla chiave di sessione tra il dispositivo GNSS esterno e la VU.

GNS_15 Il protocollo di comunicazione deve essere basato sulla norma ISO/IEC 7816-4:2013 con il ricetrasmettitore sicuro della VU che svolge il ruolo di master e il ricetrasmettitore sicuro del GNSS che svolge il ruolo di slave. Il collegamento fisico tra il dispositivo GNSS esterno e l'unità elettronica di bordo si basa sulla norma ISO/IEC 7816-12:2005 o su un'altra norma compatibile con ISO/IEC 7816-4:2013.

▼B

GNS_16 I campi di lunghezza estesa non devono essere supportati nel protocollo di comunicazione.

GNS_17 Il protocollo di comunicazione di ISO 7816 (sia *-4:2013 che *-12:2005) tra il dispositivo GNSS esterno e la VU deve essere impostato su T=1.

GNS_18 Per quanto riguarda le funzioni di 1) raccolta e distribuzione dei dati GNSS, 2) raccolta dei dati di configurazione del dispositivo GNSS esterno e 3) protocollo di gestione, il ricetrasmettitore sicuro GNSS deve simulare una smart card, l'architettura del cui file system è composta da un file master (MF) e da un file directory (DF), con l'identificativo dell'applicazione specificato nell'appendice 1, capitolo 6.2 (‘FF 44 54 45 47 4D’) e con tre EF contenenti i certificati e un solo file elementare (EF.EGF) con l'identificativo uguale a ‘2F2F’ come illustrato nella Table 1.

GNS_19 Il ricetrasmettitore sicuro GNSS deve memorizzare i dati provenienti dal ricevitore GNSS e la configurazione nel file EF.EFG. Quest'ultimo è un file di registrazione lineare a lunghezza variabile con un identificativo uguale a ‘2F2F’ in formato esadecimale.

GNS_20 La memoria usata dal ricetrasmettitore sicuro GNSS per conservare i dati deve essere in grado di eseguire almeno 20 milioni di cicli di scrittura/lettura. A parte questo aspetto, la progettazione interna e l'implementazione del ricetrasmettitore sicuro GNSS è lasciata ai fabbricanti.

La mappatura tra i numeri di registrazione e i dati è illustrata nella Table 1. Da notare che vi sono quattro frasi GSA per i quattro sistemi satellitari e il sistema satellitare di potenziamento basato su satelliti (SBAS).

GNS_21 La struttura dei file è illustrata nella Table 1. Per le condizioni di accesso (ALW, NEV, SM-MAC) cfr. appendice 2, capitolo 3.5.

Tabella 1

Struttura dei file

		Condizioni di accesso		
File	ID del file	Lettura	Aggiornamento	Criptato
MF	3F00			
EF.ICC	0002	ALW	NEV (dalla VU)	N.
DF del dispositivo GNSS	0501	ALW	NEV	N.
EF EGF_MACertificate	C100	ALW	NEV	N.
EF CA_Certificate	C108	ALW	NEV	N.
EF Link_Certificate	C109	ALW	NEV	N.
EF.EGF	2F2F	SM-MAC	NEV (dalla VU)	N.

▼B

File / Elemento di dati	Registrazione n.	Dimensioni (in byte)		Valori standard
		Min.	Max.	
MF		552	1 031	
EF.ICC				
sensorGNSSSerialNumber		8	8	
DF del dispositivo GNSS		*612*	*1 023*	
EF EGF_MACertificate		*204*	*341*	
EGFCertificate		204	341	{00..00}
EF CA_Certificate		*204*	*341*	
MemberStateCertificate		204	341	{00..00}
EF Link_Certificate		*204*	*341*	
LinkCertificate		204	341	{00..00}
EF.EGF				
Frase NMEA RMC	'01'	85	85	
1[a] frase NMEA GSA	'02'	85	85	
2[a] frase NMEA GSA	'03'	85	85	
3[a] frase NMEA GSA	'04'	85	85	
4[a] frase NMEA GSA	'05'	85	85	
5[a] frase NMEA GSA	'06'	85	85	
Numero di serie completo del dispositivo GNSS esterno definito SensorGNSSSerialNumber nell'appendice 1.	'07'	8	8	
Identificativo del sistema operativo del ricetrasmettitore sicuro GNSS definito SensorOSIdentifier nell'appendice 1.	'08'	2	2	
Numero di omologazione del dispositivo GNSS esterno definito SensorExternalGNSSApprovalNumber nell'appendice 1.	'09'	16	16	
Identificativo del componente di sicurezza del dispositivo GNSS esterno definito SensorExternalGNSSSCIdentifier nell'appendice 1.	'10'	8	8	
RFU — Riservato per uso futuro	Da '11' a 'FD'			

4.2.2 *Trasferimento sicuro di dati GNSS*

GNS_22 Il trasferimento sicuro dei dati sulla posizione GNSS deve essere consentito solo alle seguenti condizioni:

1. il processo di accoppiamento è stato completato come descritto nell'appendice 11. Meccanismi comuni di sicurezza;

▼B

2. l'accordo sulla chiave di sessione e l'autenticazione reciproca tra la VU e il dispositivo GNSS esterno, anch'essi descritti nell'appendice 11. Meccanismi comuni di sicurezza, sono stati eseguiti periodicamente con la frequenza indicata.

GNS_23 Ogni T secondi, dove T è un valore inferiore o uguale a 10, a meno che non si verifichi l'accoppiamento o l'autenticazione reciproca e l'accordo sulla chiave di sessione, la VU richiede al dispositivo GNSS esterno le informazioni sulla posizione in base alle seguenti fasi:

1. la VU richiede i dati di localizzazione al dispositivo GNSS esterno insieme ai dati sulla diluizione della precisione (dalla frase NMEA GSA). Il ricetrasmettitore sicuro VU deve usare il comando SELECT e READ RECORD(S), conforme alla norma ISO/IEC 7816-4:2013, in modalità di sola autenticazione e con messaggistica sicura, come descritto nell'appendice 11, sezione 11.5, con l'identificativo del file "2F2F" e numero di registrazione uguale a "01" per la frase NMEA RMC e '02','03','04','05','06' per la frase NMEA GSA.

2. Gli ultimi dati di localizzazione ricevuti sono memorizzati nell'EF con identificativo '2F2F' e nei registri descritti nella Table 1 del ricetrasmettitore sicuro GNSS man mano che quest'ultimo riceve i dati NMEA con una frequenza di almeno 1 Hz dal ricevitore GNSS attraverso l'interfaccia dati GNSS.

3. Il ricetrasmettitore sicuro GNSS invia la risposta al ricetrasmettitore sicuro VU usando il messaggio di risposta APDU in modalità di sola autenticazione e con messaggistica sicura come descritto nell'appendice 11, punto 11.5.

4. Il ricetrasmettitore sicuro GNSS verifica l'autenticità e l'integrità della risposta ricevuta. Se la verifica ha esito positivo, i dati di localizzazione sono trasferiti al processore della VU attraverso l'interfaccia dati GNSS.

5. Il processore della VU verifica i dati ricevuti ed estrae le informazioni (ad esempio latitudine, longitudine, ora) dalla frase NMEA RMC. La frase NMEA RMC comprende le informazioni sulla validità della posizione. Se la posizione non è valida, i dati di localizzazione non sono ancora disponibili e non possono essere usati per registrare la posizione del veicolo. Se la posizione è valida, il processore della VU estrae anche i valori di HDOP dalle frasi NMEA GSA e calcola il valore medio sui sistemi satellitari disponibili (vale a dire quando il fix è disponibile).

6. Il processore della VU memorizza nella VU le informazioni ricevute e elaborate come latitudine, longitudine, ora e velocità nel formato definito nell'appendice 1. Dizionario di dati come GeoCoordinates, insieme al valore HDOP calcolato come il minimo dei valori HDOP raccolti dai sistemi GNSS disponibili.

▼B

4.2.3 *Struttura del comando Read Record*

La presente sezione descrive in dettaglio la struttura del comando Read Record (leggi registrazione). La messaggistica sicura (in modalità di sola autenticazione) è aggiunta come descritto nell'appendice 11. Meccanismi comuni di sicurezza.

GNS_24 Il comando deve essere compatibile con la messaggistica sicura in modalità di sola autenticazione, cfr. appendice 11.

GNS_25 Messaggio di comando

Byte	Lunghezza	Valore	Descrizione
CLA	1	'0Ch'	Richiesta messaggistica sicura
INS	1	'B2h'	Leggi registrazione
P1	1	'XXh'	Numero di registrazione ('00' si riferisce alla registrazione corrente)
P2	1	'04h'	Leggi la registrazione con il numero di registrazione indicato in P1
Le	1	'XXh'	Lunghezza dei dati attesa. Numero di byte da leggere

GNS_26 La registrazione cui si riferisce P1 diventa la registrazione corrente.

Byte	Lunghezza	Valore	Descrizione
#1-#X	X	'XX..XXh'	Dati letti
SW	2	'XXXXh'	Parole di stato (SW1, SW2)

— Se il comando ha esito positivo, il ricetrasmettitore sicuro GNSS risponde '**9000**'.

— Se il file corrente non è orientato alla registrazione (record oriented), il ricetrasmettitore sicuro GNSS risponde '**6981**'.

— Se il comando è usato con P1 = '00', ma non vi è alcun EF corrente, il ricetrasmettitore sicuro GNSS risponde '**6986**' (comando non consentito).

— Se la registrazione non è stata trovata, il ricetrasmettitore sicuro GNSS risponde '**6A 83**'.

— Se il dispositivo GNSS esterno ha rilevato una manomissione, devono essere inviate in risposta le parole di stato '**66 90**'.

GNS_27 Il ricetrasmettitore sicuro GNSS deve essere compatibile coi seguenti comandi del tachigrafo di seconda generazione specificati nell'appendice 2:

Comando	Riferimento
Select	Appendice 2, capitolo 3.5.1
Read Binary	Appendice 2, capitolo 3.5.2
Get Challenge	Appendice 2, capitolo 3.5.4
PSO: Verify Certificate	Appendice 2, capitolo 3.5.7
External Authenticate	Appendice 2, capitolo 3.5.9
General Authenticate	Appendice 2, capitolo 3.5.10
MSE:SET	Appendice 2, capitolo 3.5.11

▼B

4.3. **Accoppiamento, autenticazione reciproca e accordo sulla chiave di sessione del dispositivo GNSS esterno con l'unità elettronica di bordo**

L'accoppiamento, l'autenticazione reciproca e l'accordo sulla chiave di sessione del dispositivo GNSS esterno con l'unità elettronica di bordo sono descritti nell'appendice 11. Meccanismi comuni di sicurezza, capitolo 11.

4.4. **Gestione degli errori**

La presente sezione descrive in che modo sono gestite e registrate nella VU le potenziali condizioni di errore del dispositivo GNSS esterno.

4.4.1 *Errore di comunicazione con il dispositivo GNSS esterno*

GNS_28 Se non riesce a comunicare col dispositivo GNSS esterno cui è accoppiata per più di 20 minuti consecutivi, la VU deve generare e registrare al suo interno un'anomalia di tipo EventFaultType enum '53'H *External GNSS communication fault* (errore di comunicazione GNSS esterno) con la marcatura oraria (timestamp) dell'ora corrente. L'anomalia sarà generata solo se sono date le due condizioni seguenti: a) il tachigrafo intelligente non è in modalità taratura e b) il veicolo è in marcia. In questo contesto, un errore di comunicazione è attivato quando il ricetrasmettitore sicuro VU non riceve un messaggio di risposta dopo un messaggio di richiesta come descritto in 4.2.

4.4.2 *Violazione dell'integrità fisica del dispositivo GNSS esterno*

GNS_29 Se il dispositivo GNSS esterno è stato violato, il ricetrasmettitore sicuro GNSS deve cancelare tutta la sua memoria, incluso il materiale crittografico. Come descritto in GNS_25 e GNS_26, la VU deve rilevare le manomissioni se lo stato della risposta è '6690'. La VU deve quindi generare un'anomalia di tipo EventFaultType enum *'55'H Tamper detection of GNSS* (rilevamento manomissione GNSS).

4.4.3 *Assenza di informazioni sulla posizione provenienti dal ricevitore GNSS*

GNS_30 Se il ricetrasmettitore sicuro GNSS non riceve dati dal ricevitore GNSS per più di 3 ore consecutive, il ricetrasmettitore sicuro GNSS deve generare un messaggio di risposta al comando REAR RECORD con il numero di registrazione (RECORD number) uguale a '01' e un campo di dati di 12 byte impostati tutti su 0xFF. Alla ricezione del messaggio di risposta con tale valore del campo di dati, la VU deve generare e registrare un'anomalia di tipo EventFaultType enum '52'H *external GNSS receiver fault* (errore ricevitore GNSS esterno) con la marcatura oraria (timestamp) dell'ora corrente solo se sono date le due seguenti condizioni: a) il tachigrafo intelligente non è in modalità taratura e b) il veicolo è in marcia.

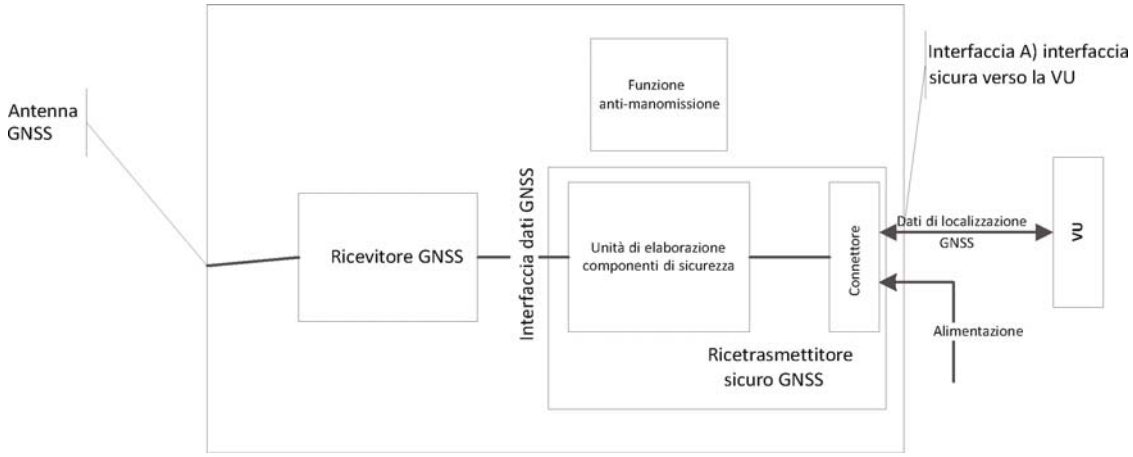
4.4.4 *Certificato del dispositivo GNSS esterno scaduto*

GNS_31 Se rileva che il certificato EGF usato per l'autenticazione reciproca non è più valido, la VU deve generare e registrare un guasto dell'apparecchio di registrazione di tipo EventFaultType enum *'56'H External GNSS facility certificate expired* (certificato del dispositivo GNSS esterno scaduto) con la marcatura oraria (timestamp) dell'ora corrente. La VU deve comunque continuare a usare i dati sulla posizione GNSS ricevuti.

▼B

Figura 4

Schema del dispositivo GNSS esterno



5. UNITÀ ELETTRONICA DI BORDO SENZA DISPOSITIVO GNSS ESTERNO

5.1. **Configurazione**

Nella presente configurazione, il ricevitore GNSS è all'interno dell'unità elettronica di bordo, come descritto nella Figure 1.

GNS_32 Il ricevitore GNSS deve fungere da sorgente e trasmettere le frasi NMEA al processore della VU, che deve fungere da ricevitore con una frequenza di 1/10 Hz o più per l'insieme predefinito di frasi NMEA, che deve includere almeno le frasi RMC e GSA.

GNS_33 Alla VU deve essere collegata un'antenna GNSS esterna installata sul veicolo o un'antenna GNSS interna.

5.2. **Gestione degli errori**

5.2.1 *Assenza di informazioni sulla posizione provenienti dal ricevitore GNSS*

GNS_34 Se non riceve dati dal ricevitore GNSS per più di 3 ore consecutive, la VU deve generare e registrare un'anomalia di tipo EventFaultType enum '51'H *Internal GNSS receiver fault* (errore ricevitore GNSS interno) con la marcatura oraria (timestamp) dell'ora corrente solo se sono date le due condizioni seguenti: a) il tachigrafo intelligente non è in modalità taratura e b) il veicolo è in marcia.

6. CONFLITTO DI ORARI DEL GNSS

Se la VU rileva una discrepanza di più di 1 minuto tra l'orario della funzione di misurazione dell'ora dell'unità elettronica di bordo e l'orario proveniente dal ricevitore GNSS, la VU registrerà un evento di tipo EventFaultType enum *'0B'H Time conflict (GNSS versus VU internal clock)* [conflitto di orari (tra GNSS e orologio interno della VU)]. Questa anomalia è registrata unitamente al valore dell'orologio interno dell'unità elettronica di bordo e accompagna un meccanismo automatico di regolazione dell'ora. Dopo che si è attivata un'anomalia «Conflitto di orari», la VU non verificherà la discrepanza di orario per le successive 12 ore. Questa anomalia non si attiva qualora nei precedenti 30 giorni non fosse rilevabile nessun segnale GNSS valido dal ricevitore GNSS. Tuttavia, quando le informazioni sulla posizione provenienti dal ricevitore GNSS sono nuovamente disponibili, deve avere luogo la regolazione automatica dell'ora.

▼B

7. CONFLITTO SUL MOVIMENTO DEL VEICOLO

GNS_35 La VU deve attivare e registrare un'anomalia «Conflitto sul movimento del veicolo» (cfr. requisito 84 del presente allegato) con una marcatura oraria (timestamp) dell'ora corrente, nel caso in cui le informazioni di movimento calcolate dal sensore di movimento contrastino con le informazioni di movimento calcolate dal ricevitore GNSS interno o dal dispositivo GNSS esterno. Al fine di individuare tali conflitti, deve essere usato il valore mediano delle differenze di velocità tra tali fonti, come specificato di seguito:

— al massimo ogni 10 secondi deve essere calcolato il valore assoluto della differenza tra la velocità del veicolo stimata dal GNSS e quella stimata dal sensore di movimento;

— tutti i valori calcolati in una finestra temporale che contiene gli ultimi cinque minuti di movimento devono essere usati per calcolare il valore mediano;

— il valore mediano deve essere calcolato come la media dell'80 % dei valori che restano dopo aver eliminato i più elevati in valori assoluti.

L'anomalia «Conflitto sul movimento del veicolo» deve essere attivata se il valore mediano supera i 10 Km/h per cinque minuti consecutivi di movimento del veicolo. Facoltativamente è possibile usare altre fonti indipendenti di rilevamento del movimento del veicolo, in modo da assicurare un rilevamento più affidabile delle manipolazioni del tachigrafo. (*Nota:* si applica l'uso del valore mediano sugli ultimi 5 minuti per attenuare il rischio di misurare valori erratici e transitori). Tale anomalia non deve essere attivata nelle seguenti condizioni: a) durante un attraversamento mediante traghetto/treno, b) quando le informazioni sulla posizione provenienti dal ricevitore GNSS non sono disponibili e c) in modalità taratura.

▼B

Appendice 13

INTERFACCIA ITS

INDCE

1. INTRODUZIONE

2. CAMPO DI APPLICAZIONE

2.1. Acronimi, definizioni e simboli

3. REGOLAMENTI E NORME DI RIFERIMENTO

4. PRINCIPI DI FUNZIONAMENTO DELL'INTERFACCIA

4.1. Precondizioni al trasferimento dati mediante l'interfaccia ITS

4.1.1 Dati forniti mediante l'interfaccia ITS

4.1.2 Contenuto dei dati

4.1.3 Applicazioni ITS

4.2. Tecnologia della comunicazione

4.3. Autorizzazione PIN

4.4. Formato del messaggio

4.5. Consenso del conducente

4.6. Recupero dati standard

4.7. Recupero dati personali

4.8. Recupero dei dati relativi ad anomalie e guasti

1. INTRODUZIONE

La presente appendice stabilisce le specifiche per la progettazione e le procedure da seguire per implementare l'interfaccia con i sistemi di trasporto intelligenti (ITS) conformemente all'articolo 10 del regolamento (UE) n. 165/2014 (*il regolamento*).

Il regolamento specifica che i tachigrafi dei veicoli possono essere muniti di interfacce standardizzate che consentono di usare i dati registrati o generati dal tachigrafo nel modo funzionamento, mediante un dispositivo esterno, a condizione che siano rispettate le seguenti condizioni:

a) l'interfaccia non pregiudica l'autenticità e l'integrità dei dati del tachigrafo;

b) l'interfaccia è conforme alle norme dettagliate di cui all'articolo 11 del regolamento;

c) il dispositivo esterno connesso all'interfaccia ha accesso ai dati personali, inclusi i dati relativi alla geolocalizzazione, solo previo consenso documentabile del conducente cui i dati si riferiscono.

2. CAMPO DI APPLICAZIONE

Il campo di applicazione della presente appendice specifica come le applicazioni situate su dispositivi esterni possano ottenere dati (*i dati*) da un tachigrafo mediante una connessione Bluetooth®.

I dati disponibili mediante quest'interfaccia sono descritti nell'allegato 1 del presente documento. Quest'interfaccia non impedisce l'applicazione di altre interfacce (ad es. tramite il bus CAN) per trasmettere i dati della VU ad altre unità di elaborazione del veicolo.

▼B

La presente appendice specifica:

— *i dati* disponibili mediante l'interfaccia ITS;

— il profilo Bluetooth® utilizzato per trasferire i dati;

— le procedure di richiesta e di trasferimento e la sequenza delle operazioni;

— il meccanismo di abbinamento tra il tachigrafo e il dispositivo esterno;

— il meccanismo di consenso disponibile per il conducente.

Per chiarezza, il presente allegato non specifica:

— la raccolta dei *dati* relativi al funzionamento e alla gestione all'interno della VU (che sarà specificata altrove nel *regolamento* oppure sarà una funzione della progettazione del prodotto);

— la forma di presentazione dei dati raccolti all'applicazione installata nel dispositivo esterno;

— le disposizioni sulla sicurezza dei dati superiore a quella fornita da Bluetooth® (ad esempio cifratura) per quanto riguarda il contenuto dei *dati* (che saranno specificate altrove nel *regolamento* [Appendice 10 Meccanismi comuni di sicurezza]);

— i protocolli Bluetooth® utilizzati dall'interfaccia ITS.

2.1. **Acronimi, definizioni e simboli**

Nella presente appendice sono utilizzati gli acronimi e le definizioni specifici che seguono:

la comunicazione	lo scambio di informazioni/dati tra un'unità master (i tachigrafi) e un'unità esterna mediante l'interfaccia ITS per via Bluetooth®.
i dati	gli insiemi di dati di cui all'allegato 1.
il regolamento	regolamento (UE) n. 165/2014 del Parlamento europeo e del Consiglio, del 4 febbraio 2014, relativo ai tachigrafi nel settore dei trasporti su strada, che abroga il regolamento (CEE) n. 3821/85 del Consiglio relativo all'apparecchio di controllo nel settore dei trasporti su strada e modifica il regolamento (CE) n. 561/2006 del Parlamento europeo e del Consiglio relativo all'armonizzazione di alcune disposizioni in materia sociale nel settore dei trasporti su strada
BR	Basic Rate (velocità di base di trasmissione dei dati)
EDR	Enhanced Data Rate (velocità di trasmissione dati potenziata)
GNSS	Global Navigation Satellite System (sistema globale di navigazione satellitare)
IRK	Identity Resolution Key (chiave di risoluzione dell'identità)
ITS	Intelligent Transport System (sistema di trasporto intelligente)
LE	Low Energy (bassa energia)
PIN	Personal Identification Number (numero di identificazione personale)
PUC	Personal Unblocking Code (codice di sblocco personale)
SID	Service Identifier (identificativo del servizio)
SPP	Serial Port Profile (profilo della porta seriale)

▼B

SSP	Secure Simple Pairing (abbinamento semplice e sicuro)
TRTP	Transfer Request Parameter (parametro di richiesta di trasferimento)
TREP	Transfer Response Parameter (parametro di risposta di trasferimento)
VU	Vehicle Unit (unità elettronica di bordo)

3. REGOLAMENTI E NORME DI RIFERIMENTO

La specifica definita nella presente appendice fa riferimento a e dipende dai regolamenti e dalle norme seguenti nella loro interezza o in parte. Le clausole della presente appendice indicano le norme pertinenti o le clausole pertinenti delle norme. In caso di qualsiasi contraddizione prevalgono le clausole della presente appendice.

Qui di seguito sono elencati i regolamenti e le norme cui fa riferimento la presente appendice:

— Regolamento (UE) n. 165/2014 del Parlamento europeo e del Consiglio, del 4 febbraio 2014, relativo ai tachigrafi nel settore dei trasporti su strada, che abroga il regolamento (CEE) n. 3821/85 del Consiglio relativo all'apparecchio di controllo nel settore dei trasporti su strada e modifica il regolamento (CE) n. 561/2006 del Parlamento europeo e del Consiglio relativo all'armonizzazione di alcune disposizioni in materia sociale nel settore dei trasporti su strada

— Regolamento (CE) n. 561/2006 del Parlamento europeo e del Consiglio, del 15 marzo 2006, relativo all'armonizzazione di alcune disposizioni in materia sociale nel settore dei trasporti su strada e che modifica i regolamenti del Consiglio (CEE) n. 3821/85 e (CE) n. 2135/98 e abroga il regolamento (CEE) n. 3820/85 del Consiglio

— ISO 16844 — 4: Road vehicles — Tachograph systems — Part 4: Can interface (Veicoli stradali — Sistemi tachigrafici — Parte 4: Interfaccia Can)

— ISO 16844 — 7: Road vehicles — Tachograph systems — Part 7: Parameters (Veicoli stradali — Sistemi tachigrafici — Parte 7: Parametri)

— Bluetooth® — Serial Port Profile — V1.2 (profilo della porta seriale — V1.2)

— Bluetooth® — Core Version 4.2 (versione di base 4.2)

— Protocollo NMEA 0183 V4.1

4. PRINCIPI DI FUNZIONAMENTO DELL'INTERFACCIA

4.1. **Precondizioni al trasferimento dati mediante l'interfaccia ITS**

È compito della VU mantenere aggiornati i dati da archiviare al suo interno, senza interventi dell'interfaccia ITS. I mezzi per conseguire questo obiettivo sono interni alla VU. Essi non sono illustrati nella presente appendice ma vengono specificati altrove nel regolamento.

4.1.1 *Dati forniti mediante l'interfaccia ITS*

È compito della VU aggiornare i dati che saranno messi a disposizione mediante l'interfaccia ITS a una frequenza determinata nell'ambito delle procedure VU, senza interventi dell'interfaccia ITS. I dati della VU vanno utilizzati come base per popolare e aggiornare i *dati*; i mezzi per raggiungere tale obiettivo sono specificati altrove nel *regolamento*. Se non esiste tale specifica, tali mezzi sono una funzione della progettazione del prodotto e non vengono specificati nella presente appendice.

▼B

4.1.2 *Contenuto dei dati*

Il contenuto dei *dati* deve essere conforme a quanto specificato nell'allegato 1 della presente appendice.

4.1.3 *Applicazioni ITS*

Le applicazioni ITS useranno i dati messi a disposizione mediante l'interfaccia ITS per, ad esempio, ottimizzare la gestione delle attività del conducente rispettando nel contempo il regolamento, individuare possibili guasti del tachigrafo o utilizzare i dati GNSS. Le specifiche delle applicazioni non rientrano nel campo di applicazione della presente appendice.

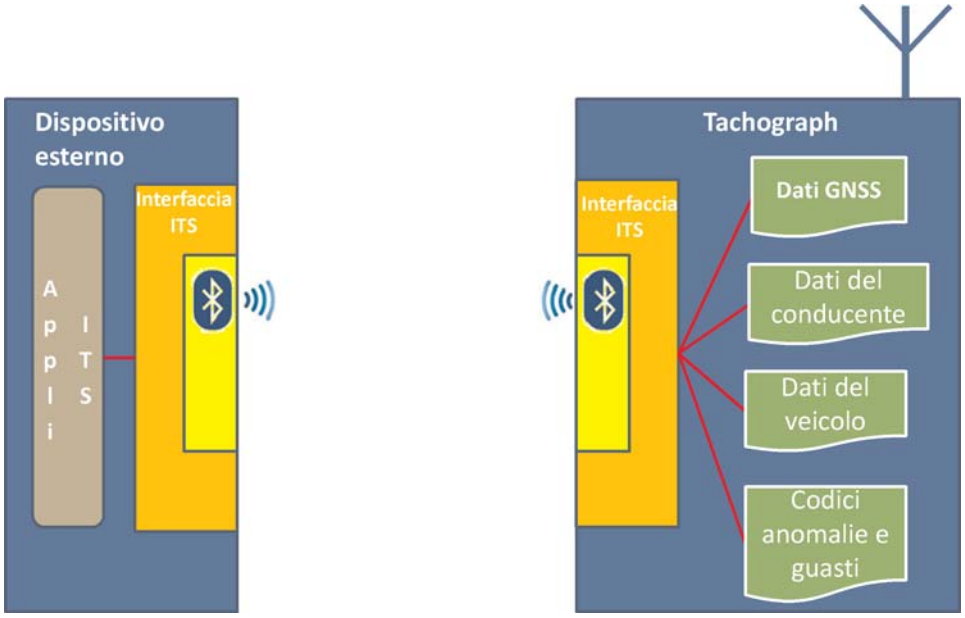
4.2. **Tecnologia della comunicazione**

Lo scambio di *dati* mediante l'interfaccia ITS deve avvenire mediante un'interfaccia Bluetooth® compatibile con la versione 4.2 o più recente. Il Bluetooth® funziona nella banda Industriale, Scientifica e Medica (ISM) senza licenza a 2,4 — 2,485 GHz. Il Bluetooth® 4.2 offre meccanismi migliorati per la privacy e la sicurezza ed aumenta la velocità e l'affidabilità dei trasferimenti di dati. Ai fini della presente specifica viene utilizzato il Bluetooth®, radio classe 2, con un campo fino a 10 metri. Ulteriori informazioni su Bluetooth® 4.2 sono disponibili all'indirizzo www.bluetooth.com (https://www.bluetooth.org/en-us/specification/adopted-specifications?_ga=1.215147412.2083380574.1435305676).

La comunicazione va stabilita con il dispositivo di comunicazione dopo il completamento di una procedura di abbinamento da parte di un dispositivo autorizzato. Poiché Bluetooth® utilizza un modello master/slave per controllare quando e dove i dispositivi possono inviare dati, il tachigrafo avrà il ruolo di master mentre il dispositivo quello di slave.

Quando un dispositivo esterno entra nel raggio della VU per la prima volta può iniziare il processo di abbinamento Bluetooth® (cfr. anche allegato 2). I dispositivi condividono i propri indirizzi, nomi, profili e chiave segreta comune (common secret key) che consente l'abbinamento automatico in futuro. In seguito il dispositivo esterno è considerato affidabile ed è in grado di iniziare le richieste di trasferimento dati dal tachigrafo. Non si prevede di aggiungere meccanismi di cifratura supplementari rispetto a quelli forniti da Bluetooth®. Tuttavia se sono necessari ulteriori meccanismi di sicurezza, essi saranno aggiunti conformemente ai meccanismi comuni di sicurezza di cui all'appendice 10.

Il principio generale di comunicazione è illustrato nella figura seguente:



▼B

Si deve utilizzare il profilo SPP (Serial Port Profile) di Bluetooth® per trasferire dati dalla VU al dispositivo esterno.

4.3. **Autorizzazione PIN**

Per motivi di sicurezza la VU deve applicare un sistema di autorizzazione con codice PIN separato rispetto all'abbinamento Bluetooth. Ogni VU deve essere in grado di generare codici PIN ai fini dell'autenticazione composti da almeno 4 cifre. Ogni volta che un dispositivo esterno si abbina alla VU deve fornire il codice PIN corretto prima di ricevere dati.

L'inserimento corretto del PIN deve comportare l'inclusione del dispositivo in una whitelist (elenco di dispositivi autorizzati). Tale whitelist deve essere in grado di memorizzare almeno 64 dispositivi abbinati alla VU in questione.

Se viene inserito il codice PIN errato per tre volte consecutive, il dispositivo deve essere incluso temporaneamente nella blacklist (elenco dei dispositivi non autorizzati). Se il dispositivo è inserito in tale blacklist, ogni altro tentativo da parte del dispositivo sarà rifiutato. Se viene inserito il codice PIN errato per altre tre volte consecutive, il dispositivo viene escluso per un periodo di tempo più lungo (cfr. tabella 1). L'inserimento corretto del PIN deve riportare la durata dell'esclusione e il numero di tentativi ai valori iniziali. Nella figura 1 dell'allegato 2 è illustrato il diagramma della sequenza di un tentativo di convalida del PIN.

Tabella 1

Durata dell'esclusione in base al numero di errori consecutivi di inserimento del codice PIN

Numero di errori consecutivi	Durata dell'esclusione
3	30 secondi
6	5 minuti
9	1 ora
12	24 ore
15	Permanente

Se viene inserito il codice PIN errato per quindici volte (5 × 3) consecutive, l'unità ITS deve essere inserita in una blacklist permanente. La cancellazione dalla blacklist permanente può avvenire soltanto mediante l'inserimento corretto del PUC.

Il PUC deve essere composto di 8 cifre e va fornito dal fabbricante con la VU. Se viene inserito il codice PUC errato per dieci volte consecutive, l'unità ITS sarà inserita nella blacklist in modo irrevocabile.

Anche se il fabbricante offrisse la possibilità di modificare il codice PIN direttamente mediante la VU, il codice PUC non deve essere modificabile. Se possibile, la modifica del codice PIN deve comportare l'inserimento dell'attuale codice PIN direttamente nella VU.

Inoltre qualsiasi dispositivo incluso nella whitelist deve rimanervi finché non viene rimosso manualmente dall'utente (ad es. mediante l'interfaccia uomo-macchina della VU o altri mezzi). In questo modo le unità ITS perse o rubate possono essere rimosse dalla whitelist. Inoltre ogni unità ITS che lascia il campo di connessione Bluetooth per oltre 24 ore sarà automaticamente rimosso dalla whitelist della VU e dovrà fornire nuovamente il codice PIN corretto per stabilire la connessione.

▼B

Non è definito il formato dei messaggi tra l'interfaccia VU e la VU e quindi è a discrezione del fabbricante. Detto fabbricante dovrà tuttavia garantire il rispetto del formato dei messaggi tra l'unità ITS e l'interfaccia VU (cfr. specifiche ASN.1).

Per ogni richiesta di dati devono essere verificate le credenziali del richiedente prima di procedere all'elaborazione. Nella figura 2 dell'allegato 2 è illustrato il diagramma della sequenza della procedura. Qualsiasi dispositivo elencato nella blacklist deve essere automaticamente rifiutato; qualsiasi dispositivo non elencato nella whitelist o nella blacklist deve ricevere una richiesta di PIN prima di reinviare la richiesta di dati.

4.4. **Formato del messaggio**

Tutti i messaggi scambiati tra l'unità ITS e l'interfaccia VU devono essere formattati secondo una struttura composta da tre parti: intestazione, costituita da un target byte (TGT), un source byte (SRC) e un byte di lunghezza (LEN);

campo di dati, costituito da un byte identificativo del servizio (SID) e una quantità variabile di dati (max 255);

byte del totale di controllo dato dalla somma su 1 byte, modulo 256, di tutti i byte del messaggio, escluso il CS stesso.

Il messaggio deve essere Big Endian.

Tabella 2

Formato generale del messaggio

Intestazione			Campo dati					Totale di controllo
TGT	SRC	LEN	SID	TRTP	CC	CM	DATI	CS
3 byte			Max 255 byte					1 byte

Intestazione

TGT e SRC: ID dei dispositivi target (TGT) e source (SRC) del messaggio. L'interfaccia VU deve avere l'ID preimpostato su “EE”. Questo ID non può essere modificato. L'unità ITS deve usare l'ID preimpostato “A0” per il primo messaggio della sessione di comunicazione. L'interfaccia VU deve assegnare in seguito un ID unico all'unità ITS e informarla di questo ID per i futuri messaggi della sessione.

Il LEN byte deve tenere conto solo della parte “DATI” del campo dati (cfr. tabella 2); i primi 4 byte sono impliciti.

L'interfaccia VU deve confermare l'autenticità del mittente del messaggio facendo un controllo incrociato del proprio elenco ID con i dati Bluetooth e controllando l'unità ITS elencata all'ID fornito e in quel momento nel campo di connessione Bluetooth.

Campo dati

Oltre al SID, il campo dati deve comprendere altri parametri: un parametro di richiesta di trasferimento (TRTP) e byte contatori.

▼B

Se i dati da trasferire sono troppo lunghi rispetto allo spazio disponibile in un messaggio, saranno suddivisi in diversi sottomessaggi. Ogni sottomessaggio deve avere la stessa intestazione e SID, ma comprendere un contatore da 2 byte, un contatore corrente (Counter Current (CC)) e un contatore massimo (Counter Max (CM)) per indicare il numero del sottomessaggio. Per abilitare la verifica degli errori e interrompere la trasmissione dati il dispositivo che riceve i dati conferma tutti i sottomessaggi. Il dispositivo che riceve i dati può: accettare un sottomessaggio, chiedere che sia ritrasmesso, richiedere al dispositivo che ha inviato il messaggio di ricominciare o interrompere la trasmissione.

Se non sono usati, a CC e CM va assegnato il valore 0xFF.

Ad esempio, il seguente messaggio:

INTESTAZIONE	SID	TRTP	CC	CM	DATI	CS
3 byte	Lunghezza superiore a 255 byte					1 byte

deve essere trasmesso come:

INTESTAZIONE	SID	TRTP	01	n	DATI	CS
3 byte	255 byte					1 byte

INTESTAZIONE	SID	TRTP	02	n	DATI	CS
3 byte	255 byte					1 byte

…

INTESTAZIONE	SID	TRTP	N	N	DATI	CS
3 byte	Max 255 byte					1 byte

La tabella 3 comprende i messaggi che la VU e l'unità ITS potranno scambiarsi. Il contenuto di ogni parametro è esadecimale. Per motivi di chiarezza CC e CM non sono illustrati nella tabella; cfr. sopra per il formato completo.

Tabella 3

Contenuto dettagliato del messaggio

Messaggio	Intestazione			DATI			Totale di controllo
	TGT	SRC	LEN	SID	TRTP	DATI	
RequestPIN	*ITSID*	EE	00	01	FF		
SendITSID	*ITSID*	EE	01	02	FF	*ITSID*	
SendPIN	EE	*ITSID*	04	03	FF	4*INTEGER (0..9)	
PairingResult	*ITSID*	EE	01	04	FF	BOOLEAN (T/F)	
SendPUC	EE	*ITSID*	08	05	FF	8*INTEGER (0..9)	

▼B

Messaggio	Intestazione			DATI			Totale di controllo
	TGT	SRC	LEN	SID	TRTP	DATI	
BanLiftingResult	*ITSID*	EE	01	06	FF	BOOLEAN (T/F)	
RequestRejected	*ITSID*	EE	08	07	FF	Ora	
RequestData							
standardTachData	EE	*ITSID*	01	08	01		
personalTachData	EE	*ITSID*	01	08	02		
gnssData	EE	*ITSID*	01	08	03		
standardEventData	EE	*ITSID*	01	08	04		
personalEventData	EE	*ITSID*	01	08	05		
standardFaultData	EE	*ITSID*	01	08	06		
manufacturerData	EE	*ITSID*	01	08	07		
ResquestAccepted	*ITSID*	EE	Len	09	TREP	Dati	
DataUnavailable							
Dati non disponibili	*ITSID*	EE	02	0A	TREP	10	
Dati personali non condivisi	*ITSID*	EE	02	0A	TREP	11	
NegativeAnswer							
Rifiuto generico	*ITSID*	EE	02	0B	SID Req	10	
Servizio non supportato	*ITSID*	EE	02	0B	SID Req	11	
Sottofunzione non supportata	*ITSID*	EE	02	0B	SID Req	12	
Lunghezza del messaggio non corretta	*ITSID*	EE	02	0B	SID Req	13	
Condizioni non soddisfatte o errore nella sequenza di richiesta	*ITSID*	EE	02	0B	SID Req	22	
Richiesta fuori valori limite	*ITSID*	EE	02	0B	SID Req	31	
Risposta pendente	*ITSID*	EE	02	0B	SID Req	78	
ITSID non corrispondente	*ITSID*	EE	02	0B	SID Req	FC	
ITSID non trovato	*ITSID*	EE	02	0B	SID Req	FB	

RequestPIN (SID 01)

Questo messaggio è emesso dall'interfaccia VU se un'unità ITS non inclusa nella blacklist ma nemmeno nella whitelist invia richieste di dati.

▼B

SendITSID (SID 02)

Questo messaggio è emesso dall'interfaccia VU quando un nuovo dispositivo invia una richiesta. Questo dispositivo deve usare il valore preimpostato "A0" per l'ID prima di ricevere un ID unico per la sessione di comunicazione.

SendPIN (SID 03)

Questo messaggio è emesso dall'unità ITS che deve essere inclusa nella whitelist dell'interfaccia VU. Il contenuto di questo messaggio è un codice di 4 numeri interi (INTEGER) tra 0 e 9.

PairingResult (SID 04)

Questo messaggio è emesso dall'interfaccia VU per informare l'unità ITS se il codice PIN inviato è corretto. Il contenuto di questo messaggio deve essere un BOOLEAN con il valore «True» se il codice PIN è corretto o «False» se è errato.

SendPUC (SID 05)

Questo messaggio è emesso dall'unità ITS per revocare l'inclusione nella blacklist dell'interfaccia VU. Il contenuto di questo messaggio è un codice di 8 numeri interi (INTEGER) tra 0 e 9.

BanLiftingResult (SID 06)

Questo messaggio è emesso dall'interfaccia VU per informare l'unità ITS se il codice PUC inviato era corretto. Il contenuto di questo messaggio deve essere un BOOLEAN con il valore «True» se il codice PUC è corretto o «False» se è errato.

RequestRejected (SID 07)

Questo messaggio è emesso dall'interfaccia VU in risposta a un messaggio inviato da un'unità ITS inclusa nella blacklist, ad eccezione del messaggio «SendPUC». Il messaggio deve contenere il tempo rimanente della permanenza dell'unità ITS nella blacklist conformemente alla sequenza del formato «Ora» di cui all'allegato 3.

RequestData (SID 08)

Questo messaggio per l'accesso ai dati è emesso dall'unità ITS. Un parametro di richiesta di trasferimento (TRTP) indica il tipo di dati richiesti. Vi sono diversi tipi di dati:

— standardTachData (TRTP 01): dati disponibili dal tachigrafo e classificati come non personali.

— personalTachData (TRTP 02): dati disponibili dal tachigrafo e classificati come personali.

— gnssData (TRTP 03): dati GNSS che sono sempre personali.

— standardEventData (TRTP 04): dati relativi alle anomalie registrati e classificati come non personali.

— personalEventData (TRTP 05): dati relativi alle anomalie registrati e classificati come personali.

— standardFaultData (TRTP 06): errori registrati e classificati come non personali.

— manufacturerData (TRTP 07): dati messi a disposizione dal fabbricante.

▼B

Cfr. allegato 3 della presente appendice per ulteriori informazioni sul contenuto di ciascun tipo di dati.

Cfr. appendice 12 per ulteriori informazioni sul formato e sul contenuto dei dati GNSS.

Cfr. allegati IB e IC per ulteriori informazioni sui codici dei dati delle anomalie e sui guasti.

ResquestAccepted (SID 09)

Questo messaggio è emesso dall'interfaccia VU se il messaggio «RequestData» inviato da un'unità ITS è stato accettato. Questo messaggio contiene un TREP da 1 byte, che è il byte TRTP del messaggio associato RequestData, e tutti i dati del tipo richiesto.

DataUnavailable (SID 0A)

Questo messaggio è emesso dall'interfaccia VU se, per un motivo specifico, i dati richiesti non sono disponibili per l'invio a un'unità ITS inclusa nella whitelist. Il messaggio contiene un TREP da 1 byte, che è il TRTP dei dati richiesti e un codice di errore da 1 byte specificato nella tabella 3. Sono disponibili i codici seguenti:

— Dati non disponibili (10): l'interfaccia VU non può accedere ai dati VU per motivi non specificati.

— Dati personali non condivisi (11): l'unità ITS tenta di accedere a dati personali che non sono condivisi.

NegativeAnswer (SID 0B)

Questi messaggi sono emessi dall'interfaccia VU se una richiesta non può essere soddisfatta per un motivo diverso dalla non disponibilità dei dati. Tipicamente, ma non esclusivamente, questi messaggi sono il risultato di un formato scorretto della richiesta (lunghezza, SID, ITSID…). Il TRTP nel campo dati contiene il SID della richiesta. Il campo dati contiene un codice che identifica il motivo della risposta negativa. Sono disponibili i seguenti codici:

— Rifiuto generico (codice: 10)

— L'azione non può essere eseguita per un motivo che non è citato sotto o nella sezione (Enter *DataUnavailable* section number).

— Servizio non supportato (codice: 11)

— Mancata comprensione del SID relativo alla richiesta.

— Sottofunzione non supportata (codice: 12)

— Mancata comprensione del TRTP relativo alla richiesta. Ad esempio, può essere mancante o al di fuori degli intervalli dei valori accettati.

— Lunghezza del messaggio non corretta (codice: 13)

— La lunghezza del messaggio ricevuto è errata (non corrispondenza tra il LEN byte e la lunghezza effettiva del messaggio).

— Condizioni non soddisfatte o errore nella sequenza di richiesta (codice: 22)

— Il servizio richiesto non è attivo o la sequenza dei messaggi di richiesta non è corretta.

— Richiesta fuori valori limite (codice: 33)

▼B

— Il parametro indicato (specifico campo dei dati) non è valido.

— Risposta pendente (codice: 78)

— L'azione richiesta non può essere completata nel tempo previsto e la VU non è pronta per accettare un'altra richiesta.

— *ITSID* Non corrispondenza (codice: FB)

— L'SRC *ITSID* non corrisponde al dispositivo associato dopo il raffronto con le informazioni Bluetooth.

— *ITSID* Non trovato (codice: FC)

— L'SRC *ITSID* non è associato ad alcun dispositivo.

Le righe da 1 a 72 (**FormatMessageModule**) del codice ASN.1 nell'allegato 3 indicano il formato dei messaggi descritto nella tabella 3. Ulteriori informazioni sul contenuto dei messaggi sono disponibili qui di seguito.

4.5. **Consenso del conducente**

Tutti i dati disponibili sono classificati come standard o personali. I dati personali devono essere accessibili solo se il conducente dà il proprio consenso e quindi accetta che i propri dati personali connessi al tachigrafo siano trasmessi ad applicazioni terze.

Il consenso del conducente è dato quando, all'atto del primo inserimento di una carta del conducente o dell'officina sconosciuta all'unità elettronica di bordo, il titolare della carta è invitato a dare il proprio consenso alla trasmissione di dati personali connessa al tachigrafo tramite l'interfaccia ITS opzionale. (cfr. anche allegato I C, punto 3.6.2).

Lo stato del consenso (abilitato/disabilitato) è registrato nella memoria del tachigrafo.

Nel caso di più conducenti, solo i dati personali relativi ai conducenti che hanno dato il loro consenso saranno condivisi con l'interfaccia ITS. Ad esempio, se vi sono due conducenti nel veicolo e solo il primo conducente ha acconsentito di condividere i propri dati personali, i dati personali concernenti il secondo conducente non saranno condivisi.

4.6. **Recupero dati standard**

La figura 3 dell'allegato 2 illustra i diagrammi della sequenza di una richiesta valida inviata dall'unità ITS per accedere ai dati standard. Se l'unità ITS è correttamente inserita nella whitelist e non richiede dati personali, non è necessaria un'ulteriore verifica. Nei diagrammi è indicato che è già stata seguita la procedura corretta illustrata nella figura 2 dell'allegato 2. Essi possono essere considerati equivalenti alla casella grigia *REQUEST TREATMENT* di cui alla figura 2.

Tra i dati disponibili sono considerati standard i dati seguenti:

— standardTachData (TRTP 01)

— StandardEventData (TRTP 04)

— standardFaultData (TRTP 06)

4.7. **Recupero dati personali**

Nella figura 4 dell'allegato 2 è illustrato il diagramma della sequenza della procedura per l'elaborazione di una richiesta di dati personali. Come indicato sopra, l'interfaccia VU deve inviare dati personali solo se il conducente ha dato esplicitamente il proprio consenso (cfr. anche punto 4.5). In caso contrario la richiesta deve essere automaticamente rifiutata.

▼B

Tra i dati disponibili, sono considerati personali:

— personalTachData (TRTP 02)

— gnssData (TRTP 03)

— personalEventData (TRTP 05)

— manufacturerData (TRTP 07)

4.8. **Recupero dei dati relativi ad anomalie e guasti**

Le unità ITS devono essere in grado di richiedere dati relativi alle anomalie contenenti l'elenco di tutte le anomalie non previste. Tali dati sono considerati standard o personali (cfr. allegato 3). Il contenuto di ogni anomalia è conforme alla documentazione di cui all'allegato 1 della presente appendice.

▼B

ALLEGATO 1

ELENCO DEI DATI DISPONIBILI MEDIANTE L'INTERFACCIA ITS

Dati	Fonte	►C2 Classificazione dei dati (personale/non personale) ◄
VehicleIdentificationNumber	Unità elettronica di bordo	**non personale**
CalibrationDate	Unità elettronica di bordo	**non personale**
TachographVehicleSpeed speed instant t	Unità elettronica di bordo	personale
Driver1WorkingState Selector driver	Unità elettronica di bordo	personale
Driver2WorkingState	Unità elettronica di bordo	personale
DriveRecognize Speed Threshold detected	Unità elettronica di bordo	**non personale**
Driver1TimeRelatedStates Weekly day time	Carta del conducente	personale
Driver2TimeRelatedStates	Carta del conducente	personale
DriverCardDriver1	Unità elettronica di bordo	**non personale**
DriverCardDriver2	Unità elettronica di bordo	**non personale**
OverSpeed	Unità elettronica di bordo	personale
TimeDate	Unità elettronica di bordo	**non personale**
HighResolutionTotalVehicleDistance	Unità elettronica di bordo	**non personale**
ServiceComponentIdentification	Unità elettronica di bordo	**non personale**
ServiceDelayCalendarTimeBased	Unità elettronica di bordo	**non personale**
Driver1Identification	Carta del conducente	personale
Driver2Identification	Carta del conducente	personale
NextCalibrationDate	Unità elettronica di bordo	**non personale**
Driver1ContinuousDrivingTime	Carta del conducente	personale
Driver2ContinuousDrivingTime	Carta del conducente	personale
Driver1CumulativeBreakTime	Carta del conducente	personale
Driver2CumulativeBreakTime	Carta del conducente	personale
Driver1CurrentDurationOfSelectedActivity	Carta del conducente	personale
Driver2CurrentDurationOfSelectedActivity	Carta del conducente	personale
SpeedAuthorised	Unità elettronica di bordo	**non personale**
TachographCardSlot1	Carta del conducente	**non personale**
TachographCardSlot2	Carta del conducente	**non personale**
Driver1Name	Carta del conducente	personale
Driver2Name	Carta del conducente	personale

▼B

Dati	Fonte	►C2 Classificazione dei dati (personale/non personale) ◄
OutOfScopeCondition	Unità elettronica di bordo	**non personale**
ModeOfOperation	Unità elettronica di bordo	**non personale**
Driver1CumulatedDrivingTimePreviousAndCurrentWeek	Carta del conducente	personale
Driver2CumulatedDrivingTimePreviousAndCurrentWeek	Carta del conducente	personale
EngineSpeed	Unità elettronica di bordo	personale
RegisteringMemberState	Unità elettronica di bordo	**non personale**
VehicleRegistrationNumber	Unità elettronica di bordo	**non personale**
Driver1EndOfLastDailyRestPeriod	Carta del conducente	personale
Driver2EndOfLastDailyRestPeriod	Carta del conducente	personale
Driver1EndOfLastWeeklyRestPeriod	Carta del conducente	personale
Driver2EndOfLastWeeklyRestPeriod	Carta del conducente	personale
Driver1EndOfSecondLastWeeklyRestPeriod	Carta del conducente	personale
Driver2EndOfSecondLastWeeklyRestPeriod	Carta del conducente	personale
Driver1CurrentDailyDrivingTime	Carta del conducente	personale
Driver2CurrentDailyDrivingTime	Carta del conducente	personale
Driver1CurrentWeeklyDrivingTime	Carta del conducente	personale
Driver2CurrentWeeklyDrivingTime	Carta del conducente	personale
Driver1TimeLeftUntilNewDailyRestPeriod	Carta del conducente	personale
Driver2TimeLeftUntilNewDailyRestPeriod	Carta del conducente	personale
Driver1CardExpiryDate	Carta del conducente	personale
Driver2CardExpiryDate	Carta del conducente	personale
Driver1CardNextMandatoryDownloadDate	Carta del conducente	personale
Driver2CardNextMandatoryDownloadDate	Carta del conducente	personale
TachographNextMandatoryDownloadDate	Unità elettronica di bordo	**non personale**
Driver1TimeLeftUntilNewWeeklyRestPeriod	Carta del conducente	personale
Driver2TimeLeftUntilNewWeeklyRestPeriod	Carta del conducente	personale
Driver1NumberOfTimes9hDailyDrivingTimesExceeded	Carta del conducente	personale
Driver2NumberOfTimes9hDailyDrivingTimesExceeced	Carta del conducente	personale

▼B

Dati	Fonte	►C2 Classificazione dei dati (personale/non personale) ◄
Driver1CumulativeUninterruptedRestTime	Carta del conducente	personale
Driver2CumulativeUninterruptedRestTime	Carta del conducente	personale
Driver1MinimumDailyRest	Carta del conducente	personale
Driver2MinimumDailyRest	Carta del conducente	personale
Driver1MinimumWeeklyRest	Carta del conducente	personale
Driver2MinimumWeeklyRest	Carta del conducente	personale
Driver1MaximumDailyPeriod	Carta del conducente	personale
Driver2MaximumDailyPeriod	Carta del conducente	personale
Driver1MaximumDailyDrivingTime	Carta del conducente	personale
Driver2MaximumDailyDrivingTime	Carta del conducente	personale
Driver1NumberOfUsedReducedDailyRestPeriods	Carta del conducente	personale
Driver2NumberOfUsedReducedDailyRestPeriods	Carta del conducente	personale
Driver1RemainingCurrentDrivingTime	Carta del conducente	personale
Driver2RemainingCurrentDrivingTime	Carta del conducente	personale
GNSS position	Unità elettronica di bordo	personale

2) DATI GNSS CONTINUI DISPONIBILI DOPO IL CONSENSO DEL CONDUCENTE

Cfr. appendice 12 — GNSS.

3) CODICI DELLE ANOMALIE DISPONIBILI SENZA IL CONSENSO DEL CONDUCENTE

Anomalia	Regole di memorizzazione	Dati da registrare per ogni anomalia
Inserimento di una carta non valida	— le 10 anomalie più recenti	— data e ora dell'anomalia — tipo, numero, Stato membro di rilascio e generazione della carta o delle carte che hanno dato origine all'anomalia — numero di anomalie simili nel giorno in questione
Conflitto di carte	— le 10 anomalie più recenti	— data e ora di inizio dell'anomalia — data e ora di fine dell'anomalia — tipo, numero, Stato membro di rilascio e generazione delle due carte che hanno dato origine al conflitto
Chiusura errata ultima sessione carta	— le 10 anomalie più recenti	— data e ora dell'inserimento della carta — tipo, numero, Stato membro di rilascio e generazione della carta o delle carte — dati relativi all'ultima sessione letti sulla carta: — data e ora dell'inserimento della carta — VRN, Stato membro di immatricolazione e generazione della VU

▼B

Anomalia	Regole di memorizzazione	Dati da registrare per ogni anomalia
Interruzione dell'alimentazione di energia (2)	— l'anomalia di maggiore durata per ciascuno degli ultimi 10 giorni in cui si è verificata — le 5 anomalie di maggiore durata nel corso degli ultimi 365 giorni	— data e ora di inizio dell'anomalia — data e ora di fine dell'anomalia — tipo, numero, Stato membro di rilascio e generazione delle carte inserite all'inizio e/o alla fine dell'anomalia — numero di anomalie simili nel giorno in questione
Errore di comunicazione con il dispositivo di comunicazione remota	— l'anomalia di maggiore durata per ciascuno degli ultimi 10 giorni in cui si è verificata — le 5 anomalie di maggiore durata nel corso degli ultimi 365 giorni	— data e ora di inizio dell'anomalia — data e ora di fine dell'anomalia — tipo, numero, Stato membro di rilascio e generazione delle carte inserite all'inizio e/o alla fine dell'anomalia — numero di anomalie simili nel giorno in questione
Assenza di informazioni sulla posizione provenienti dal ricevitore GNSS	— l'anomalia di maggiore durata per ciascuno degli ultimi 10 giorni in cui si è verificata — le 5 anomalie di maggiore durata nel corso degli ultimi 365 giorni	— data e ora di inizio dell'anomalia — data e ora di fine dell'anomalia — tipo, numero, Stato membro di rilascio e generazione delle carte inserite all'inizio e/o alla fine dell'anomalia — numero di anomalie simili nel giorno in questione
Errore dei dati di movimento	— l'anomalia di maggiore durata per ciascuno degli ultimi 10 giorni in cui si è verificata — le 5 anomalie di maggiore durata nel corso degli ultimi 365 giorni	— data e ora di inizio dell'anomalia — data e ora di fine dell'anomalia — tipo, numero, Stato membro di rilascio e generazione delle carte inserite all'inizio e/o alla fine dell'anomalia — numero di anomalie simili nel giorno in questione
Dati contrastanti sul movimento del veicolo	— l'anomalia di maggiore durata per ciascuno degli ultimi 10 giorni in cui si è verificata — le 5 anomalie di maggiore durata nel corso degli ultimi 365 giorni	— data e ora di inizio dell'anomalia — data e ora di fine dell'anomalia — tipo, numero, Stato membro di rilascio e generazione delle carte inserite all'inizio e/o alla fine dell'anomalia — numero di anomalie simili nel giorno in questione
Tentativi di violazione della sicurezza	le ultime 10 anomalie per ogni tipo di anomalia	— data e ora di inizio dell'anomalia — data e ora di fine dell'anomalia (se pertinenti) — tipo, numero, Stato membro di rilascio e generazione delle carte inserite all'inizio e/o alla fine dell'anomalia — tipo di anomalia

▼B

Anomalia	Regole di memorizzazione	Dati da registrare per ogni anomalia
Dati contrastanti sull'ora	— l'anomalia di maggiore durata per ciascuno degli ultimi 10 giorni in cui si è verificata — le 5 anomalie di maggiore durata nel corso degli ultimi 365 giorni	— data e ora dell'apparecchio di controllo — data e ora del GNSS — tipo, numero, Stato membro di rilascio e generazione delle carte inserite all'inizio e/o alla fine dell'anomalia — numero di anomalie simili nel giorno in questione

4) CODICI DELLE ANOMALIE DISPONIBILI CON IL CONSENSO DEL CONDUCENTE

Anomalia	Regole di memorizzazione	Dati da registrare per ogni anomalia
Guida in assenza di una carta adeguata	— l'anomalia di maggiore durata per ciascuno degli ultimi 10 giorni in cui si è verificata — le 5 anomalie di maggiore durata nel corso degli ultimi 365 giorni	— data e ora di inizio dell'anomalia — data e ora di fine dell'anomalia — tipo, numero, Stato membro di rilascio e generazione delle carte inserite all'inizio e/o alla fine dell'anomalia — numero di anomalie simili nel giorno in questione
Inserimento della carta durante la guida	— l'ultima anomalia per ciascuno degli ultimi 10 giorni in cui si è verificata	— data e ora dell'anomalia, — tipo, numero, Stato membro di rilascio e generazione della carta o delle carte — numero di anomalie simili nel giorno in questione
Superamento della velocità (1)	— l'anomalia più grave per ciascuno degli ultimi 10 giorni in cui si è verificata (cioè quella con la più alta velocità media) — le 5 anomalie più gravi nel corso degli ultimi 365 giorni — la prima anomalia verificatasi dopo l'ultima taratura	— data e ora di inizio dell'anomalia — data e ora di fine dell'anomalia — velocità massima misurata durante l'anomalia — media aritmetica della velocità misurata durante l'anomalia — tipo, numero, Stato membro di rilascio e generazione della carta del conducente (se applicabili) — numero di anomalie simili nel giorno in questione

5) CODICI DEI GUASTI DISPONIBILI SENZA IL CONSENSO DEL CONDUCENTE

Guasto	Regole di memorizzazione	Dati da registrare per ciascun guasto
Guasto della carta	— gli ultimi 10 guasti della carta del conducente	— data e ora di inizio del guasto — data e ora di fine del guasto — tipo, numero, Stato membro di rilascio e generazione della carta o delle carte
Guasti dell'apparecchio di controllo	— gli ultimi 10 guasti per ogni tipo di guasto — il primo guasto dopo l'ultima taratura	— data e ora di inizio del guasto — data e ora di fine del guasto — tipo di guasto — tipo, numero, Stato membro di rilascio e generazione delle carte inserite all'inizio e/o alla fine del guasto

▼B

Questo guasto deve attivarsi, quando non è attivo il modo taratura, in ciascuno dei casi seguenti:

— guasto interno della VU

— guasto della stampante

— guasto del dispositivo di visualizzazione

— guasto nel trasferimento di dati

— guasto del sensore

— guasto del ricevitore GNSS o del dispositivo GNSS esterno

— guasto del dispositivo di comunicazione remota

6) ANOMALIE SPECIFICHE DEFINITE DAL FABBRICANTE E GUASTI SENZA IL CONSENSO DEL CONDUCENTE

Anomalia o guasto	Regole di memorizzazione	Dati da registrare per ogni anomalia
Definito dal fabbricante	Definito dal fabbricante	Definito dal fabbricante

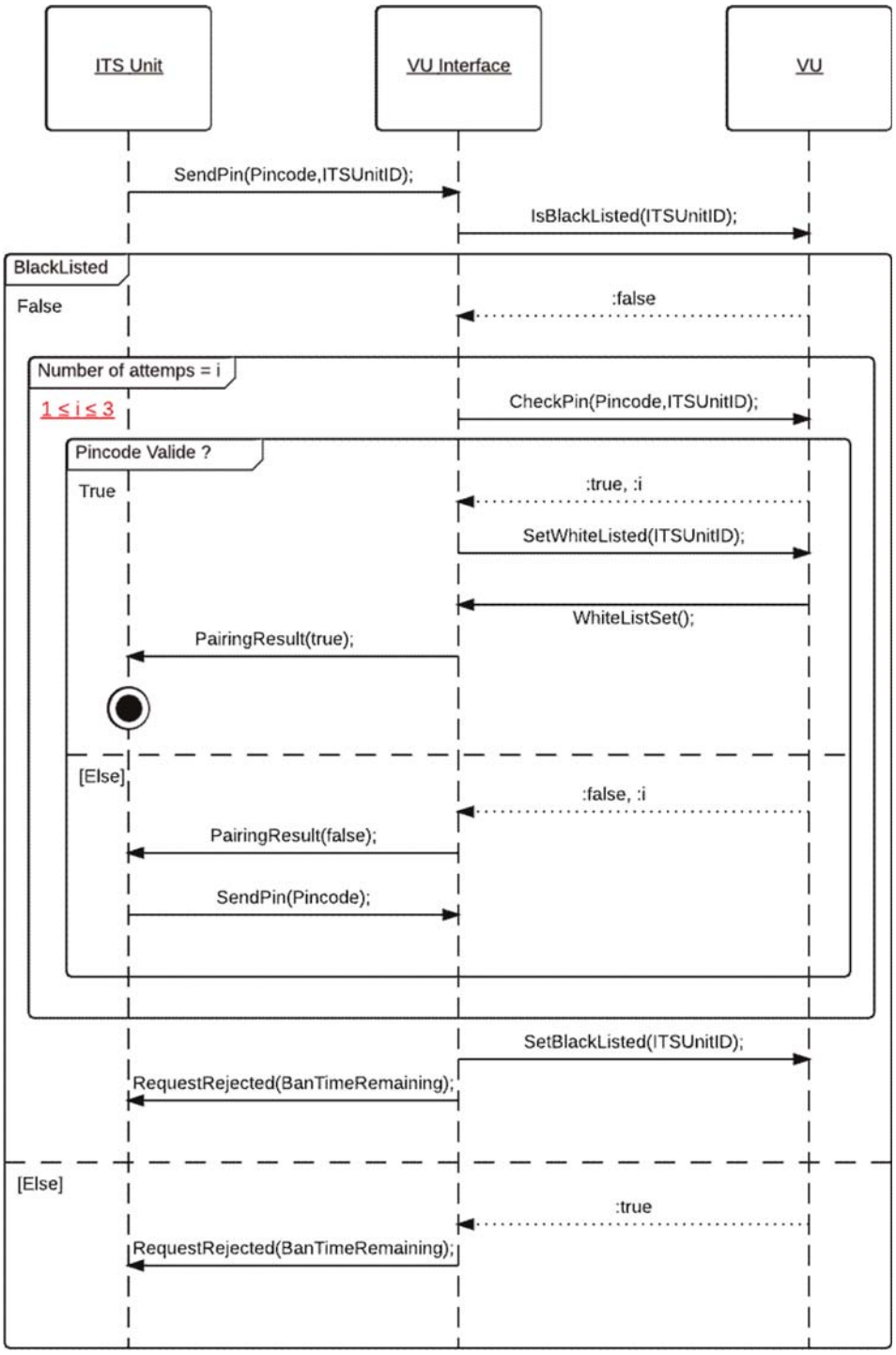
▼B

ALLEGATO 2

DIAGRAMMI DELLE SEQUENZE DEGLI SCAMBI DI MESSAGGI CON L'UNITÀ ITS

Figura 1

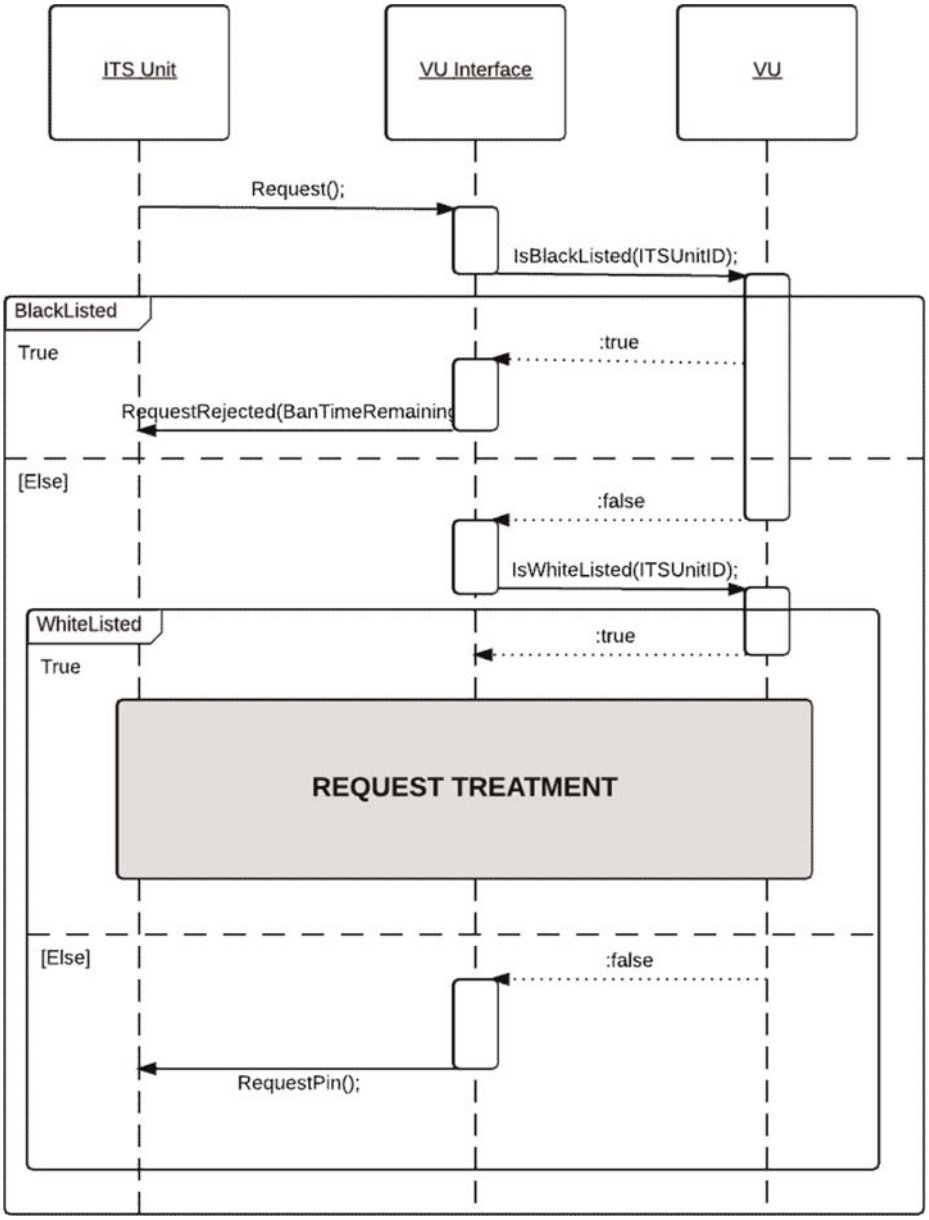
Diagramma della sequenza del tentativo di convalida del PIN



▼B

Figura 2

Diagramma della sequenza per la verifica dell'autorizzazione dell'unità ITS



▼B

Figura 3

Diagramma della sequenza di elaborazione della richiesta di dati classificati come non personali (dopo il corretto inserimento del PIN)

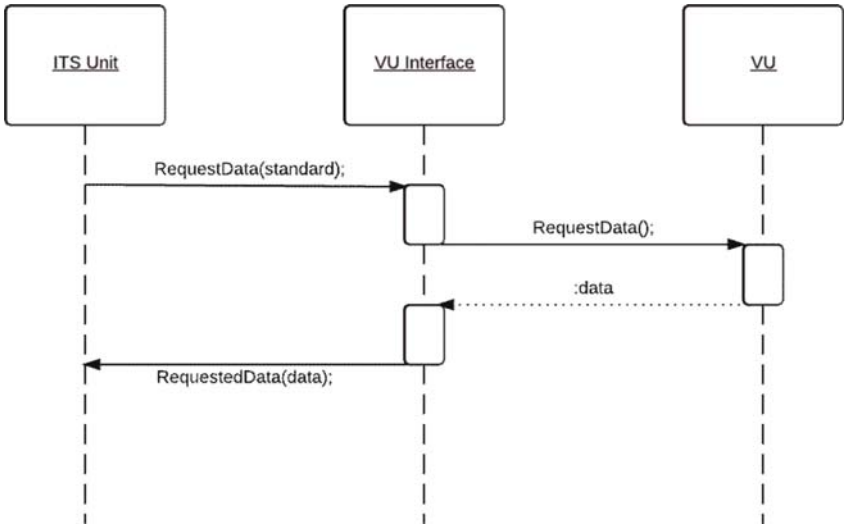
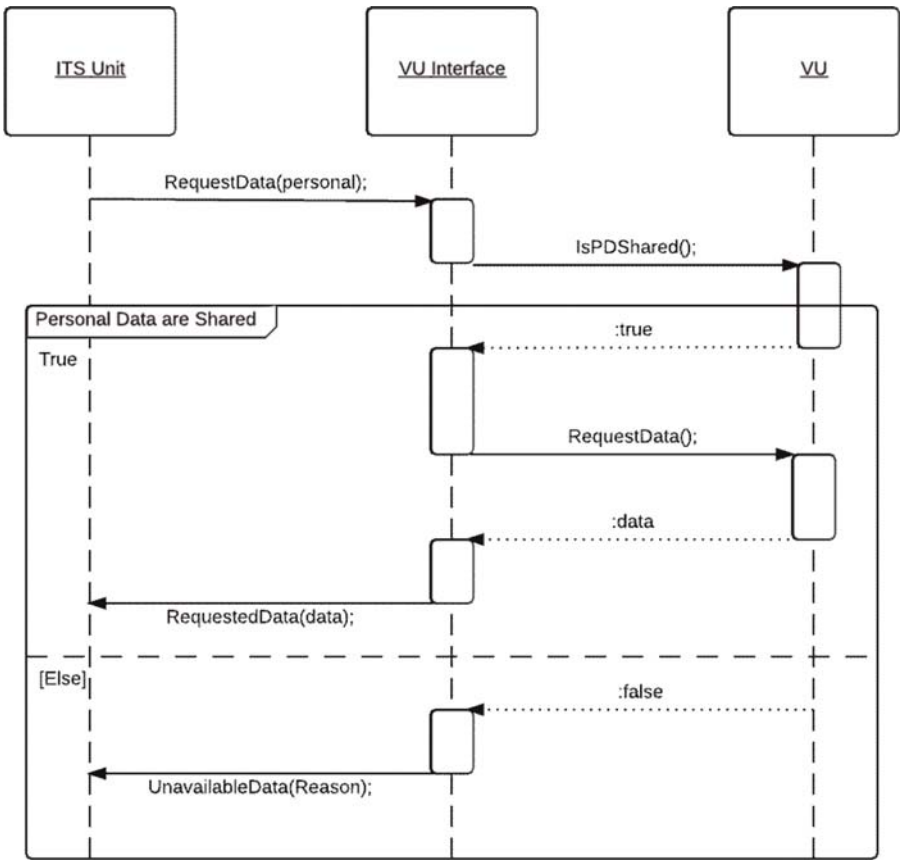


Figura 4

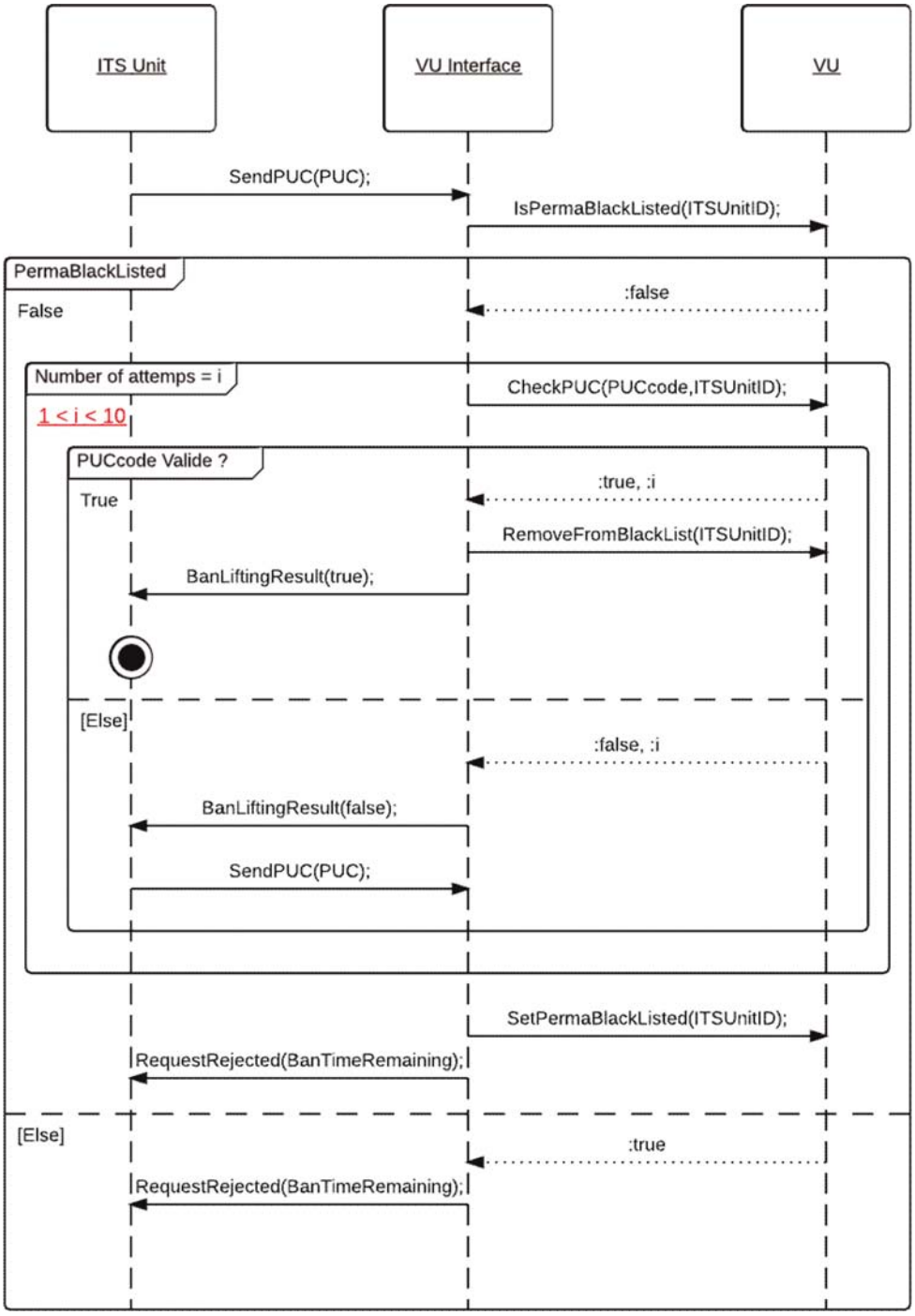
Diagramma della sequenza di elaborazione della richiesta di dati classificati come personali (dopo il corretto inserimento del PIN)



▼B

Figura 5

Diagramma della sequenza del tentativo di convalida del PUC



▼B

ALLEGATO 3

SPECIFICHE ASN.1

```
FormatMessageModule DEFINITIONS AUTOMATIC TAGS ::= BEGIN
EXPORTS ;
IMPORTS SendPIN, SendPUC, PairingResult, RequestPIN, RequestRejected,
        BanLiftingResult FROM PINPUCDataFieldsModule
        RequestAccepted,RequestData, DataUnavailable FROM
        RequestDataFieldsModule
        SendITSID, NegativeAnswer FROM OtherDataFieldsModule;

      CompleteMessage ::=SEQUENCE{
            header Header,
            data DataField,
            checksum Checksum
      }

      ----------------
      --HEADER TYPES--
      ----------------


      Header::=SEQUENCE{
            tgt IDList,
            src IDList,
            len BIT STRING (1..255)
      }

      vuID BIT STRING ::= 'EE'H
      IDList ::=CHOICE{
            vu BIT STRING (vuID),
            itsUnits SEQUENCE OF BIT STRING,
                  --Default hex Value:A0, redefined after first message exchange--
                  --Each ID will be linked to the Bluetooth ID of the device--
            ...
      }

      --------------------
      --DATAFIELDS TYPES--
      --------------------
      DataField ::=SEQUENCE{
            sid BIT STRING,
            trtp BIT STRING,
            subMBytes SubMessageBytes,
            dataField Content,
            ...
      }

      SubMessageBytes ::= SEQUENCE{
            currentSubM BIT STRING,
            totalSubM BIT STRING
      }

      Content ::= CHOICE{
            requestPIN RequestPIN,
            sendITSID SendITSID,
            sendPin SendPIN,
```

▼B

```
55                pairRslt PairingResult,
56                sendPUC SendPUC,
57                banlift BanLiftingResult,
58                requestRejected RequestRejected,
59                requestData RequestData,
60                requestOK RequestAccepted,
61                dataUnavailable DataUnavailable,
62                negAns NegativeAnswer
63          }
64
65          ------------------
66          --CHECKSUM TYPES--
67          ------------------
68
69          Checksum ::= SEQUENCE{
70                --SHA2 checksum
71          }
72    END
73
```

▼B

```
74  PINPUCDataFieldsModule DEFINITIONS AUTOMATIC TAGS ::= BEGIN
75  EXPORTS SendPIN, SendPUC, PairingResult, RequestPIN, RequestRejected,
76  BanLiftingResult;
77  IMPORTS ;
78
79        ----------
80        ---Utils--
81        ----------
82
83        PUC ::= SEQUENCE (SIZE(8)) OF
84        INTEGER (SIZE(0..9))
85
86        PIN ::=      SEQUENCE (SIZE(4)) OF
87              INTEGER (SIZE(0..9))
88
89        -------------------------
90        --Messages From ITS Unit--
91        -------------------------
92
93        SendPIN {PIN:pin} ::= SEQUENCE {
94              sid BIT STRING ('03'H),
95              pin PIN (pin)
96        }
97
98        SendPUC {PUC:puc} ::= SEQUENCE {
99              sid BIT STRING ('05'H),
100             puc PUC (puc)
101       }
102       --------------------
103       --Messages From VU--
104       --------------------
105
106       PairingResult ::= SEQUENCE{
107             sid BIT STRING ('04'H),
108             result BOOLEAN
109       }
110
111       RequestPIN {MType:receivedRequest}::= SEQUENCE{
112             sid BIT STRING ('01'H)
113       }
114
115       RequestRejected ::= SEQUENCE{
116             sid BIT STRING ('07'H),
117             banTimeRemaining GeneralizedTime, --PermaBan == 1k years-- }
118
119       BanLiftingResult ::= SEQUENCE{
120             sid BIT STRING ('06'H),
121             result BOOLEAN
122       }
123 END
124
```

▼B

```
RequestDataFields DEFINITIONS AUTOMATIC TAGS ::= BEGIN
	EXPORTS RequestAccepted,RequestData, DataUnavailable ;
	IMPORTS StandardEvent, PersonalEvent, StandardFault FROM EventsModule;

	------------------
	---From ITS Unit--
	------------------
	RequestData ::= SEQUENCE{
		sid BIT STRING ('08'H),
		requestedData DataTypeCode,
		...
	}

	-----------
	--From VU--
	-----------
	RequestAccepted ::=SEQUENCE{
		sid BIT STRING ('09'H),
		trtp DataTypeCode,
		dataSheet CHOICE{
			standardData StandardTachDataContent,
			personalData PersonalTachDataContent,
			gnss GNSSDataContent,
			standardEvent StandardEventContent,
			personalEvent PersonalEventContent,
			standardFault StandardFaultContent,
			manufacturerdata ManufacturerDataContent,
			...
		}
	}

	DataTypeCode ::=CHOICE{
		standardTachData BIT STRING ('01'H),
		personalTachData BIT STRING ('02'H),
		gnssData BIT STRING ('03'H),
		standardEventData BIT STRING ('04'H),
		personalEventData BIT STRING ('05'H),
		standardFaultData BIT STRING ('06'H),
		manufacturerData BIT STRING ('07'H),
		...
	}

	DataUnavailable ::=SEQUENCE{
		sid BIT STRING ('0A'H),
		trtp DataTypeCode,
		reason UnavailableDataCodes
	}

	UnavailableDataCodes ::= CHOICE{
		noDataAvailable BIT STRING ('10'H),
		personalDataNotShared BIT STRING ('11'H),
		...
	}
	---------------------------
	--Complete Tachograph Data--
	---------------------------
	--The format of the data was taken from the ISO16844-7 norm, more information
available in this ISO document—

```

▼B

```
Time ::= SEQUENCE{
       seconds INTEGER (0..59.75), --increment: 0.25s--
       minutes INTEGER (0..59), --increment: 1min--
       hours INTEGER (0..23), --increment: 1h--
       day INTEGER (0.25.. 31.75), --increment: 0.25d--
       month INTEGER (1..12), --increment: 1month--
       year INTEGER (1985..2235), --increment: 1year--
       locMinOffset INTEGER (-59..59), --increment: 1min--
       locHouroffset INTEGER (-23..23)--increment: 1h--
}

Date ::= SEQUENCE{
       month INTEGER (1..12), --increment: 1month--
       day INTEGER (0.25.. 31.75), --increment: 0.25d--
       year INTEGER (1985..2235) --increment: 1year--
}

DriverName ::=SEQUENCE{
       codePageSurname UTF8String, --See ISO/IEC 8859--
       surname UTF8String,
       codePageFirstname UTF8String, --See ISO/IEC 8859--
       firstname UTF8String,
}

-------------------
--Message Content--
-------------------

StandardTachDataContent ::= SEQUENCE{
       trtp DataTypeCode (DataTypeCode.&standardTachData),
       personal BOOLEAN (FALSE),
       data StandardTachyDataSheet,
}

PersonalTachDataContent ::= SEQUENCE{
       trtp DataTypeCode (DataTypeCode.&personalTachData),
       personal BOOLEAN (TRUE),
       data PersonalTachyDataSheet
}

GNSSDataContent ::= SEQUENCE{
       trtp DataTypeCode (DataTypeCode.&gnssData),
       personal BOOLEAN (TRUE),
       data GNSSDataSheet
}

StandardEventContent ::= SEQUENCE{
       trtp DataTypeCode (DataTypeCode.&standardEventData),
       personal BOOLEAN (FALSE),
       data StandardEventDataSheet
}

PersonalEventContent ::= SEQUENCE{
       trtp DataTypeCode (DataTypeCode.&personalEventData),
       personal BOOLEAN (TRUE),
       data PersonalEventDataSheet
}

StandardFaultContent ::= SEQUENCE{
```

▼B

```
243                trtp DataTypeCode (DataTypeCode.&standardFaultData),
244                personal BOOLEAN (FALSE),
245                data StandardFault
246          }
247
248          ManufacturerDataContent ::= SEQUENCE{
249                trtp DataTypeCode (DataTypeCode.&manufacturerData),
250                personal BOOLEAN (TRUE),
251                ...
252          }
253
254          ---------------
255          --DATA SHEETS--
256          ---------------
257
258          --Data sheet format follows ISO 16844-7.--
259          StandardTachyDataSheet ::= SEQUENCE{
260                vin UTF8String (SIZE(17)),
261                calibrationDate Date,
262                driveRecognize INTEGER (2 UNION 12),
263                driverCardDriver1 INTEGER (2 UNION 12),
264                driverCardDriver2 INTEGER (2 UNION 12),
265                timeDate Time,
266                highResolutionTotalVehicleDistance INTEGER (0..21055406), --increment:
267    5m--
268                serviceComponentIdentification INTEGER (0..255),
269                serviceDelayCalendarTimeBased INTEGER (-125..125), --increment: 1week-
270    -
271                nextCalibrationDate Date,
272                speedAuthorised INTEGER (0..250.996), --increment 1/256km/h--
273                tachographCardSlot1 INTEGER (0..4...), --Maximum 250--
274                tachographCardSlot2 INTEGER (0..4...), --Maximum 250--
275                outOfScopeCondition INTEGER(2 UNION 12),
276                modeOfOperation INTEGER (0..4...), --Maximum 250--
277                registeringMemberState UTF8String,
278          vehicleRegistrationNumber SEQUENCE {
279                      codePageVRN INTEGER (0..255),
280                      vrn OCTET STRING (SIZE(13)),
281                },
282                tachographNextMandatoryDownloadDate Date,
283                ...
284          }
285
286          PersonalTachyDataSheet ::= SEQUENCE{
287                tachographVehicleSpeed INTEGER (0..250.996), --increment 1/256km/h--
288                driver1WorkingState INTEGER (2 UNION 12 UNION 102 UNION 112 UNION 1002
289    UNION 1012...),
290                driver2WorkingState INTEGER (2 UNION 12 UNION 102 UNION 112 UNION 1002
291    UNION 1012...),
292
293                driver1TimeRelatedStates INTEGER(2 UNION 12 UNION 102 UNION 112 UNION
294    1002 UNION
295                                                 1012 UNION 1102 UNION 1112 UNION
296    10002 UNION 10012 UNION
297                                                 10102 UNION 10112 UNION 11002 UNION
298    11012...),
299                driver2TimeRelatedStates INTEGER(2 UNION 12 UNION 102 UNION 112 UNION
300    1002 UNION
```

▼B

```
                                                    1012 UNION 1102 UNION 1112 UNION
10002 UNION 10012 UNION
                                                    10102 UNION 10112 UNION 11002 UNION
11012...),

              overSpeed INTEGER (2 UNION 12),
              driver1Identification INTEGER (SIZE(19)), --TODO NEED FURTHER SPECS
FROM TACHO REGULATION--
              driver2Identification INTEGER (SIZE(19)), --TODO NEED FURTHER SPECS
FROM TACHO REGULATION--
              driver1ContinuousDrivingTime INTEGER (0.. 64255), --increment: 1min--
              driver2ContinuousDrivingTime INTEGER (0.. 64255), --increment: 1min--
              driver1CurrentDurationOfSelectedActivity INTEGER (0.. 64255), --
increment: 1min--
              driver2CurrentDurationOfSelectedActivity INTEGER (0.. 64255), --
increment: 1min--
              driver1Name DriverName,
              driver2Name DriverName,
              driver1CumulatedDrivingTimePreviousAndCurrentWeek INTEGER (0.. 64255),
--increment: 1min--
              driver2CumulatedDrivingTimePreviousAndCurrentWeek INTEGER (0.. 64255),
--increment: 1min--
              engineSpeed INTEGER(0..8031.875), --increment: 0,125r/min--
              driver1EndOfLastDailyRestPeriod Time,
              driver2EndOfLastDailyRestPeriod Time,
              driver1EndOfLastWeeklyRestPeriod Time,
              driver2EndOfLastWeeklyRestPeriod Time,
              driver1EndOfSecondLastWeeklyRestPeriod Time,
              driver2EndOfSecondLastWeeklyRestPeriod Time,
              driver1CurrentDailyDrivingTime INTEGER (0.. 64255), --increment: 1min-
-
              driver2CurrentDailyDrivingTime INTEGER (0.. 64255), --increment: 1min-
-
              driver1CurrentWeeklyDrivingTime INTEGER (0.. 64255), --increment:
1min--
              driver2CurrentWeeklyDrivingTime INTEGER (0.. 64255), --increment:
1min--
              driver1TimeLeftUntilNewDailyRestPeriod INTEGER (0.. 64255), --
increment: 1min--
              driver2TimeLeftUntilNewDailyRestPeriod INTEGER (0.. 64255), --
increment: 1min--
              driver1CardExpiryDate Date,
              driver2CardExpiryDate Date,
              driver1CardNextMandatoryDownloadDate Date,
              driver2CardNextMandatoryDownloadDate Date,
              driver1TimeLeftUntilNewWeeklyRestPeriod INTEGER (0.. 64255), --
increment: 1min--
              driver2TimeLeftUntilNewWeeklyRestPeriod INTEGER (0.. 64255), --
increment: 1min--
              driver1NumberOfTimes9hDailyDrivingTimesExceeded INTEGER (0..13),
              driver2NumberOfTimes9hDailyDrivingTimesExceeced INTEGER (0..13),
              driver1CumulativeUninterruptedRestTime INTEGER (0.. 64255), --
increment: 1min--
              driver2CumulativeUninterruptedRestTime INTEGER (0.. 64255), --
increment: 1min--
              driver1MinimumDailyRest INTEGER (0.. 64255), --increment: 1min--
              driver2MinimumDailyRest INTEGER (0.. 64255), --increment: 1min--
              driver1MinimumWeeklyRest INTEGER (0.. 64255), --increment: 1min--
              driver2MinimumWeeklyRest INTEGER (0.. 64255), --increment: 1min--
```

▼B

```
360                driver1MaximumDailyPeriod INTEGER (0..250), --increment: 1h--
361                driver2MaximumDailyPeriod INTEGER (0..250), --increment: 1h--
362                driver1MaximumDailyDrivingTime INTEGER (910 UNION 1010),
363                driver2MaximumDailyDrivingTime INTEGER (910 UNION 1010),
364                driver1NumberOfUsedReducedDailyRestPeriods INTEGER (0..13),
365                driver2NumberOfUsedReducedDailyRestPeriods INTEGER (0..13),
366                driver1RemainingCurrentDrivingTime INTEGER (0.. 64255), --increment:
367    1min--
368                driver2RemainingCurrentDrivingTime INTEGER (0.. 64255), --increment:
369    1min--
370                ...
371          }
372
373          GNSSDataSheet ::=  SEQUENCE {
374          gnssPosition GeoCoordinates
375                --See Appendix 1 for definition of GeoCoordinates--
376          }
377
378          StandardEventDataSheet ::= SEQUENCE{
379                events SEQUENCE OF StandardEvent
380          }
381
382          PersonalEventDataSheet ::= SEQUENCE{
383                events SEQUENCE OF PersonalEvent
384          }
385    END
386
387    EventsModule DEFINITIONS AUTOMATIC TAGS ::= BEGIN
388          EXPORTS ALL;
389          IMPORTS NationAlpha FROM Appendix1; --See Appendix 1 for more information
390    about NationAlpha--
391
392                SecurityBreachEvent ::=SEQUENCE{
393                      --See Annex 1B for more information--
394                }
395
396                RecordingEquipmentFaultType ::= SEQUENCE{
397                      --See Annex 1B for more information--
398                }
399
400                StandardEvent::= CHOICE{
401                      insertionInvalidCard InsertionOfANonValidCard,
402                      cardConflict CardConflict,
403                      timeOverlap TimeOverlap,
404                      previousSessionNotClosed LastCardSessionNotCorrectlyClosed,
405                      overSpeeding OverSpeeding,
406                      powerSupplyInterruption PowerSupplyInterruption,
407                      comErrorWithRemoteFacility
408    CommunicationErrorWithTheRemoteCommunicationFacility,
409                      absenceGNSSPosition
410    AbsenceOfPositionInformationFromGNSSReceiver,
411                      positionDataError PositionDataError,
412                      motionDataError MotionDataError,
413                      vehicleMotionConflict VehicleMotionConflict,
414                      securityBreachAttempt SecurityBreachAttempt,
415                      timeConflict TimeConflict,
416                      ...
417                }
418
```

▼B

```
PersonalEvent ::= CHOICE{
      lackOfAppropriateCard DrivingWithoutAnAppropriateCard,
      cardInsertionWhileDriving CardInsertionWhileDriving,
      overSpeeding OverSpeeding,
      ...
}

StandardFault ::= CHOICE{
      cardFault CardFault,
      recordingEquipementFault RecordingEquipmentFault,
...
}

---------------
--EVENTS LIST--
---------------

InsertionOfANonValidCard::=SEQUENCE{
      beginDate GeneralizedTime,
      endDate GeneralizedTime,
      carsdType SEQUENCE OF UTF8String,
      cardsNumber SEQUENCE OF INTEGER,
      issuingMemberState SEQUENCE OF NationAlpha,
      cardsGeneration SEQUENCE OF INTEGER
}

CardConflict ::= SEQUENCE{
      beginDate GeneralizedTime,
      endDate GeneralizedTime,
      carsdType SEQUENCE OF UTF8String,
      cardsNumber SEQUENCE OF INTEGER,
      issuingMemberState SEQUENCE OF NationAlpha,
      cardsGeneration SEQUENCE OF INTEGER
}

TimeOverlap ::=SEQUENCE{
      beginDate GeneralizedTime,
      endDate GeneralizedTime,
      carsdType SEQUENCE OF UTF8String,
      cardsNumber SEQUENCE OF INTEGER,
      issuingMemberState SEQUENCE OF NationAlpha,
      cardsGeneration SEQUENCE OF INTEGER,
      numberSimilarEvent INTEGER
}

DrivingWithoutAnAppropriateCard ::= SEQUENCE{
      beginDate GeneralizedTime,
      endDate GeneralizedTime,
      carsdType SEQUENCE OF UTF8String,
      cardsNumber SEQUENCE OF INTEGER,
      issuingMemberState SEQUENCE OF NationAlpha,
      cardsGeneration SEQUENCE OF INTEGER,
      numberOfSimilarEvent INTEGER
}

CardInsertionWhileDriving ::= SEQUENCE{
      date GeneralizedTime,
      carsdType SEQUENCE OF UTF8String,
      cardsNumber SEQUENCE OF INTEGER,
```

▼B

```
478                     issuingMemberState SEQUENCE OF NationAlpha,
479                     numberOfSimilarEvents INTEGER
480             }
481
482             LastCardSessionNotCorrectlyClosed ::=SEQUENCE{
483                     beginDate GeneralizedTime,
484                     endDate GeneralizedTime,
485                     carsdType SEQUENCE OF UTF8String,
486                     cardsNumber SEQUENCE OF INTEGER,
487                     issuingMemberState SEQUENCE OF NationAlpha,
488                     cardsGeneration SEQUENCE OF INTEGER,
489                     oldSession SEQUENCE{
490                             beginDate GeneralizedTime,
491                             endDate GeneralizedTime,
492                             vrn UTF8String,
493                             issuingMemberState NationAlpha,
494                             cardsGeneration INTEGER,
495                     }
496             }
497
498             OverSpeeding ::=SEQUENCE{
499                     beginDate GeneralizedTime,
500                     endDate GeneralizedTime,
501                     maximumSpeed INTEGER,
502                     averageSpeed INTEGER,
503                     cardType UTF8String,
504                     cardNumber INTEGER,
505                     issuingMemberState NationAlpha,
506                     cardGeneration INTEGER,
507                     numberOfSimilarEvents INTEGER
508             }
509
510             PowerSupplyInterruption ::=SEQUENCE{
511                     beginDate GeneralizedTime,
512                     endDate GeneralizedTime,
513                     carsdType SEQUENCE OF UTF8String,
514                     cardsNumber SEQUENCE OF INTEGER,
515                     issuingMemberState SEQUENCE OF NationAlpha,
516                     cardsGeneration SEQUENCE OF INTEGER,
517                     numberOfSimilarEvent INTEGER
518             }
519
520             CommunicationErrorWithTheRemoteCommunicationFacility ::=SEQUENCE{
521                     beginDate GeneralizedTime,
522                     endDate GeneralizedTime,
523                     carsdType SEQUENCE OF UTF8String,
524                     cardsNumber SEQUENCE OF INTEGER,
525                     issuingMemberState SEQUENCE OF NationAlpha,
526                     cardsGeneration SEQUENCE OF INTEGER,
527                     numberOfSimilarEvent INTEGER
528             }
529
530             AbsenceOfPositionInformationFromGNSSReceiver ::= SEQUENCE{
531                     beginDate GeneralizedTime,
532                     endDate GeneralizedTime,
533                     carsdType SEQUENCE OF UTF8String,
534                     cardsNumber SEQUENCE OF INTEGER,
535                     issuingMemberState SEQUENCE OF NationAlpha,
536                     cardsGeneration SEQUENCE OF INTEGER,
```

▼B

```
537                     numberOfSimilarEvent INTEGER
538             }
539
540             PositionDataError ::= SEQUENCE{
541                     beginDate GeneralizedTime,
542                     endDate GeneralizedTime,
543                     carsdType SEQUENCE OF UTF8String,
544                     cardsNumber SEQUENCE OF INTEGER,
545                     issuingMemberState SEQUENCE OF NationAlpha,
546                     cardsGeneration SEQUENCE OF INTEGER,
547                     numberOfSimilarEvent INTEGER
548             }
549
550             MotionDataError ::= SEQUENCE{
551                     beginDate GeneralizedTime,
552                     endDate GeneralizedTime,
553                     carsdType SEQUENCE OF UTF8String,
554                     cardsNumber SEQUENCE OF INTEGER,
555                     issuingMemberState SEQUENCE OF NationAlpha,
556                     cardsGeneration SEQUENCE OF INTEGER,
557                     numberOfSimilarEvent INTEGER
558             }
559
560             VehicleMotionConflict ::= SEQUENCE{
561                     beginDate GeneralizedTime,
562                     endDate GeneralizedTime,
563                     carsdType SEQUENCE OF UTF8String,
564                     cardsNumber SEQUENCE OF INTEGER,
565                     issuingMemberState SEQUENCE OF NationAlpha,
566                     cardsGeneration SEQUENCE OF INTEGER,
567                     numberOfSimilarEvent INTEGER
568             }
569
570             SecurityBreachAttempt ::= SEQUENCE{
571                     beginDate GeneralizedTime,
572                     endDate GeneralizedTime OPTIONAL,
573                     carsdType SEQUENCE OF UTF8String,
574                     cardsNumber SEQUENCE OF INTEGER,
575                     issuingMemberState SEQUENCE OF NationAlpha,
576                     numberOfSimilarEvent INTEGER,
577                     typeOfEvent SecurityBreachEvent
578             }
579
580
581             TimeConflict ::= SEQUENCE{
582                     beginDate GeneralizedTime,
583                     endDate GeneralizedTime,
584                     carsdType SEQUENCE OF UTF8String,
585                     cardsNumber SEQUENCE OF INTEGER,
586                     issuingMemberState SEQUENCE OF NationAlpha,
587                     cardsGeneration SEQUENCE OF INTEGER,
588                     numberOfSimilarEvent INTEGER
589             }
590
591             ---------------
592             --FAULTS LIST--
593             ---------------
594
595             CardFault ::= SEQUENCE{
```

▼B

```
596                     beginDate GeneralizedTime,
597                     endDate GeneralizedTime,
598                     carsdType SEQUENCE OF UTF8String,
599                     cardsNumber SEQUENCE OF INTEGER,
600                     issuingMemberState SEQUENCE OF NationAlpha,
601                     cardsGeneration SEQUENCE OF INTEGER,
602             }
603
604             RecordingEquipmentFault ::= SEQUENCE{
605                     beginDate GeneralizedTime,
606                     endDate GeneralizedTime,
607                     faultType RecordingEquipmentFaultType,
608                     carsdType SEQUENCE OF UTF8String,
609                     cardsNumber SEQUENCE OF INTEGER,
610                     issuingMemberState SEQUENCE OF NationAlpha,
611                     cardsGeneration SEQUENCE OF INTEGER,
612             }
613 END
```

▼B

Appendice 14

FUNZIONE DI COMUNICAZIONE REMOTA

INDICE

1 INTRODUZIONE

2 CAMPO DI APPLICAZIONE

3 ACRONIMI, DEFINIZIONI E SIMBOLI

4 SCENARI OPERATIVI

4.1 Panoramica

4.1.1 Precondizioni per il trasferimento di dati tramite l'interfaccia DSRC 5,8 GHz

4.1.2 Profilo 1a: con un lettore della comunicazione remota a fini di diagnosi precoce sorretto e puntato manualmente o posizionato su un cavalletto a lato della strada e puntato

4.1.3 Profilo 1b: con un lettore della comunicazione remota a fini di diagnosi precoce (REDCR) montato sul veicolo e puntato

4.2 Sicurezza/integrità

5 STRUTTURA E PROTOCOLLI DI COMUNICAZIONE REMOTA

5.1 Struttura

5.2 Sequenza

5.2.1 Operazioni

5.2.2 Interpretazione dei dati ricevuti tramite la comunicazione DSRC

5.3 Parametri dell'interfaccia fisica DSRC per la comunicazione remota

5.3.1 Vincoli relativi alla posizione

5.3.2 Parametri di downlink e uplink

5.3.3 Progettazione dell'antenna

5.4 Requisiti del protocollo DSRC per l'RTM

5.4.1 Panoramica

5.4.2 Comandi

5.4.3 Sequenza di comandi di interrogazione

5.4.4 Strutture dei dati

5.4.5 Elementi di RtmData, azioni eseguite e definizioni

5.4.6 Meccanismo di trasferimento dei dati

5.4.7 Descrizione dettagliata della transazione DSRC

5.4.8 Descrizione della transazione di prova DSRC

5.5 Conformità alla direttiva 2015/71/UE

5.5.1 Panoramica

5.5.2 Comandi

▼B

5.5.3 Sequenza di comandi di interrogazione

5.5.4 Strutture dei dati

5.5.5 Modulo ASN. 1 per la transazione OWS DSRC

5.5.6 Elementi di OwsData, azioni eseguite e definizioni

5.5.7 Meccanismi di trasferimento dei dati

5.6 Trasferimento di dati tra la DSRC-VU e la VU

5.6.1 Collegamento fisico e interfacce

5.6.2 Protocollo dell'applicazione

5.7 Trattamento degli errori

5.7.1 Registrazione e comunicazione dei dati nella DSRC-VU

5.7.2 Errori di comunicazione senza fili

6 PROVE DI ATTIVAZIONE E DI ISPEZIONE PERIODICA PER LA FUNZIONE DI COMUNICAZIONE REMOTA

6.1 Aspetti generali

6.2 ECHO

6.3 Prove per convalidare il contenuto dei dati sicuri

1 INTRODUZIONE

La presente appendice stabilisce le specifiche di progettazione e le procedure da seguire per realizzare la funzione di comunicazione remota (*la comunicazione*) conformemente all'articolo 9 del regolamento (UE) n. 165/2014 (*il regolamento*).

DSC_1 Il regolamento (UE) n. 165/2014 stabilisce che il tachigrafo deve essere munito di una funzionalità di comunicazione remota che consenta agli agenti delle autorità di controllo competenti di leggere le informazioni del tachigrafo dai veicoli in transito tramite un dispositivo che interroga il tachigrafo a distanza [il lettore della comunicazione remota a fini di diagnosi precoce (REDCR)]. Tale dispositivo di interrogazione si collega senza fili grazie alle interfacce CEN 5,8 GHz di comunicazione dedicata a corto raggio (DSRC).

È importante capire che questa funzionalità è intesa a fungere esclusivamente da prefiltro per scegliere i veicoli da sottoporre a ispezione e non sostituisce la procedura di ispezione formale prevista dal regolamento (UE) n. 165/2014. Si veda il considerando 9 del preambolo del presente regolamento, che stabilisce che la comunicazione remota fra il tachigrafo e le autorità preposte ai controlli ai fini dei controlli su strada agevola i controlli su strada mirati.

DSC_2 *I dati* devono essere scambiati usando *la comunicazione*, che deve consistere in uno scambio senza fili tramite DSRC 5,8 GHz conforme alla presente appendice. Essi devono essere testati per verificarne la compatibilità ai parametri pertinenti della norma EN 300 674-1, [Electromagnetic compatibility and Radio spectrum Matters (ERM); Road Transport and Traffic Telematics (RTTT); Dedicated Short Range Communication

▼B

(DSRC) transmission equipment (500 kbit/s / 250 kbit/s) operating in the 5,8 GHz Industrial, Scientific and Medical (ISM) band; Part 1: General characteristics and test methods for Road Side Units (RSU) and On -Board Units (OBU)].

DSC_3 *La comunicazione* con i relativi dispositivi deve essere stabilita solo quando richiesto dal dispositivo dell'autorità di controllo competente tramite mezzi di comunicazione radio conformi [*il lettore della comunicazione remota a fini di diagnosi precoce (REDCR)*].

DSC_4 *I dati* devono essere protetti per garantirne l'integrità.

DSC_5 L'accesso ai *dati* comunicati deve essere limitato alle autorità di controllo competenti autorizzate ad accertare le violazioni del regolamento (CE) n. 561/2006 e del regolamento (UE) n. 165/2014 e alle officine, nella misura necessaria alla verifica del corretto funzionamento del tachigrafo.

DSC_6 *I dati* scambiati durante *la comunicazione* devono limitarsi ai dati necessari ai fini dei controlli su strada mirati dei veicoli muniti di un tachigrafo potenzialmente manomesso o usato impropriamente.

DSC_7 L'integrità e la sicurezza dei dati devono essere ottenute conservando *i dati* nell'unità elettronica di bordo (VU) in modalità sicura e comunicando solo il payload in modalità sicura e i dati relativi alla sicurezza (cfr. paragrafo 5.4.4) tramite il mezzo di comunicazione remota senza fili DSRC 5,8 GHz. In questo modo solo le persone autorizzate delle autorità di controllo competenti hanno modo di capire i dati trasmessi con *la comunicazione* e di verificarne l'autenticità. Cfr. l'appendice 11 (Meccanismi comuni di sicurezza).

DSC_8 *I dati* devono contenere un timeStamp indicante l'ora dell'ultimo aggiornamento.

DSC_9 Il contenuto dei dati di sicurezza deve essere noto e sotto il controllo esclusivo delle autorità di controllo competenti e delle parti con cui condividono queste informazioni ed esula dalle disposizioni *della comunicazione* oggetto della presente appendice, tranne per il fatto che *la comunicazione* prevede il trasferimento di un pacchetto di dati di sicurezza con ciascun pacchetto di payload.

DSC_10 La stessa architettura e gli stessi dispositivi devono poter essere usati per acquisire altri concetti di dati (come il peso a bordo) usando l'architettura qui specificata.

DSC_11 A scanso di equivoci, in conformità alle disposizioni del regolamento (UE) n. 165/2014, articolo 7, i dati riguardanti l'identità del conducente non devono essere comunicati tramite *la comunicazione*.

2 CAMPO DI APPLICAZIONE

La presente appendice specifica come gli agenti delle autorità di controllo competenti usano una comunicazione senza fili DSRC 5,8 GHz specificata per ottenere dati a distanza (*i dati*) da un veicolo bersaglio,

▼B

che rivelano che tale veicolo potrebbe violare il regolamento (UE) n. 165/2014 e sarebbe opportuno valutare di fermarlo per ulteriori controlli.

Secondo il regolamento (UE) n. 165/2014, *i dati* raccolti devono limitarsi o appartenere a dati che identificano una potenziale violazione, come definita all'articolo 9 del medesimo.

In questo scenario, il tempo a disposizione per la comunicazione è limitato, perché *la comunicazione* è mirata e a corto raggio. Inoltre il mezzo di comunicazione usato per il monitoraggio a distanza del tachigrafo (RTM) può essere usato dalle autorità di controllo competenti anche per altre applicazioni (ad esempio per i pesi massimi e le dimensioni massime dei veicoli commerciali pesanti definiti nella direttiva 2015/719/UE) e tali operazioni possono essere separate o in sequenza a discrezione delle autorità di controllo competenti.

La presente appendice specifica:

— Le apparecchiature, le procedure e i protocolli di comunicazione da usare per *la comunicazione*

— Le norme e i regolamenti ai quali le apparecchiature radio devono essere conformi

— La presentazione dei *dati* alle apparecchiature di *comunicazione*

— Le procedure di richiesta e di trasferimento e la sequenza delle operazioni

— *I dati* da trasferire

— La potenziale interpretazione *dei dati* trasferiti durante *la comunicazione*

— Le disposizioni sui dati di sicurezza relativi *alla comunicazione*

— La messa a disposizione *dei dati* alle autorità di controllo competenti

— In che modo il *lettore della comunicazione remota a fini di diagnosi precoce* può richiedere diversi concetti di dati sul carico e sul parco veicoli

A fini di chiarezza, la presente appendice non specifica:

— la raccolta del funzionamento e della gestione *dei dati* all'interno della VU (che deve essere una funzione della progettazione del prodotto salvo altra indicazione nel regolamento (UE) n. 165/2014);

— la forma in cui i dati raccolti sono presentati all'agente delle autorità di controllo competenti né i criteri che le autorità di controllo competenti devono usare per decidere quali veicoli fermare (che deve essere una funzione della progettazione del prodotto salvo altra indicazione nel regolamento (UE) n. 165/2014 o una decisione delle autorità di controllo competenti). A scanso di equivoci: *la comunicazione* si limita a mettere *i dati* a disposizione delle autorità di controllo competenti per consentire loro di prendere decisioni informate;

▼B

— le disposizioni sulla sicurezza dei dati (come la cifratura) per quanto riguarda il contenuto *dei dati* (che devono essere specificate nell'appendice 11: Meccanismi comuni di sicurezza);

— i particolari in merito a concetti di dati diversi dall'RTM che possono essere ottenuti usando la stessa architettura e le stesse apparecchiature;

— i particolari in merito al comportamento e alla gestione tra VU e DSRC-VU e il comportamento nella DSRC-VU (diversi *dai dati* forniti su richiesta di un REDCR).

3 ACRONIMI, DEFINIZIONI E SIMBOLI

Nella presente appendice sono utilizzati i seguenti acronimi e le seguenti definizioni specifici:

l'antenna	dispositivo elettrico che trasforma l'energia elettrica in onde radio e viceversa, usato in combinazione con un trasmettitore o un ricevitore radio. Quando è in funzione, un trasmettitore radio fornisce ai terminali dell'antenna una corrente elettrica che oscilla a radiofrequenza e l'antenna irradia l'energia dalla corrente sotto forma di onde elettromagnetiche (onde radio). In modalità ricezione, un'antenna intercetta parte dell'energia di un'onda elettromagnetica per produrre un basso voltaggio ai terminali, che è applicato ad un ricevitore per essere amplificato.
la comunicazione	scambio di informazioni/dati tra un DSRC-REDCR e una DSRC-VU in conformità al paragrafo 5 in una relazione tra master e slave per ottenere *i dati*.
i dati	dati sicuri di formato definito (cfr. paragrafo 5.4.4) richiesti dal *DSRC-REDCR* e forniti al *DSRC-REDCR* dalla *DSRC-VU* tramite un collegamento DSRC 5,8 GHz come definito nel paragrafo 5 a seguire.
Regolamento (UE) n. 165/2014	Regolamento (UE) n. 165/2014 del Parlamento europeo e del Consiglio, del 4 febbraio 2014, relativo ai tachigrafi nel settore dei trasporti su strada, che abroga il regolamento (CEE) n. 3821/85 del Consiglio relativo all'apparecchio di controllo nel settore dei trasporti su strada e modifica il regolamento (CE) n. 561/2006 del Parlamento europeo e

▼B

	del Consiglio relativo all'armonizzazione di alcune disposizioni in materia sociale nel settore dei trasporti su strada.
AID	Identificativo dell'applicazione
BLE	Bluetooth a bassa energia
BST	Beacon Service Table (tabella di servizio del segnale)
CIWD	Inserimento carta durante la guida
CRC	Controllo di ridondanza ciclica
DSC (n)	Identificativo di un requisito per un'appendice DSRC specifica
DSRC	Comunicazione dedicata a corto raggio
DSRC-REDCR	DSRC — lettore della comunicazione remota a fini di diagnosi precoce
DSRC-VU	DSRC — unità elettronica di bordo. Si tratta del «meccanismo di diagnosi precoce remota» definito nell'allegato 1C.
DWVC	Guida in assenza di una carta valida
EID	Identificativo dell'elemento
LLC	Controllo del collegamento logico
LPDU	Unità dati del protocollo LLC
OWS	Sistema di pesatura di bordo
PDU	Unità dati del protocollo
REDCR	Lettore della comunicazione remota a fini di diagnosi precoce. Si tratta del «dispositivo di lettura della comunicazione remota a fini di diagnosi precoce» definito nell'allegato 1C.
RTM	Monitoraggio a distanza del tachigrafo
SM-REDCR	Modulo di sicurezza-Lettore della comunicazione remota a fini di diagnosi precoce
TARV	Telematics Applications for Regulated Vehicles (serie di norme ISO 15638)

▼B

VU	Unità elettronica di bordo
VUPM	Memoria del payload dell'unità elettronica di bordo
VUSM	Modulo di sicurezza dell'unità elettronica di bordo
VST	Vehicle Service Table (tabella di servizio del veicolo)
WIM	Rilevamento del peso con veicolo in movimento
WOB	Pesatura a bordo

La specifica definita nella presente appendice fa riferimento ai regolamenti e alle norme seguenti e dipende da essi nella loro interezza o in parte. Le clausole della presente appendice indicano le norme pertinenti o le clausole pertinenti delle norme. In caso di contraddizioni prevalgono le clausole della presente appendice. In caso di contraddizioni, laddove nella presente appendice non è determinata chiaramente nessuna specifica, prevale il rispetto di ERC 70-03 (e le prove per verificare la conformità ai parametri pertinenti di EN 300 674-1), seguito in ordine di preferenza discendente da EN 12795, EN 12253, EN 12834 e EN 13372, 6.2, 6.3, 6.4 e 7.1.

Di seguito sono elencati i regolamenti e le norme cui si fa riferimento nella presente appendice:

[1] Regolamento (UE) n. 165/2014 del Parlamento europeo e del Consiglio, del 4 febbraio 2014, relativo ai tachigrafi nel settore dei trasporti su strada, che abroga il regolamento (CEE) n. 3821/85 del Consiglio relativo all'apparecchio di controllo nel settore dei trasporti su strada e modifica il regolamento (CE) n. 561/2006 del Parlamento europeo e del Consiglio relativo all'armonizzazione di alcune disposizioni in materia sociale nel settore dei trasporti su strada.

[2] Regolamento (CE) n. 561/2006 del Parlamento europeo e del Consiglio, del 15 marzo 2006, relativo all'armonizzazione di alcune disposizioni in materia sociale nel settore dei trasporti su strada e che modifica i regolamenti del Consiglio (CEE) n. 3821/85 e (CE) n. 2135/98 e abroga il regolamento (CEE) n. 3820/85 del Consiglio (Testo rilevante ai fini del SEE).

[3] ERC 70-03 CEPT: ECC Recommendation 70-03: Relating to the Use of Short Range Devices (SRD).

[4] ISO 15638 Intelligent transport systems — Framework for cooperative telematics applications for regulated commercial freight vehicles (TARV).

[5] EN 300 674-1 Electromagnetic compatibility and Radio spectrum Matters (ERM); Road Transport and Traffic Telematics (RTTT); Dedicated Short Range Communication (DSRC) transmission equipment (500 kbit/s / 250 kbit/s) operating in the 5,8 GHz Industrial, Scientific and Medical (ISM) band; Part 1: General characteristics and test methods for Road Side Units (RSU) and On-Board Units (OBU).

[6] EN 12253 Road transport and traffic telematics — Dedicated short-range communication — Physical layer using microwave at 5.8 GHz.

▼B

[7] EN 12795 Road transport and traffic telematics — Dedicated short-range communication — Data link layer: medium access and logical link control.

[8] EN 12834 Road transport and traffic telematics — Dedicated short-range communication — Application layer.

[9] EN 13372 Road transport and traffic telematics — Dedicated short-range communication — Profiles for RTTT applications

[10] ISO 14906 Electronic fee collection — Application interface definition for dedicated short- range communication

4 SCENARI OPERATIVI

4.1 **Panoramica**

Il regolamento (UE) n. 165/2014 definisce gli scenari specifici e controllati entro cui si deve usare *la comunicazione*.

Gli scenari supportati sono:

«Profilo di comunicazione 1: ispezione dal lato della strada utilizzando un lettore della comunicazione remota a fini di diagnosi precoce a corto raggio senza fili che avvia un'ispezione fisica dal lato della strada (master-slave).

Profilo del lettore 1a: tramite un lettore della comunicazione remota a fini di diagnosi precoce sorretto e puntato manualmente o posizionato temporaneamente su un cavalletto a lato della strada e puntato.

Profilo del lettore 1b: tramite un lettore della comunicazione remota a fini di diagnosi precoce montato sul veicolo e puntato».

4.1.1 *Precondizioni per il trasferimento di dati tramite l'interfaccia DSRC 5,8 GHz*

NOTA: per capire il contesto delle precondizioni si prega di far riferimento alla figura 14.3 a seguire.

4.1.1.1 Dati memorizzati nella VU

DSC_12 È compito della VU aggiornare ogni 60 secondi e conservare i dati da archiviare al suo interno, senza interventi della funzione di comunicazione DSRC. I mezzi per conseguire questo obiettivo sono interni alla VU e sono specificati nel regolamento (UE) n. 165/2014, allegato 1C, paragrafo 3.19 «*Comunicazione remota per controlli su strada mirati*» e non sono specificati nella presente appendice.

4.1.1.2 Dati forniti al dispositivo DSRC-VU

DSC_13 È compito della VU aggiornare i dati DSRC del tachigrafo (*i dati*) ogniqualvolta i dati memorizzati nella VU sono aggiornati agli intervalli determinati al paragrafo 4.1.1.1 (DSC_12), senza interventi della funzione di comunicazione DSRC.

DSC_14 I dati della VU vanno utilizzati come base per popolare e aggiornare *i dati*; i mezzi per raggiungere tale obiettivo sono specificati nell'allegato 1C, paragrafo 3.19 «*Comunicazione remota per controlli su strada mirati*» o in assenza di tale specifica, sono una funzione della progettazione del prodotto e non sono specificati nella presente appendice. Per la struttura del collegamento tra il dispositivo DSRC-VU e la VU si prega di far riferimento al paragrafo 5.6.

▼B

4.1.1.3 Contenuto dei dati

DSC_15 Il contenuto e il formato *dei dati* devono essere tali da consentire che, una volta decriptati, i dati siano strutturati e resi disponibili nella forma e nel formato specificati al paragrafo 5.4.4 della presente appendice (Strutture dei dati).

4.1.1.4 Presentazione dei dati

DSC_16 *I dati*, che sono stati tenuti frequentemente aggiornati secondo le procedure di cui al paragrafo 4.1.1.1, devono essere resi sicuri prima di essere presentati alla *DSRC-VU* e devono essere presentati come un valore sicuro del concetto di dati per essere temporaneamente memorizzati nella *DSRC-VU* quale versione corrente *dei dati*. Questi dati sono trasferiti dal *VUSM* alla funzione DSRC *VUMP*. *VUSM* e *VUPM* sono funzioni e non necessariamente entità fisiche. La forma di istanziazione fisica per eseguire queste funzioni deve essere una questione di progettazione del prodotto salvo altra indicazione nel regolamento (UE) n. 165/2014.

4.1.1.5 Dati di sicurezza

DSC_17 I dati di sicurezza (*securityData)*, compresi i dati richiesti dal *REDCR* per completare la sua capacità di decriptare *i dati*, devono essere forniti come definito nell'appendice 11 (Meccanismi comuni di sicurezza) e presentati come un valore del concetto di dati per essere temporaneamente memorizzati nella *DSRC-VU* quale versione corrente dei *securityData* nella forma definita al paragrafo 5.4.4 della presente appendice.

4.1.1.6 Dati VUMP disponibili per essere trasferiti tramite l'interfaccia DSRC

DSC_18 Il concetto di dati che deve sempre essere disponibile nella funzione DSRC VUMP per il trasferimento immediato su richiesta del *REDCR* è definito al paragrafo 5.4.4 per le specifiche complete del modulo ASN.1.

Panoramica generale del profilo di comunicazione 1

Questo profilo riguarda il caso di impiego in cui un agente delle autorità di controllo competenti usa un lettore della comunicazione remota a fini di diagnosi precoce (*il REDCR*) per una comunicazione remota a corto raggio (interfacce DSRC 5,8 GHz che funzionano in conformità alla norma ERC 70-03 e sono testate per verificarne la conformità ai parametri pertinenti di EN 300 674-1, come descritto al paragrafo 5) finalizzata ad identificare a distanza un veicolo che potrebbe violare il regolamento (UE) n. 165/2014. Una volta identificato, l'agente delle autorità di controllo competenti, che sta controllando il dispositivo di interrogazione, decide se il veicolo debba essere fermato.

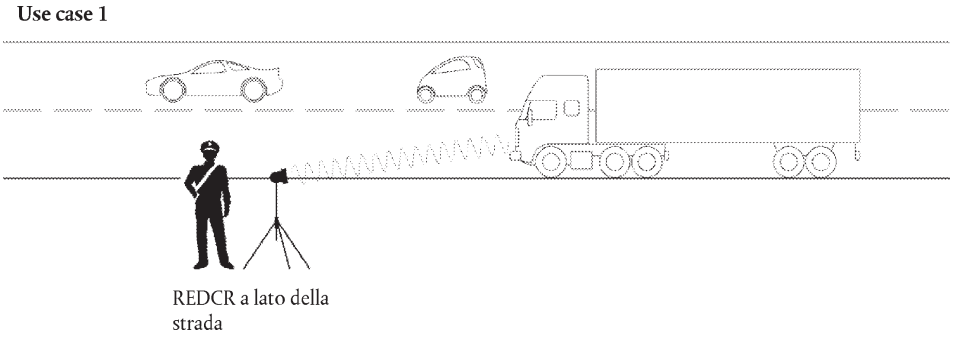
4.1.2 *Profilo 1a: con un lettore della comunicazione remota a fini di diagnosi precoce sorretto e puntato manualmente o posizionato su un cavalletto a lato della strada e puntato*

In questo caso d'impiego, l'agente delle autorità di controllo competenti è posizionato a lato della strada e punta un *REDCR*, che regge in mano o che è montato su un cavalletto o su un sostegno simile, dal ciglio della strada al centro del parabrezza del veicolo bersaglio. L'interrogazione avviene tramite interfacce DSRC 5,8 GHz che funzionano in conformità alla norma ERC 70-03 e sono testate per verificarne la conformità ai parametri pertinenti di EN 300 674-1, come descritto al paragrafo 5. Cfr. la figura 14.1 (Caso d'impiego 1).

▼B

Figura 14.1

Interrogazione dal lato della strada tramite interfacce DSRC 5,8 GHz

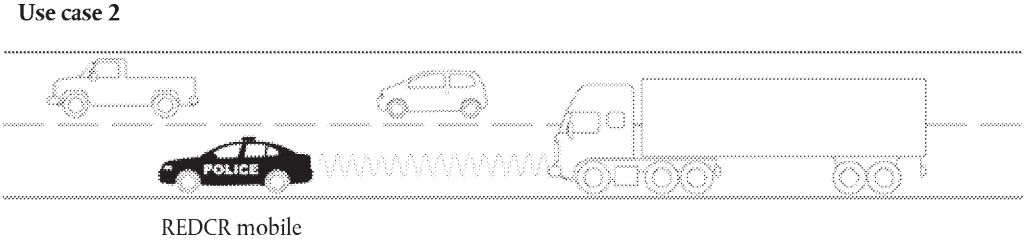


4.1.3 *Profilo 1b: con un lettore della comunicazione remota a fini di diagnosi precoce (REDCR) montato sul veicolo e puntato*

In questo caso d'impiego, l'agente delle autorità di controllo competenti si trova su un veicolo in movimento e punta un *REDCR* portatile, che regge in mano, dal veicolo al centro del parabrezza del veicolo bersaglio oppure il *REDCR* è montato nel o sul veicolo in modo da puntare verso il centro del parabrezza del veicolo bersaglio quando il veicolo in cui si trova il lettore della comunicazione remota a fini di diagnosi precoce è in una particolare posizione rispetto al veicolo bersaglio, ad esempio direttamente davanti ad esso in un flusso di traffico. L'interrogazione avviene tramite interfacce DSRC 5,8 GHz che funzionano in conformità alla norma ERC 70-03 e sono testate per verificarne la conformità ai parametri pertinenti di EN 300 674-1, come descritto al paragrafo 5. Cfr. la figura 14.2. (Caso d'impiego 2).

Figura 14.2

Interrogazione da un veicolo tramite interfacce DSRC 5,8 GHz



4.2 **Sicurezza/integrità**

Per consentire la verifica dell'autenticità e dell'integrità dei dati trasferiti tramite comunicazione remota, *i dati* sicuri sono verificati e decriptati conformemente all'appendice 11 (Meccanismi comuni di sicurezza).

5 STRUTTURA E PROTOCOLLI DI COMUNICAZIONE REMOTA

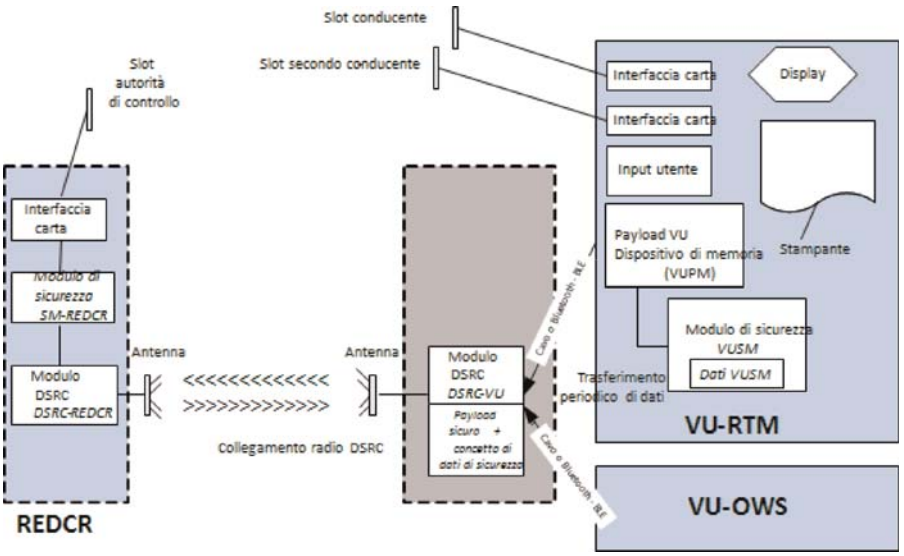
5.1 **Struttura**

La struttura della funzione di comunicazione remota nel tachigrafo intelligente è illustrata nella figura 14.3.

▼B

Figura 14.3

Struttura della funzione di comunicazione remota



DSC_19 Le seguenti funzioni si trovano nella VU:

— modulo di sicurezza (*VUSM*). Questa funzione presente nella VU è responsabile della sicurezza *dei dati* che devono essere trasmessi dalla *DSRC-VU* all'agente delle autorità di controllo competenti tramite comunicazione remota.

— I dati sicuri sono memorizzati nella memoria VUSM. Agli intervalli determinati al paragrafo 4.1.1.1 (DSC_12), la VU cripta e ricostituisce il concetto di dati RTM conservato nella memoria della DSRC-VU. Tale concetto di dati RTM comprende i valori del concetto di dati del payload e di sicurezza determinati più avanti nella presente appendice. Il funzionamento del modulo di sicurezza è definito nell'appendice 11 (Meccanismi comuni di sicurezza) ed esula dal campo di applicazione della presente appendice, salvo l'obbligo di fornire aggiornamenti al dispositivo di comunicazione della VU ogni volta che cambiano i dati della VUSM.

— La comunicazione tra la VU e la DSRC-VU può essere cablata o Bluetooth a bassa energia (BLE) e la DSRC-VU può essere integrata nell'antenna sul parabrezza del veicolo, nella VU o posizionata tra le due.

— La DSRC-VU deve avere una fonte affidabile di energia sempre disponibile. La modalità di fornitura dell'energia alla DSRC-VU è una decisione progettuale.

— La memoria della DSRC-VU deve essere non volatile per conservare *i dati* anche quando il veicolo viene spento.

— Se la comunicazione tra la VU e la DSRC-VU avviene tramite BLE e la fonte di energia è una batteria non ricaricabile, tale fonte di energia deve essere sostituita ad ogni ispezione periodica e il fabbricante delle apparecchiature della DSRC-VU è responsabile di garantire che la fornitura

▼B

di energia copra il periodo tra due ispezioni periodiche, assicurando l'accesso usuale ai dati da parte di un REDCR per tutto il periodo senza malfunzionamenti o interruzioni.

— Dispositivo di memoria dei dati utili trasmessi dalla VU durante l'RTM (*VUPM*). Questa funzione presente nella VU è responsabile della fornitura e dell'aggiornamento *dei dati*. Il contenuto *dei dati* («TachographPayload») è definito ai paragrafi 5.4.4/5.4.5 a seguire ed è aggiornato agli intervalli determinati al paragrafo 4.1.1.1 (DSC_12).

— DSRC-VU. Questa funzione, integrata o collegata all'antenna e in comunicazione con la VU tramite una connessione cablata o senza fili (BLE), contiene i dati correnti (*dati della VUMP)* e gestisce la risposta ad un'interrogazione attraverso l'interfaccia DSRC 5,8 GHz. Lo scollegamento del dispositivo DSRC o l'interferenza con il suo funzionamento durante il normale funzionamento del veicolo saranno interpretati come una violazione del regolamento (UE) n. 165/2014.

— Il modulo di sicurezza (REDCR) (*SM-REDCR*) è la funzione usata per decriptare e controllare l'integrità dei dati provenienti dalla VU. Le modalità di esecuzione di tali operazioni sono definite nell'appendice 11 (Meccanismi comuni di sicurezza) e non nella presente appendice.

— La funzione (REDCR) del dispositivo DSRC (*DSRC-REDCR*) comprende un ricetrasmettitore 5,8 GHz e il firmware e il software associati che gestiscono *la comunicazione* con la *DSRC-VU* secondo la presente appendice.

— Il *DSRC-REDCR* interroga la *DSRC-VU* del veicolo bersaglio, ottiene *i dati* (i *dati della VUPM* correnti del veicolo bersaglio) tramite il collegamento DSRC e elabora e memorizza i dati ricevuti nel suo *SM-REDCR*.

— L'antenna *DSRC-VU* (l'antenna) deve essere posizionata in modo da ottimizzare la comunicazione DSRC tra il veicolo e l'antenna a lato della strada (generalmente al centro o in prossimità del centro del parabrezza del veicolo). Per i veicoli pesanti, ciò significa entro o in prossimità della parte inferiore del parabrezza. Sui veicoli leggeri è appropriato installarla nella parte superiore del parabrezza.

— Non devono esserci oggetti metallici (ad esempio, cartellini con il nome, adesivi, strisce antiriflesso (colorate), parasole, tergicristallo a riposo) davanti o vicino all'antenna, che possano interferire con la comunicazione.

— L'antenna va montata in modo che il suo asse di puntamento sia all'incirca parallelo alla superficie della strada.

▼B

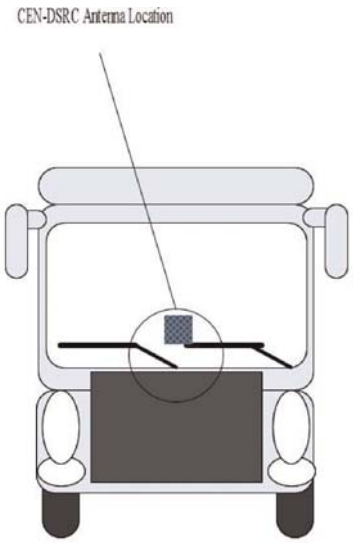
DSC_20 L'antenna e la comunicazione devono funzionare in conformità alla norma ERC 70-03 e devono essere testate per verificarne la conformità ai parametri pertinenti di EN 300 674-1, come descritto nel paragrafo 5. L'antenna e la comunicazione possono applicare tecniche di mitigazione del rischio di interferenze senza fili, come descritto nella relazione 228 dell'ECC, utilizzando, ad esempio, filtri nella comunicazione CEN DSRC 5,8 GHz.

DSC_21 L'antenna DSRC deve essere collegata al dispositivo DSRC-VU direttamente nel modulo montato sul o in prossimità del parabrezza o tramite un cavo dedicato costruito in modo da renderne difficile lo scollegamento non autorizzato. Lo scollegamento o l'interferenza col funzionamento dell'antenna saranno considerati una violazione del regolamento (UE) n. 165/2014. La schermatura deliberata o qualsiasi stratagemma per impedire all'antenna di funzionare correttamente saranno interpretati come una violazione del regolamento (UE) n. 165/2014.

DSC_22 Il fattore di forma dell'antenna non è definito ed è una decisione commerciale, purché la DSRC-VU montata soddisfi i requisiti di conformità definiti nel paragrafo 5 di seguito. L'antenna deve essere posizionata come determinato in DSC_19 e illustrato nella figura 14.4 (linea ovale) e deve supportare efficacemente i casi d'impiego descritti ai paragrafi 4.1.2 e 4.1.3.

Figura 14.4

Esempio di posizionamento dell'antenna DSRC 5,8 GHz sul parabrezza dei veicoli oggetto del regolamento



Il fattore di forma *del REDCR* e della sua antenna può variare a seconda che il lettore sia montato su un cavalletto, tenuto in mano, montato sul veicolo, ecc. e secondo il modus operandi dell'agente delle autorità di controllo competenti.

Si usa una funzione di visualizzazione e/o di notifica per presentare i risultati della funzione di comunicazione remota all'agente delle autorità di controllo competenti. Tali risultati possono essere visualizzati sullo schermo, stampati, segnalati acusticamente o si può usare una combinazione di questi sistemi. La forma di tale visualizzazione e/o notifica dipende dalle esigenze degli agenti delle autorità di controllo competenti e dalla progettazione delle apparecchiature e non è specificata nella presente appendice.

▼B

DSC_23 Il progetto e il fattore di forma del *REDCR* sono una questione di design commerciale, nel rispetto della norma ERC 70-03 e delle specifiche concernenti il progetto e le prestazioni di cui alla presente appendice (paragrafo 5.3.2). In questo modo è garantita massima flessibilità di mercato per progettare e fornire apparecchiature adatte agli scenari di interrogazione specifici delle diverse autorità di controllo competenti.

DSC_24 Il progetto e il fattore di forma della *DSRC-VU* e il suo posizionamento all'interno o all'esterno della VU sono una questione di design commerciale, nel rispetto della norma ERC 70-03 e delle specifiche concernenti il progetto e le prestazioni di cui alla presente appendice (paragrafo 5.3.2) e alla presente clausola (5.1).

DSC_25 La *DSRC-VU* deve tuttavia essere ragionevolmente in grado di accettare valori dei concetti di dati di altre apparecchiature intelligenti del veicolo, ad esempio da dispositivi di pesatura a bordo, grazie a un collegamento e a protocolli comuni standard aperti, purché tali concetti di dati siano identificati da identificativi dell'applicazione/nomi di file noti. Le istruzioni per il funzionamento di tali protocolli devono essere messe a disposizione della Commissione europea e dei fabbricanti delle apparecchiature pertinenti gratuitamente.

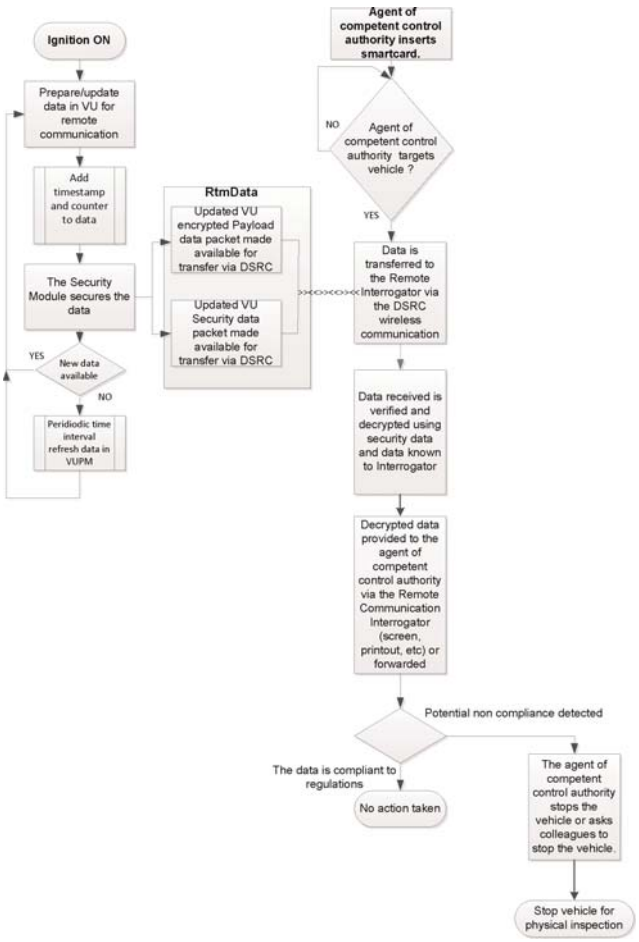
5.2 **Sequenza**

5.2.1 *Operazioni*

La sequenza delle operazioni è rappresentata nella figura 14.5.

Figura 14.5

Sequenza della funzione di comunicazione remota



▼B

Le fasi sono descritte di seguito:

a. quando il veicolo è in funzione (accensione ON), il tachigrafo invia dati alla funzione VU. La funzione VU prepara *i dati* (criptati) per la funzione di comunicazione remota e aggiorna la *VUPM* conservata nella memoria della *DSRC-VU* (come definita ai paragrafi 4.1.1.1 e 4.1.1.2). *I dati* raccolti devono essere formattati come prescritto ai paragrafi 5.4.4 e 5.4.5 a seguire.

b. Ogni volta che *i dati* sono aggiornati, deve essere aggiornato il time-Stamp definito nel concetto di dati di sicurezza.

c. La funzione *VUSM* rende i dati sicuri secondo le procedure definite nell'appendice 11.

d. Ogni volta che *i dati* sono aggiornati (cfr. i paragrafi 4.1.1.1 e 4.1.1.2), essi sono trasferiti alla *DSRC-VU*, dove sostituiscono gli eventuali dati precedenti, in modo che i dati correnti aggiornati (*i dati*) siano sempre disponibili e possano sempre essere forniti ad un *REDCR* in caso di interrogazione. Quando *i dati* sono forniti dalla VU alla DSRC-VU, essi devono essere identificabili dal nome del file *RTMData* o tramite identificativi dell'applicazione e dell'attributo.

e. Se un agente delle autorità di controllo competenti vuole raccogliere *i dati* di un veicolo, egli deve innanzitutto inserire la propria smartcard nel *REDCR* per consentire *la comunicazione* e per consentire all'*SM-REDCR* di verificare l'autenticità dei dati e di decriptarli.

f. Poi l'agente dell'autorità di controllo competente punta un veicolo e ne richiede i dati tramite comunicazione remota. Il *REDCR,* tramite l'interfaccia DSRC 5,8 GHz, apre una sessione con la *DSRC-VU* del veicolo bersaglio e richiede *i dati*. *I dati* sono trasferiti al *REDCR* tramite il sistema di comunicazione senza fili come un attributo DSRC usando l'applicazione GET definita al paragrafo 5.4. L'attributo contiene i valori criptati del payload e i dati di sicurezza DSRC.

g. I dati sono analizzati dalle apparecchiature *REDCR* e forniti all'agente dell'autorità di controllo competente.

h. L'agente dell'autorità di controllo competente usa i dati per decidere se fermare o meno il veicolo per ispezionarlo nel dettaglio o se chiedere ad un altro agente dell'autorità di controllo competente di fermare il veicolo.

5.2.2 *Interpretazione dei dati ricevuti tramite la comunicazione DSRC*

DSC_26 I dati ricevuti tramite l'interfaccia 5,8 GHz devono conservare esclusivamente il significato e il valore definiti ai successivi paragrafi 5.4.4 e 5.4.5 e devono essere intesi nel quadro degli obiettivi ivi definiti. In conformità alle disposizioni del regolamento (UE) n. 165/2014, *i dati* devono essere usati esclusivamente per fornire informazioni pertinenti ad un'autorità di

▼B

controllo competente per aiutare gli agenti a decidere quali veicoli fermare per ispezionarli fisicamente e devono essere successivamente distrutti in conformità all'articolo 9 del regolamento (UE) n. 165/2014.

5.3 **Parametri dell'interfaccia fisica DSRC per la comunicazione remota**

5.3.1 *Vincoli relativi alla posizione*

DSC_27 L'interrogazione remota dei veicoli tramite un'interfaccia DSRC 5,8 GHz non va usata nel raggio di 200 metri da un carroponte DSRC 5,8 GHz operativo.

5.3.2 *Parametri di downlink e uplink*

DSC_28 Le apparecchiature usate per il monitoraggio remoto dei tachigrafi devono essere conformi alla norma ERC 70-03 e funzionare secondo i parametri definiti nelle tabelle 14.1 e 14.2 a seguire.

DSC_29 Inoltre, per garantire la compatibilità ai parametri operativi di altri sistemi DSRC 5,8 GHz standardizzati, le apparecchiature usate per il monitoraggio remoto dei tachigrafi devono rispettare i parametri delle norme EN 12253 e EN 13372.

Nello specifico:

Tabella 14.1

Parametri di downlink

Voce n.	Parametro	Valori	Osservazioni
D1	Frequenze di downlink del vettore	Ci sono quattro alternative che possono essere usate da un REDCR: 5,7975 GHz 5,8025 GHz 5,8075 GHz 5,8125 GHz	In conformità alla norma ERC 70-03. Le frequenze del vettore possono essere scelte da chi usa il sistema a lato della strada e non devono essere note alla DSRC-VU (In conformità alle norme EN 12253 e EN 13372)
D1a (*)	Tolleranza del vettore Frequenze	entro ± 5 ppm	(In conformità alla norma EN 12253)
D2 (*)	Maschera di spettro del trasmettitore RSU (REDCR)	In conformità alla norma ERC 70-03. Il REDCR deve essere conforme alla classe B,C come definita in EN 12253 Nessun'altra prescrizione specifica nel quadro del presente allegato	Parametro usato per controllare l'interferenza tra interrogatori in prossimità (come definiti in EN 12253 e EN 13372)
D3	Intervallo minimo della frequenza dell'OBU (DSRC-VU)	5,795 — 5,815 GHz	(In conformità alla norma EN 12253)
D4 (*)	E.I.R.P. massimo	In conformità alla norma ERC 70-03 (senza licenza) e alle norme nazionali Massimo + 33 dBm	(In conformità alla norma EN 12253)

▼B

Voce n.	Parametro	Valori	Osservazioni
D4a	Maschera angolare dell'E.I.R.P.	Secondo le specifiche dichiarate e pubblicate del progettista dell'interrogatore	(In conformità alla norma EN 12253)
D5	Polarizzazione	Circolare antioraria	(In conformità alla norma EN 12253)
D5a	Polarizzazione incrociata	XPD: Sull'asse di puntamento: (REDCR) RSU t ≥ 15 dB (DSRC-VU) OBU r ≥ 10 dB Nella zona -3 dB: (REDCR) RSU t ≥ 10 dB (DSRC-VU) OBU r ≥ 6 dB	(In conformità alla norma EN 12253)
D6 (*)	Modulazione	Modulazione a due livelli dell'ampiezza.	(In conformità alla norma EN 12253)
D6a (*)	Indice di modulazione	0,5 … 0,9	(In conformità alla norma EN 12253)
D6b	Diagramma ad occhio	≥ 90 % (tempo) / ≥ 85 % (ampiezza)	
D7 (*)	Codifica dei dati	FM0 Il bit “1” ha transizioni solo all'inizio e alla fine dell'intervallo di bit. Il bit “0” ha un'ulteriore transizione al centro dell'intervallo di bit rispetto al bit “1”	(In conformità alla norma EN 12253)
D8 (*)	Velocità di trasmissione	500 kBit/s	(In conformità alla norma EN 12253)
D8a	Tolleranza del Bit Clock	Meglio di ± 100 ppm	(In conformità alla norma EN 12253)
D9 (*)	Tasso d'errore di bit (B.E.R.) per la comunicazione	$\leq 10^{-6}$ quando la potenza incidente all'OBU (DSRC-VU) rientra nell'intervallo [da D11a a D11b].	(In conformità alla norma EN 12253)
D10	Wake-up trigger (segnale di riattivazione) per l'OBU (DSRC-VU)	L'OBU (DSRC-VU) si deve svegliare al ricevimento di un frame con 11 o più ottetti (incluso il preambolo)	Non è necessaria nessuna sequenza di riattivazione speciale La DSRC-VU può svegliarsi al ricevimento di un frame con meno di 11 ottetti (In conformità alla norma EN 12253)
D10a	Tempo di inizio massimo	≤ 5 ms	(In conformità alla norma EN 12253)
D11	Zona di comunicazione	Regione spaziale entro la quale si ottiene un B.E.R. secondo D9a	(In conformità alla norma EN 12253)
D11a (*)	Limite di potenza per la comunicazione (superiore)	-24dBm	(In conformità alla norma EN 12253)

▼B

Voce n.	Parametro	Valori	Osservazioni
D11b (*)	Limite di potenza per la comunicazione (inferiore)	Potenza incidente: –43 dBm (asse di puntamento) – 41 dBm [tra – 45° e + 45°, corrispondente al piano parallelo alla superficie stradale quando la DSRC-VU è successivamente installata sul veicolo (azimut)]	(In conformità alla norma EN 12253) Prescrizione estesa per gli angoli orizzontali fino a ± 45°, in virtù dei casi d'impiego definiti nel presente allegato
D12 (*)	Livello della potenza di interruzione della (DSRC-VU)	– 60 dBm	(In conformità alla norma EN 12253)
D13	Preambolo	Il preambolo è obbligatorio	(In conformità alla norma EN 12253)
D13a	Lunghezza e configurazione del preambolo	16 bit ± 1 bit di FM0 codificato “1” bit	(In conformità alla norma EN 12253)
D13b	Forma dell'onda del preambolo	Una sequenza alternata di livello basso e livello alto con una durata dell'impulso di 2 μs La tolleranza è data da D8a	(In conformità alla norma EN 12253)
D13c	Trailing bits (bit più a destra)	L'RSU (REDCR) può trasmettere un massimo di 8 bit dopo l'indicatore di fine. Un OBU (DSRC-VU) non deve tenere in considerazione questi bit aggiuntivi	(In conformità alla norma EN 12253)

(*) I parametri di downlink devono superare le prove di conformità per i parametri specificate nella norma EN 300 674-1

Tabella 14.2

Parametri di uplink

Voce n.	Parametro	Valori	Osservazioni
U1 (*)	Frequenze del sottoportante	Un OBU (DSRC-VU) deve supportare 1,5 MHz e 2,0 MHz Un RSU (REDCR) deve supportare 1,5 MHz o 2,0 MHz o entrambi. U1-0: 1,5 MHz U1-1: 2,0 MHz	Scelta della frequenza del sottoportante (1,5 MHz o 2,0 MHz) secondo il profilo EN 13372 scelto
U1a (*)	Tolleranza delle frequenze del sottoportante	Entro ± 0,1 %	(In conformità alla norma EN 12253)
U1b	Uso di bande laterali	Stessi dati su entrambi i lati	(In conformità alla norma EN 12253)
U2 (*)	Maschera di spettro del trasmettitore OBU (DSRC-VU)	Secondo la norma EN 12253 1) Potenza fuori banda: cfr. ETSI EN 300674-1	(In conformità alla norma EN 12253)

▼B

Voce n.	Parametro	Valori	Osservazioni
		2) Potenza in banda: [U4a] dBm in 500 kHz 3) Emissione in qualsiasi altro canale uplink: U2(3)-1 = – 35 dBm in 500 kHz	
U4a (*)	E.I.R.P massimo con banda laterale unica (asse di puntamento)	Due opzioni: U4a-0: -14 dBm U4a-1: -21 dBm	Secondo le specifiche dichiarate e pubblicate del progettista delle apparecchiature
U4b (*)	E.I.R.P massimo con banda laterale unica (35°)	Due opzioni: — Non applicabile — – 17dBm	Secondo le specifiche dichiarate e pubblicate del progettista delle apparecchiature
U5	Polarizzazione	Circolare antioraria	(In conformità alla norma EN 12253)
U5a	Polarizzazione incrociata	XPD: Sull'asse di puntamento: (REDCR) RSU r ≥ 15 dB (DSRC-VU) OBU t ≥ 15 dB In – 3 dB: (REDCR) RSU r ≥ 10 dB (DSRC-VU) OBU t ≥ 6 dB	(In conformità alla norma EN 12253)
U6	Modulazione del sottoportante	2-PSK Dati codificati sincronizzati con il sottoportante: le transizioni dei dati codificati coincidono con le transizioni del sottoportante.	(In conformità alla norma EN 12253)
U6b	Ciclo di lavoro	Ciclo di lavoro: 50 % ± α, α ≤ 5 %	(In conformità alla norma EN 12253)
U6c	Modulazione sul vettore	Moltiplicazione del sottoportante modulato per il vettore	(In conformità alla norma EN 12253)
U7 (*)	Codifica dei dati	NRZI (nessuna transizione all'inizio del bit "1", transizione all'inizio del bit "0", nessuna transizione all'interno del bit)	(In conformità alla norma EN 12253)
U8 (*)	Velocità di trasmissione	250 kbit/s	(In conformità alla norma EN 12253)
U8a	Tolleranza del Bit Clock	Entro ± 1 000 ppm	(In conformità alla norma EN 12253)
U9	Tasso d'errore di bit (B.E.R.) per la comunicazione	$\leq 10^{-6}$	(In conformità alla norma EN 12253)

▼B

Voce n.	Parametro	Valori	Osservazioni
U11	Zona di comunicazione	La regione spaziale in cui è situata la DSRC-VU in modo tale che le sue trasmissioni siano ricevute dal REDCR con un B.E.R. inferiore a quello dato in U9a	(In conformità alla norma EN 12253)
U12a (*)	Guadagno di conversione (limite inferiore)	1 dB per ciascuna banda laterale Ampiezza dell'angolo: circolarmente simmetrica tra l'asse di puntamento e ± 35° e	
		tra – 45° e + 45°, corrispondente al piano parallelo alla superficie stradale quando la DSRC-VU è successivamente installata sul veicolo (azimut)	Ampiezza maggiore del valore specificato per gli angoli orizzontali fino a ± 45°, in virtù dei casi d'impiego definiti nel presente allegato
U12b (*)	Guadagno di conversione (limite superiore)	10 dB per ciascuna banda laterale	Ampiezza minore del valore specificato per ciascuna banda laterale entro un cono circolare attorno ad un asse di puntamento con un di angolo di apertura di ± 45°
U13	Preambolo	Il preambolo è obbligatorio	(In conformità alla norma EN 12253)
U13a	Preambolo Lunghezza e configurazione	Da 32 a 36 µs modulati solo con il sottoportante, poi 8 bit di bit “0” codificati NRZI	(In conformità alla norma EN 12253)
U13b	Trailing bits (bit più a destra)	La DSRC-VU può trasmettere un massimo di 8 bit dopo l'indicatore di fine Un RSU (REDCR) non deve tenere in considerazione questi bit aggiuntivi	(In conformità alla norma EN 12253)

(*) I parametri di uplink devono superare le prove di conformità per i parametri specificate nella norma EN 300 674-1

5.3.3 *Progettazione dell'antenna*

5.3.3.1 Antenna del REDCR

DSC_30 La progettazione dell'antenna del *REDCR* è una questione di design commerciale. L'antenna deve funzionare entro i limiti di cui al paragrafo 5.3.2, che sono adattati per ottimizzare le prestazioni di lettura del *DSRC-REDCR* per la finalità specifica e alle situazioni di lettura per cui il *REDCR* è stato progettato per funzionare.

5.3.3.2 Antenna della VU

DSC_31 La progettazione dell'antenna della *DSRC-VU* è una questione di design commerciale. L'antenna deve funzionare entro i limiti di cui al paragrafo 5.3.2, che sono adattati per ottimizzare le prestazioni di lettura del *DSRC-REDCR* per la finalità specifica e alle situazioni di lettura per cui il *REDCR* è stato progettato per funzionare.

▼B

DSC_32 L'antenna della VU deve essere fissata sul o in prossimità del parabrezza del veicolo, come specificato al precedente paragrafo 5.1.

DSC_33 In un ambiente di prova in un'officina (cfr. il paragrafo 6.3), un'antenna della DSRC-VU, fissata in conformità al precedente paragrafo 5.1, deve collegarsi correttamente con una comunicazione standard di prova e deve fornire correttamente una transazione RTM, come definita nella presente appendice, a una distanza tra 2 e 10 metri, per oltre il 99 % del tempo, facendo la media su oltre 1 000 interrogazioni di lettura.

5.4 **Requisiti del protocollo DSRC per l'RTM**

5.4.1 *Panoramica*

DSC_34 Il protocollo di transazione per scaricare *i dati* tramite il collegamento all'interfaccia DSRC 5,8 GHz deve essere conforme alle fasi descritte di seguito. La presente sezione descrive un flusso di transazioni in condizioni ideali, senza ritrasmissioni o interruzioni della comunicazione.

NOTA La finalità della fase di inizializzazione (Fase 1) consiste nello stabilire una comunicazione tra il *REDCR* e le DSRC-VU che sono entrate nella zona di transazione (master-slave) DSRC 5,8 GHz, ma che non hanno ancora stabilito una comunicazione con il *REDCR,* e nell'informarne i processi applicativi.

— **Fase 1** Inizializzazione. Il *REDCR* invia un frame contenente una «tabella di servizio del segnale» (BST), che include gli identificativi dell'applicazione (AID) nell'elenco dei servizi che supporta. Nell'applicazione RTM, si tratterà semplicemente del servizio con il valore AID = 2 (Freight&Fleet = carico e parco veicoli). La *DSRC-VU* valuta la BST ricevuta e deve rispondere (vedi oltre) con l'elenco delle applicazioni supportate nel dominio Freight&Fleet o, se non è supportata nessuna applicazione, non deve rispondere. Se il *REDCR* non offre AID = 2, la DSRC-VU non deve rispondergli.

— **Fase 2** La *DSRC-VU* invia un frame contenente una richiesta di allocazione di finestra privata.

— **Fase 3** Il *REDCR* invia un frame contenente un'allocazione di finestra privata.

— **Fase 4** La *DSRC-VU* usa la finestra privata allocata per inviare un frame contenente la sua tabella di servizio del veicolo (VST). Questa VST comprende un elenco di tutte le diverse istanziazioni delle applicazioni che questa *DSRC-VU* supporta nel quadro di AID = 2. Le diverse istanziazioni devono essere identificate per mezzo di EID generati univocamente, ciascuno associato ad un valore del parametro «segnale contestuale dell'applicazione» indicante l'applicazione e la norma supportate.

— **Fase 5** A questo punto il *REDCR* analizza la VST offerta e termina la connessione (RELEASE), perché non è interessato a nulla di ciò che la VST ha da offrire (vale a dire che sta ricevendo una VST da una *DSRC-VU* che non supporta la transazione RTM) oppure, se riceve una VST appropriata, avvia un'istanziazione dell'applicazione.

▼B

— **Fase 6** Per fare ciò, il REDCR deve inviare un frame contenente un comando per recuperare i dati RTM, identificando l'istanziazione dell'applicazione RTM specificando l'identificativo corrispondente (come specificato dalla DSRC-VU nella VST), e deve allocare una finestra privata.

— **Fase 7** La *DSRC-VU* usa la finestra privata appena allocata per inviare un frame contenente l'identificativo cui si rivolge, corrispondente all'istanziazione dell'applicazione RTM come fornita nella VST, seguito dall'attributo *RtmData* (elemento del payload + elemento di sicurezza).

— **Fase 8** Se sono richiesti più servizi, il valore 'n' è sostituito dal numero di riferimento del servizio successivo e il processo è ripetuto.

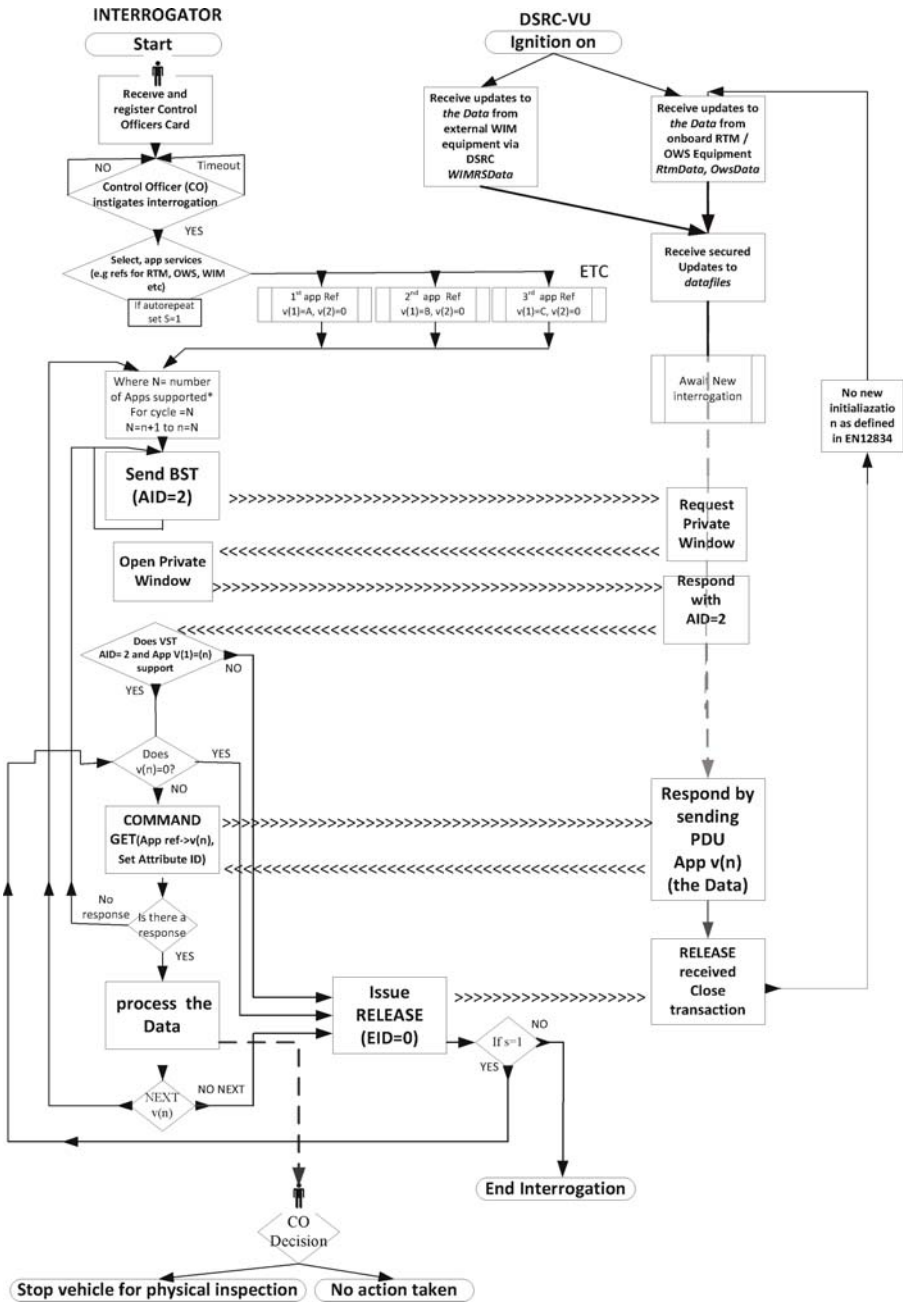
— **Fase 9** Il *REDCR* conferma la ricezione dei dati inviando un frame contenente un comando RELEASE alla *DSRC-VU* per concludere la sessione OPPURE, se non è riuscito a convalidare una ricezione corretta dell'LDPU, torna alla fase 6.

Cfr. la figura 14.6 per una raffigurazione del protocollo di transazione.

▼B

Figura 14.6

Fasi del processo RTM tramite DSRC 5,8 GHz



5.4.2 *Comandi*

DSC_35 I seguenti comandi sono le uniche funzioni usate in una fase di transazione RTM

— **INITIALISATION.request**: comando inviato dal REDCR sotto forma di una trasmissione con definizione delle applicazioni supportate dal REDCR.

— **INITIALISATION.response**: risposta da parte della DSRC-VU che conferma la connessione e che contiene un elenco di istanze applicative supportate con caratteristiche e informazioni su come gestirle (EID).

▼B

— **GET.request**: comando, inviato dal *REDCR* alla *DSRC-VU*, che specifica l'istanziazione dell'applicazione da considerare per mezzo di un EID definito, come ricevuto nella VST, e dà istruzioni alla *DSRC-VU* di inviare gli attributi scelti con *i dati*. L'obiettivo del comando GET è che il *REDCR* ottenga *i dati* dalla *DSRC-VU*.

— **GET.response**: risposta dalla DSRC-VU che contiene *i dati* richiesti.

— **ACTION.request ECHO**: comando che dà istruzioni alla *DSRC-VU* di rimandare dati al *REDCR*. L'obiettivo del comando ECHO è di permettere alle officine o ai laboratori di prova per il rilascio delle omologazioni di verificare che il collegamento DSRC funzioni senza bisogno di accedere alle credenziali di sicurezza.

— **ACTION**.response ECHO: una risposta da parte della DSRC-VU al comando ECHO.

— **EVENT_REPORT.request** RELEASE: un comando che informa la *DSRC-VU* che la transazione è conclusa. L'obiettivo del comando RELEASE è concludere la sessione con la *DSRC-VU*. Al ricevimento del RELEASE, la *DSRC-VU* non deve rispondere a nessun'altra interrogazione nel corso della connessione corrente. Si noti che secondo la norma EN 12834, una DSRC-VU non si collegherà due volte allo stesso interrogatore, a meno che non si sia trovata al di fuori della zona di comunicazione per 255 secondi o che l'ID del segnale dell'interrogatore non sia cambiato.

5.4.3 *Sequenza di comandi di interrogazione*

DSC_36 Dal punto di vista della sequenza di comandi e risposte, la transazione è descritta come segue:

Sequenza	Mittente		Destinatario	Descrizione	Azione
1	REDCR	>	DSRC-VU	Inizializzazione della comunicazione collegamento — richiesta	Il REDCR trasmette la BST
2	*DSRC-VU*	>	*REDCR*	*Inizializzazione della comunicazione collegamento — risposta*	*Se la BST supporta AID = 2 allora la DSRC-VU richiede una finestra privata*
3	REDCR	>	DSRC-VU	Alloca una finestra privata	Invia un frame contenente l'allocazione della finestra privata
4	*DSRC-VU*	>	*REDCR*	*Invia la VST*	*Invia un frame comprendente la VST*
5	REDCR	>	DSRC-VU	Invia GET.request per i dati nell'attributo per l'EID specifico	
6	*DSRC-VU*	>	*REDCR*	*Invia GET.response con l'attributo richiesto per l'EID specifico*	*Invia l'attributo (dati RTM, dati OWS...) con i dati per l'EID specifico*

▼B

Sequenza	Mittente		Destinatario	Descrizione	Azione
7	REDCR	>	DSRC-VU	Invia GET.request per i dati diversi dall'attributo (se del caso)	
8	*DSRC-VU*	>	*REDCR*	*Invia GET.response con l'attributo richiesto*	*Invia l'attributo con i dati per l'EID specifico*
9	REDCR	>	DSRC-VU	Conferma la ricezione corretta dei dati	Invia il comando RELEASE che chiude la transazione
10	*DSRC-VU*			*Chiude la transazione*	

Un esempio della sequenza e del contenuto della transazione dei frame scambiati è riportato ai paragrafi 5.4.7 e 5.4.8.

5.4.4 *Strutture dei dati*

DSC_37 La struttura semantica *dei dati* trasmessi tramite l'interfaccia DSRC 5,8 GHz deve essere coerente con quanto descritto nella presente appendice. Il modo in cui questi dati sono strutturati è specificato nella presente clausola.

DSC_38 Il payload (dati RTM) consiste nella concatenazione dei

1. dati EncryptedTachographPayload, che sono la cifratura del TachographPayload definito in ASN. 1 nel paragrafo 5.4.5. Il metodo di cifratura è descritto nell'appendice 11.

2. DSRCSecurityData, specificati nell'appendice 11.

DSC_39 I dati RTM sono considerati come RTM attributo = 1 e sono trasferiti nel contenitore RTM = 10.

DSC_40 Il segnale contestuale RTM deve identificare la parte supportata della norma nella serie di norme TARV (RTM corrisponde alla parte 9)

La definizione del modulo ASN.1 per i dati DSRC all'interno dell'applicazione RTM è la seguente:

▼B

```
TarvRtm {iso(1) standard(0) 15638 part9(9) version1(1)}
DEFINITIONS AUTOMATIC TAGS
::= BEGIN
IMPORTS
-- Imports data attributes and elements from EFC which are used for RTM
LPN
FROM EfcDsrcApplication {iso(1) standard(0) 14906 application(0) version5(5)}

-- Imports function parameters from the EFC Application Interface Definition
SetMMIRq
FROM EfcDsrcApplication {iso(1) standard(0) 14906 application(0) version5(5)}

-- Imports the L7 DSRCData module data from the EFC Application Interface Definition
Action-Request, Action-Response, ActionType, ApplicationList, AttributeIdList, AttributeList,
Attributes,
BeaconID, BST, Dsrc-EID, DSRCApplicationEntityID, Event-Report-Request, Event-Report- Response,
EventType, Get-Request, Get-Response, Initialisation-Request, Initialisation-Response,
ObeConfiguration, Profile, ReturnStatus, Time, T-APDUs, VST
FROM EfcDsrcGeneric {iso(1) standard(0) 14906 generic(1) version5(5)};


-- Definitions of the RTM functions:
RTM-InitialiseComm-Request ::= BST
RTM-InitialiseComm-Response::= VST
RTM-DataRetrieval-Request::= Get-Request (WITH COMPONENTS {fill (SIZE(1)), eid, accessCredentials ABSENT,iid
ABSENT,  attrIdList})
RTM-DataRetrieval-Response::= Get-Response {RtmContainer} (WITH COMPONENTS {..., eid, iid ABSENT})
RTM-TerminateComm::= Event-Report-Request {RtmContainer}(WITH COMPONENTS {mode (FALSE), eid (0),
eventType (0)})

RTM-TestComm-Request::= Action-Request {RtmContainer} (WITH COMPONENTS {..., eid (0), actionType
(15), accessCredentials ABSENT, iid ABSENT})

RTM-TestComm-Response::= Action-Response {RtmContainer} (WITH COMPONENTS {..., fill (SIZE(1)), eid
(0), iid ABSENT})

-- Definitions of the RTM attributes:
RtmData ::= SEQUENCE {
      encryptedTachographPayload OCTET STRING (SIZE(67)) (CONSTRAINED BY { -- calculated encrypting
TachographPayload as per Appendix 11 --}),
      DSRCSecurityData OCTET STRING
      }
TachographPayload ::= SEQUENCE {
            tp15638VehicleRegistrationPlate LPN -- Vehicle Registration Plate as per EN 15509.
            tp15638SpeedingEvent            BOOLEAN,  -- 1= Irregularities in speed (see Annex 1C)
            tp15638DrivingWithoutValidCard  BOOLEAN,     -- 1= Invalid card usage (see Annex 1C)
            tp15638DriverCard               BOOLEAN,-- 0= Indicates a valid driver card  (see Annex 1C)
            tp15638CardInsertion            BOOLEAN, -- 1= Card insertion while driving (see Annex 1C)
            tp15638MotionDataError          BOOLEAN, -- 1= Motion data error (see Annex 1C)
            tp15638VehicleMotionConflict    BOOLEAN, -- 1= Motion conflict (see Annex 1C)
            tp156382ndDriverCard            BOOLEAN, -- 1= Second driver card inserted (see Annex 1C)
            tp15638CurrentActivityDriving   BOOLEAN, -- 1= other activity selected;
                                                      -- 0= driving selected
            tp15638LastSessionClosed        BOOLEAN, -- 1= improperly, 0= properly, closed
            tp15638PowerSupplyInterruption  INTEGER (0..127), -- Supply interrupts in the last 10 days
            tp15638SensorFault              INTEGER (0..255),-- eventFaultType as per data dictionary
-- All subsequent time related types as defined in Annex 1C.
            tp15638TimeAdjustment           INTEGER(0..4294967295), -- Time of the last time adjustment
            tp15638LatestBreachAttempt      INTEGER(0..4294967295), -- Time of last breach attempt
            tp15638LastCalibrationData      INTEGER(0..4294967295), -- Time of last calibration data
            tp15638PrevCalibrationData      INTEGER(0..4294967295), -- Time of previous calibration data
            tp15638DateTachoConnected       INTEGER(0..4294967295), -- Date tachograph connected
            tp15638CurrentSpeed             INTEGER (0..255), -- Last current recorded speed
            tp15638Timestamp                INTEGER(0..4294967295) -- Timestamp of current record[2]
            }
Rtm-ContextMark ::= SEQUENCE {
 standardIdentifier    StandardIdentifier, -- identifier of the TARV part and its version

 RtmCommProfile          INTEGER {
                           C1 (1),
                           C2 (2)
                           } (0..255) DEFAULT 1
 }
RtmTransferAck ::= INTEGER {
                Ok (1),
                NoK (2)
                } SIZE (1..255)
```

▼B

```
StandardIdentifier ::= OBJECT IDENTIFIER
RtmContainer ::= CHOICE {
        integer                     [0]    INTEGER,
        bitstring                   [1]    BIT STRING,
        octetstring                 [2]    OCTET STRING (SIZE (0..127, ...)),
        universalString             [3]    UniversalString,
        beaconId                    [4]    BeaconID,
        t-apdu                      [5]    T-APDUs,
        dsrcApplicationEntityId     [6]    DSRCApplicationEntityID,
        dsrc-Ase-Id                 [7]    Dsrc-EID,
        attrIdList                  [8]    AttributeIdList,
        attrList                    [9]    AttributeList{RtmContainer},
        rtmData                     [10]   RtmData,
        rtmContextmark              [11]   Rtm-ContextMark,
        reserved12                  [12]   NULL,
        reserved13                  [13]   NULL,
        reserved14                  [14]   NULL,
        time                        [15]   Time,
-- values from 16 to 255 reserved for ISO/CEN usage
        }}

END
```

5.4.5 *Elementi di RtmData, azioni eseguite e definizioni*

DSC_41 I valori dei dati che la VU deve calcolare e usare per aggiornare i dati sicuri nella DSRC-VU devono essere calcolati secondo le regole definite nella tabella 14.3.

Tabella 14.3

Elementi di RtmData, azioni eseguite e definizioni

(1) Elemento di dati RTM	(2) Azione eseguita dalla VU		(3) Definizione di ASN.1 dei dati
RTM1 **Targa del veicolo**	La VU deve fissare il valore dell'elemento di dati RTM1 *tp15638VehicleRegistrationPlate* dal valore registrato del tipo di dati *VehicleRegistrationIdentification* come definito nell'appendice 1 *VehicleRegistrationIdentification*	Targa del veicolo espressa come stringa di caratteri	`tp15638VehicleRegstrationPlate_LPN, --Targa del veicolo importata da ISO 14906 con la limitazione di cui alla norma EN 15509, che è una SEQUENZA comprendente il codice paese seguito da un indicatore alfabetico seguito dal numero di targa, che è sempre di 14 ottetti (riempiti con zeri) di modo che la lunghezza del tipo LPN di EN 15509 sia sempre di 17 ottetti, di cui 14 sono il numero di targa "reale".`
RTM2 **Superamento di velocità**	La VU deve generare un valore booleano per l'elemento di dati RTM2 tp15638SpeedingEvent. Il valore tp15638SpeedingEvent deve essere calcolato dalla VU dal numero di superamenti di velocità registrati nella VU negli ultimi 10 giorni, come definito nell'allegato 1C.	1 (VERO) = Indica irregolarità per quanto concerne la velocità negli ultimi 10 giorni	`tp15638speedingEvent BOOLEAN,`

▼B

(1) Elemento di dati RTM	(2) Azione eseguita dalla VU		(3) Definizione di ASN.1 dei dati
	Se c'è almeno un tp15638SpeedingEvent negli ultimi 10 giorni, il valore tp15638SpeedingEvent deve essere impostato su VERO. Se non ci sono superamenti di velocità negli ultimi 10 giorni, tp15638SpeedingEvent deve essere impostato su FALSO.		
RTM3 **Guida in assenza di una carta valida**	La VU deve generare un valore booleano per l'elemento di dati RTM3 tp15638DrivingWithoutValidCard. La VU deve attribuire un valore di Vero alla variabile tp15638DrivingWithoutValidCard, se negli ultimi 10 giorni i dati della VU hanno registrato almeno un'anomalia del tipo «Guida in assenza di una carta valida», come definita nell'allegato 1C. SE INVECE non ci sono state anomalie di questo tipo negli ultimi 10 giorni, la variabile tp15638DrivingWithoutValidCard deve essere impostata su FALSO.	1 (VERO) = Indica l'uso di una carta non valida	`tp15638DrivingWithoutValidCard` `BOOLEAN,`
RTM4 **Carta del conducente valida**	La VU deve generare un valore booleano per l'elemento di dati RTM4 tp15638DriverCard sulla base dei dati memorizzati nella VU e definiti nell'appendice 1. Se non è presente nessuna carta del conducente valida, la VU deve impostare la variabile su VERO SE INVECE è presente una carta del conducente valida, la VU deve impostare la variabile su FALSO	0 (FALSO) = Indica una carta del conducente valida	`tp15638DriverCard` `BOOLEAN,`
RTM5 **Inserimento della carta durante la guida**	La VU deve generare un valore booleano per l'elemento di dati RTM5. La VU deve attribuire un valore di VERO alla variabile tp15638CardInsertion, se negli ultimi 10 giorni i dati della VU hanno registrato almeno un'anomalia del tipo «Inserimento della carta durante la guida», come definita nell'allegato 1C. SE INVECE non ci sono state anomalie di questo tipo negli ultimi 10 giorni, la variabile tp15638CardInsertion deve essere impostata su FALSO.	1 (VERO) = indica l'inserimento della carta durante la guida, negli ultimi 10 giorni	`tp15638CardInsertion` `BOOLEAN,`
RTM6 **Errore dati di movimento**	La VU deve generare un valore booleano per l'elemento di dati RTM6. La VU deve attribuire un valore di VERO alla variabile tp15638MotionDataError, se negli ultimi 10 giorni i dati della VU hanno registrato almeno un'anomalia del tipo «Errore dati di movimento», come definita nell'allegato 1C. SE INVECE non ci sono state anomalie di questo tipo negli ultimi 10 giorni, la variabile tp15638MotionDataError deve essere impostata su FALSO.	1 (VERO) = Indica un «errore dati di movimento» negli ultimi 10 giorni	`tp15638motionDataError` `BOOLEAN,`

▼B

(1) Elemento di dati RTM	(2) Azione eseguita dalla VU		(3) Definizione di ASN.1 dei dati
RTM7 **Dati contrastanti sul movimento del veicolo**	La VU deve generare un valore booleano per l'elemento di dati RTM7. La VU deve attribuire un valore di VERO alla variabile tp15638vehicleMotionConflict, se i dati della VU negli ultimi 10 giorni hanno registrato almeno un'anomalia del tipo Dati contrastanti sul movimento del veicolo (valore '0A'H). SE INVECE non ci sono state anomalie di questo tipo negli ultimi 10 giorni, la variabile tp15638vehicleMotionConflict deve essere impostata su FALSO.	1 (VERO) = Indica dati contrastanti sul movimento del veicolo negli ultimi 10 giorni	`tp15638vehicleMotionConflict` `BOOLEAN,`
RTM8 **Carta del secondo conducente**	La VU deve generare un valore booleano per l'elemento di dati RTM8 sulla base dell'allegato 1C («Dati relativi all'attività del conducente», EQUIPAGGIO e SECONDO CONDUCENTE). Se è presente una seconda carta del conducente valida, la VU deve impostare la variabile su VERO SE INVECE non è presente una seconda carta del conducente valida, la VU deve impostare la variabile su FALSO	1 (FALSO) = Indica una seconda carta del conducente inserita	`tp156382ndDriverCard` `BOOLEAN,`
RTM9 **Attività in corso**	La VU deve generare un valore booleano per l'elemento di dati RTM9. Se l'attività in corso è registrata nella VU come attività diversa da «GUIDA», come definita nell'allegato 1C, la VU deve impostare la variabile su VERO SE INVECE l'attività in corso è registrata nella VU come «GUIDA», la VU deve impostare la variabile su FALSO	1 (VERO) = altra attività selezionata; 0 (FALSO) = guida selezionata	`tp15638currentActivityDriving` `BOOLEAN`
RTM10 **Ultima sessione chiusa**	La VU deve generare un valore booleano per l'elemento di dati RTM10. Se l'ultima sessione della carta non si è chiusa correttamente, come definito nell'allegato 1C, la VU deve impostare la variabile su VERO. SE INVECE l'ultima sessione della carta si è chiusa correttamente, la VU deve impostare la variabile su FALSO.	1 (VERO) = chiusa non correttamente 0 (FALSO) = chiusa correttamente	`tp15638lastSessionClosed` `BOOLEAN`
RTM11 **Interruzione dell'alimentazione di energia**	La VU deve generare un valore intero per l'elemento di dati RTM11. La VU deve attribuire un valore alla variabile tp15638PowerSupplyInterruption pari all'interruzione dell'alimentazione di energia più lunga, a norma dell'articolo 9 del regolamento (UE) n. 165/2014, del tipo «Interruzione dell'alimentazione di energia», come definita nell'allegato 1C.	— Numero di interruzioni dell'alimentazione di energia negli ultimi 10 giorni	`tp15638powerSupplyInterruption` `INTEGER (0..127),`

▼B

(1) Elemento di dati RTM	(2) Azione eseguita dalla VU		(3) Definizione di ASN.1 dei dati
	SE INVECE negli ultimi 10 giorni non si sono verificate anomalie del tipo «interruzione dell'alimentazione di energia», il valore dell'intero deve essere impostato a 0.		
RTM12 **Guasto del sensore**	La VU deve generare un valore intero per l'elemento di dati RTM12. La VU deve assegnare alla variabile sensorFault un valore di: — 1 se un'anomalia di tipo '35'H «guasto del sensore» è stata registrata negli ultimi 10 giorni, — 2 se un'anomalia di tipo «guasto del ricevitore GNSS» (interno o esterno con i valori ENUM '51'H o '52'H) è stata registrata negli ultimi 10 giorni. — 3 se un'anomalia di tipo '53'H «guasto della comunicazione del GNSS esterno» è stata registrata negli ultimi 10 giorni. — 4 se sono stati registrati sia un guasto del sensore che guasti del ricevitore GNSS negli ultimi 10 giorni. — 5 se sono stati registrati sia un guasto del sensore che guasti della comunicazione del GNSS esterno negli ultimi 10 giorni. — 6 se sono stati registrati sia un guasto del ricevitore GNSS che un guasto della comunicazione del GNSS esterno negli ultimi 10 giorni. — 7 se sono stati registrati tutti e tre i guasti del sensore negli ultimi 10 giorni. Deve INVECE attribuire un valore di 0 se non sono state registrate anomalie negli ultimi 10 giorni.	— Guasto del sensore, un ottetto secondo il dizionario di dati	`tp15638SensorFault INTEGER (0..255),`
RTM13 **Regolazione dell'ora**	La VU deve generare un valore intero (timeReal dall'appendice 1) per l'elemento di dati RTM13 sulla base della presenza di dati relativi alla regolazione dell'ora, come definita nell'allegato 1C. La VU deve attribuire il valore temporale corrispondente al dato dell'ultima anomalia del tipo «regolazione dell'ora». SE INVECE nella VU non è presente nessuna anomalia del tipo «regolazione dell'ora», come definita nell'allegato 1C, la VU deve impostare un valore di 0	Ora dell'ultima regolazione dell'ora	`tp15638TimeAdjustment` `INTEGER(0..4294967295),`
RTM14 **Tentativo di violazione della sicurezza**	La VU deve generare un valore intero (timeReal dall'appendice 1) per l'elemento di dati RTM14 sulla base della presenza di un'anomalia del tipo «tentativo di violazione della sicurezza», come definita nell'allegato 1C. La VU deve impostare il valore temporale dell'ultima anomalia del tipo «tentativo di violazione della sicurezza» registrata dalla VU.	Ora dell'ultimo tentativo di violazione — Valore di default = 0x00FF	`tp15638LatestBreachAttempt` `INTEGER(0..4294967295),`

▼B

(1) Elemento di dati RTM	(2) Azione eseguita dalla VU		(3) Definizione di ASN.1 dei dati
	SE INVECE nella VU non è presente nessuna anomalia del tipo «tentativo di violazione della sicurezza», come definita nell'allegato 1C, la VU deve impostare un valore di 0x00FF.		
RTM15 **Ultima taratura**	La VU deve generare un valore intero (timeReal dall'appendice 1) per l'elemento di dati RTM15 sulla base della presenza di dati relativi all'ultima taratura, come definita nell'allegato 1C. La VU deve impostare il valore temporale delle ultime due tarature (RTM15 e RTM16), che sono impostate nei VuCalibrationData definiti nell'appendice 1. La VU deve impostare il valore di RTM15 al timeReal dell'ultima registrazione relativa alla taratura.	Ora dei dati dell'ultima taratura	`tp15638LastCalibrationData` `INTEGER(0..4294967295),`
RTM16 **Taratura precedente**	La VU deve generare un valore intero (timeReal dall'appendice 1) per l'elemento di dati RTM16 relativo alla registrazione della penultima taratura SE INVECE non vi c'è stata nessuna taratura precedente, la VU deve impostare il valore di RTM16 a 0.	Ora dei dati della taratura precedente	`tp15638PrevCalibrationData` `INTEGER(0..4294967295),`
RTM17 **Data del collegamento del tachigrafo**	Per l'elemento di dati RTM17, la VU deve generare un valore intero (timeReal dall'appendice 1). La VU deve impostare il valore dell'ora dell'installazione iniziale della VU. La VU deve estrarre questo dato da VuCalibrationData (appendice 1) da vuCalibrationRecords con CalibrationPurpose pari a: ‘03’H	Data del collegamento del tachigrafo	`tp15638DateTachoConnected` `INTEGER(0..4294967295),`
RTM18 **Velocità corrente**	La VU deve generare un valore intero per l'elemento di dati RTM18. La VU deve impostare il valore di RTM18 all'ultima velocità corrente registrata al momento dell'ultimo aggiornamento di RtmData.	Ultima velocità corrente registrata	`tp15638CurrentSpeed` `INTEGER (0..255),`
RTM19 **Marcatura oraria**	Per l'elemento di dati RTM19, la VU deve generare un valore intero (timeReal dall'appendice 1). La VU deve impostare il valore di RTM19 al momento dell'ultimo aggiornamento di RtmData.	Marcatura oraria (timestamp) della registrazione TachographPayload corrente	`tp15638Timestamp` `INTEGER(0..4294967295),`

5.4.6 *Meccanismo di trasferimento dei dati*

DSC_42 Il payload precedentemente definito è richiesto dal REDCR dopo la fase di inizializzazione ed è successivamente trasmesso dalla *DSRC-VU* nella finestra allocata. Il comando GET è usato dal REDCR per recuperare i dati.

▼B

DSC_43 Per tutti gli scambi DSRC, i dati devono essere codificati usando le PER (regole di codifica a pacchetto).

5.4.7 *Descrizione dettagliata della transazione DSRC*

DSC_44 L'inizializzazione avviene in conformità alle clausole da DSC_44 a DSC_48 e alle tabelle da 14.4 a 14.9. Nella fase di inizializzazione, il REDCR inizia ad inviare un frame contenente una BST (tabella di servizio del segnale) secondo le norme EN 12834 e EN 13372, paragrafi 6.2, 6.3, 6.4 e 7.1 con le impostazioni come specificato nella seguente tabella 14.4.

Tabella 14.4

Inizializzazione — Impostazioni del frame contenente una BST

Campo	Impostazioni
Link Identifier	Indirizzo di trasmissione
BeaconId	In conformità a EN 12834
Ora	In conformità a EN 12834
Profilo	Nessuna estensione, usare 0 o 1
MandApplications	Nessuna estensione, EID assente, parametro assente, AID = 2 Freight&Fleet
NonMandApplications	Assente
ProfileList	Nessuna estensione, numero di profili nell'elenco = 0
Fragmentation header	Nessuna frammentazione
Layer 2 settings	PDU del comando, comando UI

La tabella 14.5 a seguire riporta un esempio pratico delle impostazioni specificate nella tabella 14.4, con un'indicazione delle codifiche dei bit.

Tabella 14.5

Inizializzazione — Esempio dei contenuti del frame contenente una BST

Ottetto #	Attributo/Campo	Bit nell'ottetto	Descrizione
1	FLAG	0111 1110	Indicatore di inizio
2	Broadcast ID	1111 1111	Indirizzo di trasmissione
3	MAC Control Field	1010 0000	PDU del comando
4	LLC Control field	0000 0011	Comando UI

▼B

Ottetto #	Attributo/Campo	Bit nell'ottetto	Descrizione
5	Intestazione della frammentazione	1xxx x001	Nessuna frammentazione
6	BST	1000	Richiesta di inizializzazione
	SEQUENCE {		
	OPTION indicator BeaconID SEQUENCE { ManufacturerId INTEGER (0..65535)	0	Applicazioni NonMand assenti
		xxx	Identificativo del fabbricante
7		xxxx xxxx	
8		xxxx x	
	IndividualID INTEGER (0..134217727)	xxx	ID di 27 bit disponibile per il fabbricante
9		xxxx xxxx	
10		xxxx xxxx	
11	}	xxxx xxxx	
12	Time INTEGER (0..4294967295)	xxxx xxxx	Tempo reale UNIX 32 bit
13		xxxx xxxx	
14		xxxx xxxx	
15		xxxx xxxx	
16	Profile INTEGER (0..127,...)	0000 0000	Nessuna estensione. Profilo esemplificativo 0
17	MandApplications SEQUENCE (SIZE(0..127,…)) OF {	0000 0001	Nessuna estensione, numero di mandApplications = 1
18	SEQUENCE {		
	OPTION indicator	0	EID assente
	OPTION indicator	0	Parametro assente
	AID DSRCApplicationEntityID } }	00 0010	Nessuna estensione. AID= 2 Freight&Fleet

▼B

Ottetto #	Attributo/Campo	Bit nell'ottetto	Descrizione
19	ProfileList SEQUENCE (0..127,…) OF Profile }	0000 0000	Nessuna estensione, numero di profili nell'elenco = 0
20	FCS	xxxx xxxx	Sequenza di controllo del frame
21		xxxx xxxx	
22	Flag	0111 1110	Indicatore di fine

DSC_45 Quando una *DSRC-VU* riceve una BST, richiede l'allocazione di una finestra privata, come specificato nelle norme EN 12795 e EN 13372, paragrafo 7.1.1, senza impostazioni RTM specifiche. La tabella 14.6 riporta un esempio di codifica dei bit.

Tabella 14.6

Inizializzazione — Contenuto del frame di richiesta di allocazione di finestra privata

Ottetto #	Attributo/Campo	Bit nell'ottetto	Descrizione
1	FLAG	0111 1110	Indicatore di inizio
2	LID privato	xxxx xxxx	Indirizzo del collegamento della DSRC-VU specifica
3		xxxx xxxx	
4		xxxx xxxx	
5		xxxx xxxx	
6	MAC Control field	0110 0000	Richiesta di finestra privata
7	FCS	xxxx xxxx	Sequenza di controllo del frame
8		xxxx xxxx	
9	Flag	0111 1110	Indicatore di fine

DSC_46 Il REDCR allora risponde allocando una finestra privata, come specificato nelle norme EN 12795 e EN 13372, paragrafo 7.1.1, senza impostazioni RTM specifiche.

La tabella 14.7 riporta un esempio di codifica dei bit.

Tabella 14.7

Inizializzazione — Contenuto del frame di allocazione di finestra privata

Ottetto #	Attributo/Campo	Bit nell'ottetto	Descrizione
1	FLAG	0111 1110	Indicatore di inizio
2	LID privato	xxxx xxxx	Indirizzo del collegamento della DSRC-VU specifica
3		xxxx xxxx	

▼B

Ottetto #	Attributo/Campo	Bit nell'ottetto	Descrizione
4		xxxx xxxx	
5		xxxx xxxx	
6	MAC Control field	0010 s000	Allocazione della finestra privata
7	FCS	xxxx xxxx	Sequenza di controllo del frame
8		xxxx xxxx	
9	Flag	0111 1110	Indicatore di fine

DSC_47 Quando riceve l'allocazione della finestra privata, la *DSRC-VU* invia la sua VST (tabella di servizio del veicolo) come definita nelle norme EN 12834 e EN 13372, paragrafi 6.2, 6.3, 6.4 e 7.1, con le impostazioni specificate nella tabella 14.8, usando la finestra di trasmissione allocata.

Tabella 14.8

Inizializzazione — Impostazioni del frame della VST

Campo	Impostazioni
LID privato	In conformità a EN 12834
Parametri della VST	Riempimento=0, allora per ciascuna applicazione supportata: EID presente, parametro presente, AID=2, EID come generato dall'OBU
Parametro	Nessuna estensione, contiene il segnale contestuale RTM
ObeConfiguration	Il campo opzionale ObeStatus può essere presente, ma non deve essere usato dal REDCR
Intestazione della frammentazione	Nessuna frammentazione
Impostazioni del livello 2	PDU del comando, comando UI

DSC_48 La *DSRC-VU* deve supportare l'applicazione «carico e parco veicoli» identificata dall'identificativo dell'applicazione '2'. Possono essere supportati anche altri identificativi dell'applicazione, che però non devono essere presenti in questa VST, poiché la BST richiede solo AID=2. Il campo «applicazioni» contiene un elenco di istanze applicative supportate nella *DSRC-VU*. Per ciascuna istanziazione delle applicazioni supportate è dato un riferimento alla norma appropriata, costituito da un segnale contestuale RTM, che è composto da un IDENTIFICATIVO DELL'OGGETTO, che rappresenta la relativa norma, la parte (9 per RTM) e eventualmente la versione, più un EID generato dalla DSRC-VU e associato a tale istanza applicativa.

La tabella 14.9 riporta un esempio pratico delle impostazioni specificate nella tabella 14.8, con un'indicazione delle codifiche dei bit.

▼B

Tabella 14.9

Inizializzazione — Esempio di contenuti del frame della VST

Ottetto #	Attributo/Campo	Bit nell'ottetto	Descrizione
1	FLAG	0111 1110	Indicatore di inizio
2	LID privato	xxxx xxxx	Indirizzo del collegamento della DSRC-VU specifica
3		xxxx xxxx	
4		xxxx xxxx	
5		xxxx xxxx	
6	MAC Control field	1100 0000	PDU del comando
7	LLC Control field	0000 0011	Comando UI
8	Intestazione della frammentazione	1xxx x001	Nessuna frammentazione
9	VST SEQUENCE {	1001	Risposta di inizializzazione
	Fill BIT STRING (SIZE(4))	0000	Non usato e impostato a 0
10	Profile INTEGER (0..127,...) Applications SEQUENCE OF {	0000 0000	Nessuna estensione. Profilo esemplificativo 0
11		0000 0001	Nessuna estensione, 1 applicazione
12	SEQUENCE {		
	OPTION indicator	1	EID presente
	OPTION indicator	1	Parametro presente
	AID DSRCApplicationEntityID	00 0010	Nessuna estensione. AID= 2 Freight&Fleet
13	EID Dsrc-EID	xxxx xxxx	Definito nell'ambito dell'OBU e che identifica l'istanza applicativa
14	Parameter Container {	0000 0010	Nessuna estensione, scelta del contenitore = 02, stringa di ottetti
15		0000 1000	Nessuna estensione, lunghezza del segnale contestuale Rtm = 8

▼B

Ottetto #	Attributo/Campo	Bit nell'ottetto	Descrizione
16	Rtm-ContextMark::= SEQUENCE	0000 0110	Identificativo dell'oggetto della norma, della parte e della versione supportate. Esempio: ISO (1) Norma (0) TARV (15638) Parte 9(9) Versione 1 (1). Il primo ottetto è 06H, che è l'identificativo dell'oggetto; il secondo ottetto è 06H, che è la sua lunghezza. I 6 ottetti successivi codificano l'identificativo dell'oggetto preso come esempio Si noti che un solo elemento della sequenza è presente (l'elemento facoltativo RtmCommProfile è omesso)
17	{	0000 0110	
18	StandardIdentifier standardIdentifier	0010 1000	
19		1000 0000	
20		1111 1010	
21		0001 0110	
22		0000 1001	
23		0000 0001	
24	ObeConfiguration Sequence { OPTION indicator	0	ObeStatus assente
	EquipmentClass INTEGER (0..32767)	xxx xxxx	
25		xxxx xxxx	
26	ManufacturerId INTEGER (0..65535)	xxxx xxxx	Identificativo del fabbricante per la DSRC-VU, come descritto nella norma ISO 14816 — Registrarsi
27		xxxx xxxx	
28	FCS	xxxx xxxx	Sequenza di controllo del frame
29		xxxx xxxx	
30	Flag	0111 1110	Indicatore di fine

DCS_49 Il REDCR legge poi i dati inviando un comando GET conforme al comando GET definito nella norma EN 13372, paragrafi 6.2, 6.3, 6.4, e nella norma EN 12834 con le impostazioni specificate nella tabella 14.10.

Tabella 14.10

Presentazione — Impostazioni del frame di richiesta GET

Campo	Impostazioni
Invoker Identifier (IID)	Assente
Link Identifier (LID)	Indirizzo del collegamento della DSRC-VU specifica
Chaining	N.
Element Identifier (EID)	Come specificato nella VST. Nessuna estensione

▼B

Campo	Impostazioni
Access Credentials	N.
AttributeIdList	Nessuna estensione, 1 attributo, AttributeID = 1 (RtmData)
Frammentazione	N.
Layer2 settings	PDU del comando, comando ACn interrogato

La tabella 14.11 riporta un esempio di lettura dei dati RTM.

Tabella 14.11

Presentazione — Esempio di frame di richiesta GET

Ottetto #	Attributo/Campo	Bit nell'ottetto	Descrizione
1	FLAG	0111 1110	Indicatore di inizio
2	LID privato	xxxx xxxx	Indirizzo del collegamento della DSRC-VU specifica
3		xxxx xxxx	
4		xxxx xxxx	
5		xxxx xxxx	
6	MAC Control field	1010 s000	PDU del comando
7	LLC Control field	n111 0111	Comando ACn interrogato, n bit
8	Intestazione della frammentazione	1xxx x001	Nessuna frammentazione
9	Get.request SEQUENCE {	0110	Get request
	OPTION indicator	0	Credenziali di accesso assenti
	OPTION indicator	0	IID assente
	OPTION indicator	1	AttributeIdList presente
	Fill BIT STRING(SIZE(1))	0	Impostato a 0
10	EID INTEGER(0..127,…)	xxxx xxxx	L'EID dell'istanza applicativa RTM, come specificato nella VST. Nessuna estensione
11	AttributeIdList SEQUENCE OF { AttributeId }}	0000 0001	Nessuna estensione, numero di attributi = 1
12		0000 0001	AttributeId=1, RtmData. Nessuna estensione
13	FCS	xxxx xxxx	Sequenza di controllo del frame
14		xxxx xxxx	
15	Flag	0111 1110	Indicatore di fine

▼B

DSC_50 La *DSRC-VU*, quando riceve la richiesta GET, invia una riposta GET con i dati richiesti conforme alla risposta GET definita nella norma EN 13372, paragrafi 6.2, 6.3, 6.4, e nella norma EN 12834 con le impostazioni come specificato nella tabella 14.12.

Tabella 14.12

Presentazione — Impostazioni del frame di risposta GET

Campo	Impostazioni
Invoker Identifier (IID)	Assente
Link Identifier (LID)	In conformità a EN 12834
Chaining	N.
Element Identifier (EID)	Come specificato nella VST
Access Credentials	N.
Frammentazione	N.
Layer2 settings	Risposta PDU, risposta disponibile e comando accettato, comando ACn

La tabella 14.13 riporta un esempio di lettura dei dati RTM.

Tabella 14.13

Presentazione — Esempio di contenuti del frame di risposta

Ottetto #	Attributo/Campo	Bit nell'ottetto	Descrizione
1	FLAG	0111 1110	Indicatore di inizio
2	LID privato	xxxx xxxx	Indirizzo del collegamento della DSRC-VU specifica
3		xxxx xxxx	
4		xxxx xxxx	
5		xxxx xxxx	
6	MAC Control field	1101 0000	Risposta PDU
7	LLC Control field	n111 0111	Risposta disponibile, n bit del comando ACn
8	LLC Status field	0000 0000	Risposta disponibile e comando accettato
9	Intestazione della frammentazione	1xxx x001	Nessuna frammentazione
10	Get.response SEQUENCE {	0111	Ottieni la risposta

▼B

Ottetto #	Attributo/Campo	Bit nell'ottetto	Descrizione
	OPTION indicator	0	IID assente
	OPTION indicator	1	Elenco degli attributi presente
	OPTION indicator	0	Stato risposta inviata assente
	Fill BIT STRING(SIZE(1))	0	Non utilizzato
11	EID INTEGER(0..127,…)	xxxx xxxx	Risposta dall'istanza applicativa RTM. Nessuna estensione,
12	AttributeList SEQUENCE OF {	0000 0001	Nessuna estensione, numero di attributi = 1
13	Attributes SEQUENCE { AttributeId	0000 0001	Nessuna estensione, AttributeId = 1 (RtmData)
14	AttributeValue CONTAINER {	0000 1010	Nessuna estensione, scelta del contenitore = $10_{,10}$.
15		kkkk kkkk	RtmData
16		kkkk kkkk	
17		kkkk kkkk	
…		…	
n	}}}}	kkkk kkkk	
n+1	FCS	xxxx xxxx	Sequenza di controllo del frame
n+2		xxxx xxxx	
n+3	Flag	0111 1110	Indicatore di fine

DSC_51 Il REDCR chiude allora il collegamento inviando un comando EVENT_REPORT, RELEASE conforme alla norma EN 13372, paragrafi 6.2, 6.3, 6.4, e alla norma EN 12834, paragrafo 7.3.8, senza impostazioni RTM specifiche. La tabella 14.14 illustra un esempio di codifica dei bit del comando RELEASE.

Tabella 14.14

Chiusura. Contenuto del frame EVENT_REPORT Release

Ottetto #	Attributo/Campo	Bit nell'ottetto	Descrizione
1	FLAG	0111 1110	Indicatore di inizio
2	LID privato	xxxx xxxx	Indirizzo del collegamento della DSRC-VU specifica
3		xxxx xxxx	
4		xxxx xxxx	

▼B

Ottetto #	Attributo/Campo	Bit nell'ottetto	Descrizione
5		xxxx xxxx	
6	MAC Control field	1000 s000	Il frame contiene un comando LPDU
7	LLC Control field	0000 0011	Comando UI
8	Intestazione della frammentazione	1xxx x001	Nessuna frammentazione
9	EVENT_REPORT.request SEQUENCE {	0010	EVENT_REPORT (Release)
	OPTION indicator	0	Credenziali di accesso assenti
	OPTION indicator	0	Parametro dell'anomalia assente
	OPTION indicator	0	IID assente
	Mode BOOLEAN	0	Nessuna risposta attesa
10	EID INTEGER (0..127,…)	0000 0000	Nessuna estensione, EID = 0 (Sistema)
11	EventType INTEGER (0..127,…) }	0000 0000	Tipo di anomalia 0 = Release
12	FCS	xxxx xxxx	Sequenza di controllo del frame
13		xxxx xxxx	
14	Flag	0111 1110	Indicatore di fine

DSC_52 Non è attesa alcuna risposta da parte della *DSRC-VU* al comando Release. La comunicazione a questo punto si chiude.

5.4.8 *Descrizione della transazione di prova DSRC*

DSC_53 Prove complete, comprese verifiche delle procedure per garantire dati sicuri, devono essere condotte, come definito nell'appendice 11 (Meccanismi comuni di sicurezza), da persone autorizzate aventi accesso alle procedure di sicurezza, usando il comando normale GET, come definito sopra.

DSC_54 Le prove di attivazione e le prove di ispezione periodica che richiedono la decifrazione e la comprensione del contenuto dei dati decifrati devono essere condotte come specificato nell'appendice 11 (Meccanismi comuni di sicurezza) e nell'appendice 9 (Elenco di omologazione delle prove minime richieste).

La comunicazione DSRC di base può tuttavia essere testata tramite il comando ECHO. Tali prove possono essere richieste all'atto dell'attivazione, durante le ispezioni periodiche, dall'autorità di controllo competente o in conformità al regolamento (UE) n. 165/2014 (cfr. paragrafo 6 a seguire).

▼B

DSC_55 Per effettuare questa prova di comunicazione di base, il REDCR invia il comando ECHO durante una sessione, vale a dire dopo che una fase di inizializzazione è stata completata correttamente. La sequenza di interazione è dunque simile a quella di un'interrogazione:

— Fase 1 *Il REDCR* invia una «tabella di servizio del segnale» (BST), che include gli identificativi dell'applicazione (AID) nell'elenco dei servizi che supporta. Nelle applicazioni RTM, si tratterà semplicemente del servizio con il valore AID = 2.

La *DSRC-VU* valuta la BST ricevuta e laddove identifica che la BST sta chiedendo Freight&Fleet (AID = 2), la *DSRC-VU* deve rispondere. Se *il REDCR* non offre AID = 2, la *DSRC-VU* deve chiudere la transazione con *il REDCR*.

— Fase 2 *La DSRC-VU* invia una richiesta di allocazione di finestra privata.

— Fase 3 Il REDCR invia un'allocazione di finestra privata.

— Fase 4 La *DSRC-VU* usa la finestra privata allocata per inviare la sua tabella di servizio del veicolo (VST). Questa VST comprende un elenco di tutte le diverse istanziazioni delle applicazioni che questa *DSRC-VU* supporta nel quadro di AID = 2. Le diverse istanziazioni devono essere identificate per mezzo di EID generati univocamente, ciascuno associato ad un valore di parametro indicante l'istanza applicativa supportata.

— Fase 5 A questo punto *il REDCR* analizza la VST offerta e termina la connessione (RELEASE), perché non è interessato a nulla di ciò che la VST ha da offrire (vale a dire che sta ricevendo una VST da una *DSRC-VU* che non è una RTM VU) oppure, se riceve una VST appropriata, avvia un'istanziazione dell'applicazione.

— Fase 6 Il *REDCR* invia un comando (ECHO) alla *DSRC-VU* specifica e alloca una finestra privata.

— Fase 7 La *DSRC-VU* usa la finestra privata appena allocata per inviare un frame di risposta ECHO.

Le tabelle a seguire illustrano un esempio pratico di una sessione di scambio ECHO.

DSC_56 L'inizializzazione avviene in conformità al paragrafo 5.4.7 (da DSC_44 a DSC_48) e alle tabelle da 14.4 a 14.9.

DSC_57 Il REDCR a questo punto invia un comando ACTION, ECHO conforme alla norma ISO 14906 contenente 100 ottetti di dati e senza impostazioni specifiche per l'RTM. La tabella 14.15 illustra il contenuto del frame inviato dal REDCR.

▼B

Tabella 14.15

Esempio di frame di richiesta ACTION, ECHO

Ottetto #	Attributo/Campo	Bit nell'ottetto	Descrizione
1	FLAG	0111 1110	Indicatore di inizio
2	LID privato	xxxx xxxx	Indirizzo del collegamento della DSRC-VU specifica
3		xxxx xxxx	
4		xxxx xxxx	
5		xxxx xxxx	
6	MAC Control field	1010 s000	PDU del comando
7	LLC Control field	n111 0111	Comando ACn interrogato, n bit
8	Intestazione della frammentazione	1xxx x001	Nessuna frammentazione
9	ACTION.request SEQUENCE {	0000	Richiesta di azione (ECHO)
	OPTION indicator	0	Credenziali di accesso assenti
	OPTION indicator	1	Parametro dell'azione presente
	OPTION indicator	0	IID assente
	Mode BOOLEAN	1	Risposta attesa
10	EID INTEGER (0..127,…)	0000 0000	Nessuna estensione, EID = 0 (Sistema)
11	ActionType INTEGER (0..127,…)	0000 1111	Nessuna estensione, richiesta di azione di tipo ECHO
12	ActionParameter CONTAINER {	0000 0010	Nessuna estensione, scelta del contenitore = 2
13		0110 0100	Nessuna estensione. Lunghezza della stringa = 100 ottetti
14		xxxx xxxx	Dati da ripetere
…		…	
113	}}	xxxx xxxx	
114614	FCS	xxxx xxxx	Sequenza di controllo del frame
115715		xxxx xxxx	
116816	Flag	0111 1110	Indicatore di fine

▼B

DSC_58 Quando la *DSRC-VU* riceve la richiesta di ECHO, invia una risposta ECHO di 100 ottetti di dati riflettendo il comando ricevuto, in conformità alla norma ISO 14906, senza impostazioni specifiche per l'RTM. La tabella 14.16 illustra un esempio di codifica del livello di bit.

Tabella 14.16

Esempio di frame di risposta ACTION, ECHO

Ottetto #	Attributo/Campo	Bit nell'ottetto	Descrizione
1	FLAG	0111 1110	Indicatore di inizio
2	LID privato	xxxx xxxx	Indirizzo del collegamento della VU specifica
3		xxxx xxxx	
4		xxxx xxxx	
5		xxxx xxxx	
6	MAC Control field	1101 0000	Risposta PDU
7	LLC Control field	n111 0111	n bit del comando ACn
8	LLC status field	0000 0000	Risposta disponibile
9	Intestazione della frammentazione	1xxx x001	Nessuna frammentazione
10	ACTION.response SEQUENCE {	0001	ACTION.response (ECHO)
	OPTION indicator	0	IID assente
	OPTION indicator	1	Parametro di risposta presente
	OPTION indicator	0	Stato risposta inviata assente
	Fill BIT STRING (SIZE (1))	0	Non utilizzato
11	EID INTEGER (0..127,…)	0000 0000	Nessuna estensione, EID = 0 (Sistema)
12	ResponseParameter CONTAINER {	0000 0010	Nessuna estensione, scelta del contenitore = 2
13		0110 0100	Nessuna estensione. Lunghezza della stringa = 100 ottetti
14		xxxx xxxx	Dati ripetuti
…		…	
113	}}	xxxx xxxx	
114	FCS	xxxx xxxx	Sequenza di controllo del frame
115		xxxx xxxx	
116	Flag	0111 1110	Indicatore di fine

▼B

5.5 **Conformità alla direttiva 2015/71/UE**

5.5.1 *Panoramica*

DSC_59 Per supportare la direttiva 2015/719/UE sulle dimensioni massime e i pesi massimi dei veicoli commerciali pesanti, il protocollo della transazione per scaricare i dati OWS tramite il collegamento dell'interfaccia DSRC 5,8 GHz sarà lo stesso usato per i dati RTM (cfr. il paragrafo 5.4.1), con l'unica differenza che l'identificativo dell'oggetto relativo alla norma TARV riguarderà la norma ISO 15638 (TARV) parte 20 concernente i WOB/OWS.

5.5.2 *Comandi*

DSC_ 60 I comandi usati per una transazione OWS saranno gli stessi usati per una transazione RTM.

5.5.3 *Sequenza di comandi di interrogazione*

DSC_ 61 La sequenza di comandi di interrogazione per i dati OWS sarà la stessa dei dati RTM.

5.5.4 *Strutture dei dati*

DSC_62 Il payload (dati OWS) consiste nella concatenazione dei

1. dati EncryptedOwsPayload, che sono la cifratura dell'OwsPayload definito in ASN. 1 nel paragrafo 5.5.5. Il metodo di cifratura deve essere lo stesso adottato per RtmData, specificato all'appendice 11.

2. DSRCSecurityData, calcolati con gli stessi algoritmi adottati per RtmData, specificati all'appendice 11.

▼B

5.5.5 *Modulo ASN. 1 per la transazione OWS DSRC*

DSC_63. La definizione del modulo ASN.1 per i dati DSRC all'interno dell'applicazione RTM è la seguente:

```
TarvOws {iso(1) standard(0) 15638 part20(20)
version1(1)} DEFINITIONS AUTOMATIC TAGS
::= BEGIN
IMPORTS
-- Imports data attributes and elements from EFC which are used for OWS
LPN
FROM EfcDsrcApplication {iso(1) standard(0) 14906 application(0) version5(5)}

-- Imports function parameters from the EFC Application Interface Definition
SetMMIRq
FROM EfcDsrcApplication {iso(1) standard(0) 14906 application(0) version5(5)}

-- Imports the L7 DSRCData module data from the EFC Application Interface Definition
Action-Request, Action-Response, ActionType, ApplicationList, AttributeIdList, AttributeList,
Attributes,
BeaconID, BST, Dsrc-EID, DSRCApplicationEntityID, Event-Report-Request, Event-Report- Response,
EventType, Get-Request, Get-Response, Initialisation-Request, Initialisation-Response,
ObeConfiguration, Profile, ReturnStatus, Time, T-APDUs, VST
FROM EfcDsrcGeneric {iso(1) standard(0) 14906 generic(1) version5(5)};

-- Definitions of the OWS functions:
OWS-InitialiseComm-Request ::= BST
OWS-InitialiseComm-Response::= VST
OWS-DataRetrieval-Request::= Get-Request (WITH COMPONENTS {fill (SIZE(1)), eid, accessCredentials
ABSENT, iid ABSENT, attrIdList})
OWS-DataRetrieval-Response::= Get-Response {OwsContainer} (WITH COMPONENTS {..., eid, iid ABSENT})
OWS-TerminateComm::= Event-Report-Request {OwsContainer}(WITH COMPONENTS {mode (FALSE), eid (0),
eventType (0)})
OWS-TestComm-Request::= Action-Request {OwsContainer} (WITH COMPONENTS {..., eid (0), actionType
(15), accessCredentials ABSENT, iid ABSENT})
OWS-TestComm-Response::= Action-Response {OwsContainer} (WITH COMPONENTS {..., fill (SIZE(1)), eid
(0), iid ABSENT})

-- Definitions of the OWS attributes:
OwsData :: = SEQUENCE {
     encryptedOwsPayload OCTET STRING (SIZE(51)) (CONSTRAINED BY { -- calculated encrypting
OwsPayload as per Appendix 11 --}),
     DSRCSecurityData OCTET STRING
     }
OwsPayload :: = SEQUENCE {
           tp15638VehicleRegistrationPlate LPN -- Vehicle Registration Plate as per EN 15509.
           recordedWeight INTEGER (0..65535),           -- 0= Total measured weight of the  heavy
goods vehicle                                                          -- with 10 Kg
resolution.
           axlesConfiguration OCTET STRING SIZE (3),     -- 0= 20 bits allowed for the number
                                                                  -- of axles for 10 axles.
           axlesRecordedWeight OCTET STRING SIZE (20),   -- 0= Recorded Weight for each axle
                                                                  -- with 10 Kg resolution.
           tp15638Timestamp              INTEGER(0..4294967295)      -- Timestamp of current record
     }

Ows-ContextMark ::= SEQUENCE {
 standardIdentifier    StandardIdentifier, -- identifier of the TARV part and its version
     }

StandardIdentifier ::= OBJECT IDENTIFIER
 OwsContainer ::= CHOICE {
     integer                    [0]    INTEGER,
     bitstring                  [1]    BIT STRING,
     octetstring                [2]    OCTET STRING (SIZE (0..127, ...)),
     universalString            [3]    UniversalString,
     beaconId                   [4]    BeaconID,
     t-apdu                     [5]    T-APDUs,
     dsrcApplicationEntityId    [6]    DSRCApplicationEntityID,
     dsrc-Ase-Id                [7]    Dsrc-EID,
     attrIdList                 [8]    AttributeIdList,
     attrList                   [9]    AttributeList{RtmContainer},
     reserved10                 [10]   NULL,
     OwsContextmark             [11]   Ows-ContextMark,
     OwsData                    [12]   OwsData,
     reserved13                 [13]   NULL,
     reserved14                 [14]   NULL,
     time                       [15]   Time,
-- values from 16 to 255 reserved for ISO/CEN usage
     }}

END
```

▼B

5.5.6 *Elementi di OwsData, azioni eseguite e definizioni*

Gli elementi di OwsData sono definiti per supportare la direttiva 2015/719/UE sui pesi massimi e le dimensioni massime dei veicoli commerciali pesanti. Il loro significato è:

— recordedWeight rappresenta il peso totale misurato del veicolo commerciale pesante con una risoluzione di 10 kg, come definito nella norma EN ISO 14906. Ad esempio un valore di 2500 rappresenta un peso di 25 tonnellate.

— axlesConfiguration rappresenta la configurazione del veicolo commerciale pesante come numero di assi. La configurazione è definita con la maschera di bit di 20 bit (estesa dalla norma EN ISO 14906).

Una maschera di bit di 2 bit rappresenta la configurazione di un asse con il formato seguente:

— il valore 00B significa che il valore non è disponibile in quanto il veicolo non è dotato di dispositivi per misurare il peso sull'asse.

— Il valore 01B significa che l'asse non è presente.

— Il valore 10B significa che l'asse è presente e il peso è stato calcolato e misurato ed è riportato nel campo axlesRecorded-Weight.

— Il valore 11B è riservato per usi futuri.

Gli ultimi 4 bit sono riservati per usi futuri.

Numero di assi										
Numero di assi sulla motrice			Numero di assi sul rimorchio							
00/01/ 10/11	00/01/ 10/11	00/01/ 10/11	00/01/ 10/11	00/01/ 10/11	00/01/ 10/11	00/01/ 10/11	00/01/ 10/11	00/01/ 10/11	00/01/ 10/11	RFU (4 bit)

— axlesRecordedWeight rappresenta il peso specifico misurato per ciascun asse con una risoluzione di 10 kg. Si usano due ottetti per ciascun asse. Ad esempio un valore di 150 rappresenta un peso di 1 500 kg.

Gli altri tipi di dati sono definiti al paragrafo 5.4.5.

5.5.7 *Meccanismi di trasferimento dei dati*

DSC_64 Il meccanismo di trasferimento dei dati per i dati OWS tra l'interrogatore e il dispositivo DSRC nel veicolo deve essere lo stesso dei dati RTM (cfr. paragrafo 5.4.6).

DSC_ 65 Il trasferimento dei dati tra la piattaforma di raccolta dei dati sui pesi massimi e il dispositivo DSRC nel veicolo si deve basare sul collegamento fisico e sulle interfacce e sul protocollo definiti al paragrafo 5.6.

5.6 **Trasferimento di dati tra la DSRC-VU e la VU**

5.6.1 *Collegamento fisico e interfacce*

DSC_66 Il collegamento tra la *VU* e la *DSRC-VU* può essere un cavo fisico o una comunicazione senza fili a corto raggio basata su Bluetooth v4.0 BLE.

▼B

DSC_67 Indipendentemente dalla scelta del collegamento fisico e dell'interfaccia, i seguenti requisiti devono essere soddisfatti:

DSC_68 a) al fine di potersi rivolgere a fornitori diversi per la fornitura della VU, della DSRC-VU e di diversi lotti di DSRC-VU, il collegamento tra la VU e la DSRC-VU deve essere un collegamento standard aperto. La VU deve collegarsi alla DSRC-VU:

i) tramite un cavo fisso di almeno 2 metri, utilizzando un connettore Straight DIN 41612 H11; un connettore maschio approvato a 11 pin dalla DSRC-VU e un connettore femmina corrispondente simile, conforme alla norma DIN/ISO, dalla VU,

ii) tramite Bluetooth a bassa energia (BLE),

iii) tramite un collegamento conforme alla norma ISO 11898 o SAE J1939;

DSC_69 b) la definizione delle interfacce e del collegamento tra la VU e la DSRC-VU deve supportare i comandi del protocollo dell'applicazione definiti al paragrafo 5.6.2 e

DSC_70 c) la VU e la DSRC-VU devono supportare l'operazione di trasferimento di dati tramite il collegamento in termini di prestazioni e di alimentazione di energia.

5.6.2 *Protocollo dell'applicazione*

DSC_71 Il protocollo dell'applicazione tra il dispositivo di comunicazione remota della VU e la DSRC-VU è responsabile del trasferimento periodico dei dati della comunicazione remota dalla VU alla DSRC.

DSC_72 Si identificano i seguenti comandi principali:

1. Inizializzazione del collegamento di comunicazione -richiesta

2. Inizializzazione del collegamento di comunicazione -risposta

3. Invio dei dati con identificativo dell'applicazione RTM e payload definiti dai dati RTM

4. Riconoscimento dei dati

5. Fine del collegamento di comunicazione -richiesta

6. Fine del collegamento di comunicazione -risposta

DSC_73 In ASN1.0, i comandi precedenti possono essere definiti come:

▼B

```
Remote Communication DT Protocol DEFINITIONS ::= BEGIN

     RCDT-Communication Link Initialization - Request ::= SEQUENCE {
          LinkIdentifier INTEGER
     }

     RCDT-Communication Link Initialization - Response::= SEQUENCE {
          LinkIdentifier INTEGER,
          answer         BOOLEAN
     }

          RCDT- Send Data ::=
          SEQUENCE { LinkIdentifier
          INTEGER, DataTransactionId
          INTEGER, RCDTData
          SignedTachographPayload
     }

          RCDT Data Acknowledgment ::
          SEQUENCE { LinkIdentifier
          INTEGER, DataTransactionId
          INTEGER,
          answer         BOOLEAN
     }

          RCDT-Communication Link Termination - Request ::= SEQUENCE {
          LinkIdentifier INTEGER
     }

          RCDT-Communication Link Termination - Response::= SEQUENCE {
          LinkIdentifier INTEGER,
          answer         BOOLEAN
     }

End
```

DSC_74 La descrizione dei comandi e dei parametri è la seguente:

— `RCDT-Communication Link Initialization – Request` si usa per inizializzare il collegamento di comunicazione. Il comando è inviato dalla VU alla DSRC-VU. Il LinkIdentifier è impostato dalla VU e comunicato alla DSRC-VU per tracciare un collegamento di comunicazione specifico.

(*Nota:* serve a supportare collegamenti futuri e altre applicazioni/altri moduli come la pesatura a bordo).

— `RCDT-Communication Link Initialization – Response` è usato dalla DSRC-VU per rispondere alla richiesta di inizializzazione del collegamento di comunicazione. Il comando è inviato dalla DSRC-VU alla VU. Il comando dà il risultato dell'inizializzazione come risposta = 1 (avvenuta) o = 0 (fallita).

DSC_75 L'inizializzazione del collegamento di comunicazione deve essere fatta solo dopo l'installazione, la taratura e l'avvio del motore/l'accensione della VU.

▼B

— RCDT-Send Data è usato dalla VU per inviare i dati firmati RCDTData (= *i dati della comunicazione remota*) alla DSRC-VU. I dati saranno inviati ogni 60 secondi. Il parametro DataTransactionId identifica la trasmissione di dati specifica. Il LinkIdentifier si usa anche per garantire che il collegamento appropriato sia corretto.

— RCDT-Data Acknowledgment è inviato dalla DSRC-VU per informare la VU della ricezione dei dati da un comando RCDT-Send Data identificato dal parametro DataTransactionId. Il parametro di risposta è 1 (avvenuta) o = 0 (fallita). Se la VU riceve più di tre risposte uguali a 0 o se la VU non riceve un RCDT-Data Acknowledgment per un RCDT- Send Data specifico precedentemente inviato con un DataTransactionId specifico, la Vu genererà e registrerà un'anomalia.

— RCDT-Communication Link Termination request è inviato dalla VU alla DSRC-VU per chiudere un collegamento per un LinkIdentifier specifico.

DSC_76 Al riavvio della DSRC-VU o di una VU, tutti i collegamenti di comunicazione esistenti dovrebbero essere rimossi, poiché potrebbero esserci collegamenti «pendenti» dovuti all'arresto improvviso di una VU.

— RCDT-Communication Link Termination - Response è inviato dalla DSRC-VU alla VU per confermare la richiesta della VU di chiusura del collegamento per il LinkIdentifier specifico.

5.7 **Trattamento degli errori**

5.7.1 *Registrazione e comunicazione dei dati nella DSRC-VU*

DSC_77 *I dati* devono essere forniti, già sicuri, dalla funzione *VUSM* alla *DSRC-VU*. La *VUSM* deve verificare che i dati registrati nella *DSRC-VU* siano stati registrati correttamente. La registrazione e la comunicazione degli eventuali errori nel trasferimento dei dati dalla *VU* alla memoria della *DSRC-VU* devono essere registrate insieme al timestamp come EventFaultType e con il valore ENUM impostato a '62'H (errore di comunicazione del dispositivo di comunicazione remota).

DSC_78 La *VU* deve conservare un file, identificato con un nome unico e facilmente identificabile dagli ispettori, al fine di registrare «le mancate comunicazioni interne alla VU».

DSC_79 Se la VUPM cerca di ottenere dati della VU dal modulo di sicurezza (da passare alla DSRC-VU), ma senza successo, deve registrare tale tentativo fallito insieme al timestamp come EventFaultType e con il valore ENUM impostato a *'62'H Errore di comunicazione del dispositivo di comunicazione remota*. La

▼B

mancata comunicazione è rilevata quando un messaggio `RCDT Data Acknowledgment` non è ricevuto per i relativi `RCDT Send Data` (vale a dire con lo stesso DataTransactionId nei messaggi `Send Data and Acknowledgment`) per oltre tre volte consecutive.

5.7.2 *Errori di comunicazione senza fili*

DSC_80 La gestione degli errori di comunicazione deve essere conforme alle relative norme DSRC, nello specifico EN 300 674-1, EN 12253, EN 12795, EN 12834, e ai parametri appropriati di EN 13372.

5.7.2.1 *Errori di cifratura e di firma*

DSC_81 Gli errori di cifratura e di firma devono essere gestiti come definito nell'appendice 11 (Meccanismi comuni di sicurezza) e non sono presenti in nessun messaggio di errore associato al trasferimento DSRC di dati.

5.7.2.2 *Registrazione degli errori*

Il mezzo DSRC è una comunicazione senza fili dinamica in un ambiente con condizioni atmosferiche e di interferenza incerte, in particolare nelle combinazioni «REDCR portatile» e «veicolo in movimento» usate in questa applicazione. Di conseguenza è necessario accertare la differenza tra un «mancata lettura» e una condizione di «errore». In una transazione tramite un'interfaccia senza fili, le mancate letture sono comuni e la conseguenza consiste generalmente nel riprovare, vale a dire nel ritrasmettere la BST e nel riprovare la sequenza, il che nella maggior parte dei casi porta a un collegamento di comunicazione con esito positivo e al trasferimento dei dati, a meno che il veicolo bersaglio non esca dal raggio del dispositivo nel periodo necessario per la ritrasmissione. (Una «lettura» con «esito positivo» può aver comportato diversi tentativi ripetuti).

Una mancata lettura può essere causata dall'abbinamento non corretto delle antenne (errore di «puntamento»); dal fatto che una delle antenne è schermata, deliberatamente o a causa della presenza fisica di un altro veicolo; da interferenze radio, causate in particolare da WIFI a circa 5,8 GHz o da altre comunicazioni senza fili di accesso pubblico, da interferenze radar o da condizioni atmosferiche difficili (ad esempio durante un temporale); o semplicemente dal fatto di uscire dal raggio di comunicazione della DSRC. I singoli casi di mancata lettura non possono essere registrati, per la loro stessa natura, semplicemente perché la comunicazione non è avvenuta.

Se tuttavia l'agente dell'autorità di controllo competente punta un veicolo e cerca di interrogare la sua *DSRC-VU*, ma non avviene nessun trasferimento di dati, questo tentativo fallito potrebbe essere causato da una manomissione deliberata e dunque l'agente dell'autorità di controllo competente deve poterlo registrare ed avvisare i colleghi a valle della possibile violazione. I colleghi possono quindi fermare il veicolo e ispezionarlo fisicamente. Tuttavia, siccome non è avvenuta nessuna comunicazione con esito positivo, la DSRC-VU non può fornire dati riguardanti il tentativo fallito. Questa comunicazione deve dunque essere una funzione di progettazione dell'apparecchiatura REDCR.

«Mancata lettura» è diverso da «errore» da un punto di vista tecnico. In questo contesto un «errore» è l'acquisizione di un valore errato.

▼B

I dati trasferiti alla *DSRC-VU* sono forniti già sicuri e devono quindi essere verificati dal fornitore degli stessi (cfr. paragrafo 5.4).

I dati successivamente trasferiti tramite l'interfaccia aerea sono controllati tramite controlli di ridondanza ciclica al livello delle comunicazioni. Se il CRC convalida, allora i dati sono corretti. Se il CRC non convalida, i dati sono ritrasmessi. La probabilità che dati potrebbero superare erroneamente un CRC è talmente remota statisticamente da poter essere scartata.

Se il CRC non convalida e non c'è tempo di ritrasmettere e ricevere i dati corretti, il risultato non sarà un errore, ma un'istanziazione di un tipo specifico di mancata lettura.

L'unico dato significativo riguardante i tentativi falliti che può essere registrato è il numero di inizializzazioni corrette di transazioni che non portano ad un trasferimento corretto di dati al REDCR.

DSC_82 Il *REDCR* deve dunque registrare con timestamp il numero di casi in cui la fase di «inizializzazione» di un'interrogazione DSRC va a buon fine, ma la transazione termina prima che *i dati* siano recuperati con successo dal REDCR. Questo dato deve essere messo a disposizione dell'agente dell'autorità di controllo competente e deve essere salvato nella memoria dell'attrezzatura REDCR. Il mezzo per raggiungere tale obiettivo è una questione di progettazione del prodotto o deve essere oggetto di specifiche di un'autorità di controllo competente.

L'unico dato significativo riguardante gli «errori» che può essere registrato è il numero di casi in cui il REDCR non riesce a decriptare *i dati* ricevuti. Va tuttavia sottolineato che ciò sarà riferito esclusivamente all'efficienza del software del REDCR. I dati possono essere decriptati dal punto di vista tecnico, ma dal punto di vista semantico non hanno senso.

DSC_83 Il *REDCR* deve dunque registrare con timestamp il numero di casi in cui ha cercato, senza successo, di decriptare dati ricevuti tramite l'interfaccia DSRC.

6 PROVE DI ATTIVAZIONE E DI ISPEZIONE PERIODICA PER LA FUNZIONE DI COMUNICAZIONE REMOTA

6.1 **Aspetti generali**

DSC_84 Per la funzione di comunicazione remota sono previsti due tipi di prove:

1) Una prova ECHO per convalidare il canale di comunicazione *senza fili DSRC-REDCR>>-:-<DSRC-VU*.

2) Una prova di sicurezza end-to-end per garantire che una carta dell'officina sia in grado di avere accesso al contenuto dei dati criptati e firmati creato dalla VU e trasmesso tramite il canale di comunicazione senza fili.

6.2 **ECHO**

Questa clausola contiene disposizioni elaborate specificamente per testare solo il fatto che il collegamento *DSRC-REDCR >>-:-<DSRC-VU* sia funzionalmente attivo.

▼B

L'obiettivo del comando ECHO è di permettere alle officine o ai laboratori di prova per il rilascio delle omologazioni di verificare che il collegamento DSRC funzioni senza bisogno di accedere alle credenziali di sicurezza. Le attrezzature di chi esegue le prove dunque devono essere in grado solamente di inizializzare una comunicazione DSRC (inviando una BST con AID=2) e poi di inviare il comando ECHO e, supponendo che il DSRC funzioni, riceveranno una risposta ECHO. Per informazioni dettagliate si rimanda al paragrafo 5.4.8. Supponendo che riceva correttamente questa risposta, il collegamento DSRC (*DSRC-REDCR >>-:-<DSRC-VU*) può essere convalidato come funzionante correttamente.

6.3 **Prove per convalidare il contenuto dei dati sicuri**

DSC_85 Questa prova è eseguita per convalidare la sicurezza del flusso di dati da un estremo all'altro (end-to-end). Per eseguire la prova è necessario un lettore di prova DSRC. Il lettore di prova DSRC ha la stessa funzionalità ed è usato secondo le stesse specifiche del lettore utilizzato dalle forze dell'ordine, con la differenza che per autenticare l'utente del lettore di prova DSRC si deve usare una carta dell'officina anziché una carta di controllo. La prova può essere eseguita dopo l'attivazione iniziale di un tachigrafo intelligente o al termine della procedura di taratura. Dopo l'attivazione, l'unità elettronica di bordo deve generare e comunicare alla DSRC-VU i dati sicuri di diagnosi precoce.

DSC_86 Il personale dell'officina deve posizionare il lettore di prova DSRC a una distanza tra i 2 e i 10 metri davanti al veicolo.

DSC_87 Poi il personale dell'officina deve inserire una carta dell'officina nel lettore di prova DSRC per chiedere l'interrogazione dei dati di diagnosi precoce all'unità elettronica di bordo. Dopo un'interrogazione con esito positivo, il personale dell'officina deve avere accesso ai dati ricevuti per garantire che la loro integrità sia stata correttamente convalidata e che siano stati correttamente decriptati.

▼B

Appendice 15

MIGRAZIONE: GESTIONE DELLA COESISTENZA DI DIVERSE GENERAZIONI DI APPARECCHIATURE

INDICE

1. DEFINIZIONI

2. DISPOSIZIONI GENERALI

2.1. Transizione

2.2. Interoperabilità tra la VU e le carte

2.3. Interoperabilità tra VU e MS

2.4. Interoperabilità tra unità elettroniche di bordo, carte tachigrafiche e apparecchi per il trasferimento di dati

2.4.1 Trasferimento diretto dalla carta mediante IDE

2.4.2 Trasferimento di dati dalla carta mediante un'unità elettronica di bordo

2.4.3 Trasferimento dall'unità elettronica di bordo

2.5. Interoperabilità tra VU e apparecchiatura di taratura

3. FASI PRINCIPALI PRIMA DELL'INTRODUZIONE

4. DISPOSIZIONI PER IL PERIODO SUCCESSIVO ALL'INTRODUZIONE

1. DEFINIZIONI

Ai fini della presente appendice si applicano le seguenti definizioni:

sistema tachigrafico intelligente*:* come definito dal presente allegato (capitolo 1: definizione bbb);

tachigrafo di prima generazione*:* come definito dal presente regolamento (articolo 2: definizione 1);

tachigrafo di seconda generazione*:* come definito dal presente regolamento (articolo 2: definizione 7);

data di introduzione*:* come definito dal presente allegato (capitolo 1: definizione ccc);

Apparecchio intelligente dedicato [IDE (Intelligent dedicated equipment)]*:* apparecchio utilizzato per il trasferimento di dati, conformemente alla definizione di cui all'appendice 7 del presente allegato.

2. DISPOSIZIONI GENERALI

2.1. **Transizione**

Il preambolo del presente allegato fornisce un prospetto della transizione dal sistema tachigrafico di prima generazione a quello di seconda generazione.

Oltre alle disposizioni del presente preambolo:

— i sensori di movimento di prima generazione non saranno interoperabili con le unità elettroniche di bordo di seconda generazione;

— l'installazione nei veicoli dei sensori di movimento di seconda generazioni inizierà contemporaneamente all'installazione delle unità elettroniche di bordo di seconda generazione;

▼B

— i dispositivi per il trasferimento dei dati e per la taratura dovranno evolvere in modo da poter supportare l'utilizzo di apparecchi di controllo e di carte tachigrafiche di prima e seconda generazione.

2.2. **Interoperabilità tra la VU e le carte**

È sottinteso che le carte tachigrafiche di prima generazione sono interoperabili con le unità elettroniche di bordo di prima generazione (conformemente all'allegato 1B del presente regolamento), mentre le carte tachigrafiche di seconda generazione sono interoperabili con le unità elettroniche di bordo di seconda generazione (conformemente all'allegato 1C del presente regolamento). Inoltre si applicano i seguenti requisiti.

MIG_001 Ad eccezione dei requisiti MIG_004 e MIG_005, le carte tachigrafiche di prima generazione possono continuare ad essere utilizzate nelle unità elettroniche di bordo di seconda generazione fino alla scadenza della loro validità. I detentori possono tuttavia chiedere la sostituzione di tali carte con carte tachigrafiche di seconda generazione non appena queste ultime sono disponibili.

MIG_002 Le unità elettroniche di bordo di seconda generazione devono essere in grado di utilizzare ogni carta del conducente, di controllo o dell'azienda di prima generazione inserita che sia valida.

MIG_003 Questa capacità può essere soppressa definitivamente in tali unità elettroniche di bordo dalle officine in modo che le carte tachigrafiche di prima generazione non siano più accettate. Tuttavia ciò sarà possibile solo dopo che la Commissione europea avrà avviato una procedura per richiedere alle officine di compiere tale azione, ad esempio durante l'ispezione periodica del tachigrafo.

MIG_004 Le unità elettroniche di bordo di seconda generazione devono essere in grado di utilizzare esclusivamente le carte dell'officina di seconda generazione.

MIG_005 Per determinare le modalità di funzionamento, le unità elettroniche di bordo di seconda generazione devono tenere in considerazione solo il tipo della carta valida inserita, indipendentemente dalla sua generazione.

MIG_006 Ogni carta tachigrafica di seconda generazione valida deve poter essere utilizzata nelle unità elettroniche di bordo di prima generazione nello stesso modo di una carta tachigrafica di prima generazione dello stesso tipo.

2.3. **Interoperabilità tra VU e MS**

È sottinteso che i sensori di movimento (MS) di prima generazione sono interoperabili con le unità elettroniche di bordo di prima generazione, mentre i sensori di movimento di seconda generazione sono interoperabili con le unità elettroniche di bordo di seconda generazione Inoltre si applicano i seguenti requisiti.

MIG_007 Le unità elettroniche di bordo di seconda generazione non potranno essere abbinate a sensori di movimento di prima generazione.

MIG_008 I sensori di movimento di seconda generazione potranno essere abbinati e utilizzati unicamente con unità elettroniche di bordo di seconda generazione oppure con entrambe le generazioni di unità elettroniche di bordo.

2.4. **Interoperabilità tra unità elettroniche di bordo, carte tachigrafiche e apparecchi per il trasferimento di dati**

MIG_009 Gli apparecchi per il trasferimento di dati possono essere utilizzati solo con una generazione di unità elettroniche di bordo oppure con entrambe.

▼B

2.4.1 *Trasferimento diretto dalla carta mediante IDE*

MIG_010 I dati vanno trasferiti mediante IDE dalle carte tachigrafiche di prima generazione inserite nei lettori di carte, utilizzando i meccanismi di sicurezza e il protocollo di trasferimento dati di questa generazione. I dati trasferiti devono corrispondere al formato definito per questa generazione.

MIG_011 Per consentire il controllo dei conducenti da parte di autorità non UE deve essere inoltre possibile trasferire dati dalle carte del conducente (e dell'officina) di seconda generazione allo stesso modo delle carte del conducente (e dell'officina) di prima generazione. Tali trasferimenti devono includere:

— EF `IC` e `ICC` non firmati,

— EF (prima generazione) `Card_Certificate` e `CA_Certificate` non firmati,

— gli altri EF dei dati applicativi (entro `TACHO` DF) richiesti dal protocollo di trasferimento della carta di prima generazione. Tali informazioni devono essere securizzate mediante una firma digitale conformemente ai meccanismi di sicurezza di prima generazione.

Tali trasferimenti di dati non devono includere gli EF dei dati applicativi presenti solo nelle carte del conducente (e dell'officina) di seconda generazione (EF dei dati applicativi entro `TACHO_G2` DF).

2.4.2 *Trasferimento di dati dalla carta mediante un'unità elettronica di bordo*

MIG_012 I dati vanno trasferiti da una carta di seconda generazione inserita in un'unità elettronica di bordo di prima generazione utilizzando il protocollo di trasferimento dati di prima generazione. La carta deve rispondere ai comandi dell'unità elettronica di bordo esattamente nello stesso modo in cui risponde una carta di prima generazione. I dati trasferiti devono avere lo stesso formato dei dati trasferiti da una carta di prima generazione.

MIG_013 I dati vanno trasferiti da una carta di prima generazione inserita in un'unità elettronica di bordo di seconda generazione utilizzando il protocollo di trasferimento dati di cui all'appendice 7 del presente allegato. L'unità elettronica di bordo deve inviare i comandi alla carta esattamente nello stesso modo in cui li invia un'unità elettronica di bordo di prima generazione. I dati trasferiti devono rispettare il formato definito per le carte di prima generazione.

2.4.3 *Trasferimento dall'unità elettronica di bordo*

MIG_014 I dati vanno trasferiti da un'unità elettronica di bordo di seconda generazione utilizzando i meccanismi di sicurezza di seconda generazione e il protocollo di trasferimento dati di cui all'appendice 7 del presente allegato.

MIG_015 Per consentire il controllo dei conducenti da parte di autorità non UE e il trasferimento di dati dall'unità elettronica di bordo da officine non UE, facoltativamente, può essere possibile trasferire i dati da unità elettroniche di bordo di seconda generazione utilizzando meccanismi di sicurezza di prima generazione e il protocollo di trasferimento dati di prima generazione. I dati trasferiti devono avere lo stesso formato dei dati trasferiti da un'unità elettronica di bordo di prima generazione. Questa capacità può essere selezionata mediante i comandi del menù.

▼B

2.5. **Interoperabilità tra VU e apparecchiatura di taratura**

MIG_016 L'apparecchiatura di taratura deve essere in grado di tarare ogni generazione di tachigrafo, utilizzando il protocollo di taratura della generazione in questione. L'apparecchiatura di taratura può essere utilizzata con una sola generazione di tachigrafo o con entrambe.

3. FASI PRINCIPALI PRIMA DELL'INTRODUZIONE

MIG_017 Chiavi e certificati di prova devono essere messi a disposizione dei fabbricanti almeno **30 mesi** prima della data di introduzione.

MIG_018 Le prove di interoperabilità devono essere pronte ad iniziare, su richiesta dei fabbricanti, almeno **15 mesi** prima della data di introduzione.

MIG_019 Chiavi e certificati ufficiali devono essere messi a disposizione dei fabbricanti almeno **12 mesi** prima della data di introduzione.

MIG_020 Gli Stati membri devono essere in grado di rilasciare carte dell'officina di seconda generazione almeno **3 mesi** prima della data di introduzione.

MIG_021 Gli Stati membri devono essere in grado di rilasciare tutti i tipi di carte tachigrafiche di seconda generazione almeno **1 mese prima della data di introduzione**.

4. DISPOSIZIONI PER IL PERIODO SUCCESSIVO ALL'INTRODUZIONE

MIG_022 Dopo la data di introduzione gli Stati membri potranno rilasciare soltanto carte tachigrafiche di seconda generazione.

MIG_023 I fabbricanti di unità elettroniche di bordo/sensori di movimento potranno produrre unità elettroniche di bordo/sensori di movimento di prima generazione finché essi sono utilizzati sul campo, in modo che sia possibile sostituire componenti che non funzionano correttamente.

MIG_024 I fabbricanti di unità elettroniche di bordo/sensori di movimento potranno richiedere e ottenere l'omologazione della manutenzione di unità elettroniche di bordo/sensori di movimento di prima generazione che sono stati già omologati.

▼B

Appendice 15

ADATTATORE PER VEICOLI DELLE CATEGORIE M1 E N1

INDICE

1. ABBREVIAZIONI E DOCUMENTI DI RIFERIMENTO

1.1. Abbreviazioni

1.2. Norme di riferimento

2. CARATTERISTICHE E FUNZIONI GENERALI DELL'ADATTATORE

2.1. Descrizione generale dell'adattatore

2.2. Funzioni

2.3. Sicurezza

3. REQUISITI DELL'APPARECCHIO DI CONTROLLO QUANDO È MONTATO UN ADATTATORE

4. REQUISITI DI COSTRUZIONE E FUNZIONAMENTO DELL'ADATTATORE

4.1. Interfaccia e adattamento degli impulsi di velocità in entrata

4.2. Trasferimento degli impulsi in entrata al sensore di movimento incorporato

4.3. Sensore di movimento incorporato

4.4. Requisiti di sicurezza

4.5. Caratteristiche prestazionali

4.6. Materiali

4.7. Contrassegni

5. MONTAGGIO DELL'APPARECCHIO DI CONTROLLO QUANDO È UTILIZZATO UN ADATTATORE

5.1. Montaggio

5.2. Sigilli

6. VERIFICHE, CONTROLLI E RIPARAZIONI

6.1. Controlli periodici

7. OMOLOGAZIONE DELL'APPARECCHIO DI CONTROLLO QUANDO È UTILIZZATO UN ADATTATORE

7.1. Prescrizioni generali

7.2. Certificato funzionale

1. ABBREVIAZIONI E DOCUMENTI DI RIFERIMENTO

1.1. **Abbreviazioni**

TBD To Be Defined (da definire)

VU Vehicle Unit (Unità elettronica di bordo)

1.2. **Norme di riferimento**

ISO16844-3 Road vehicles — Tachograph systems — Part 3: Motion sensor interface (Veicoli stradali — Sistemi tachigrafici — Parte 3: Interfaccia del sensore di movimento).

2. CARATTERISTICHE E FUNZIONI GENERALI DELL'ADATTATORE

2.1. **Descrizione generale dell'adattatore**

ADA_001 L'adattatore fornisce a una VU collegata dati di movimento securizzati che sono costantemente rappresentativi della velocità del veicolo e della distanza percorsa.

L'adattatore è destinato esclusivamente ai veicoli per i quali è obbligatorio il montaggio dell'apparecchio di controllo in conformità del presente regolamento.

▼B

Esso è montato e utilizzato esclusivamente sui tipi di veicoli definiti alla lettera yy) «adattatore» dell'allegato IC, nei casi in cui non è meccanicamente possibile montare un altro tipo di sensore di movimento che sia altrimenti conforme alle disposizioni del presente allegato e delle appendici da 1 a 16 dello stesso.

L'adattatore non deve essere collegato meccanicamente a una parte mobile del veicolo, bensì agli impulsi relativi alla velocità/distanza generati da sensori integrati o interfacce alternative.

ADA_002 Un sensore di movimento omologato (conformemente alle disposizioni del presente allegato IC, sezione 8 — omologazione dell'apparecchio di controllo e delle carte tachigrafiche) è montato nell'alloggiamento dell'adattatore, che comprende inoltre un dispositivo di conversione che trasferisce gli impulsi in entrata al sensore di movimento incorporato. Il sensore di movimento incorporato deve a sua volta essere collegato alla VU in modo che l'interfaccia tra la VU e l'adattatore sia conforme ai requisiti della norma ISO16844-3.

2.2. **Funzioni**

ADA_003 L'adattatore svolge le seguenti funzioni:

— interfaccia e adattamento degli impulsi di velocità in entrata;

— trasferimento degli impulsi in entrata al sensore di movimento incorporato;

— tutte le funzioni del sensore di movimento incorporato per fornire alla VU dati di movimento securizzati.

2.3. **Sicurezza**

ADA_004 La certificazione di sicurezza dell'adattatore non si basa sugli obiettivi generali di sicurezza per i sensori di movimento di cui all'appendice 10 del presente allegato. A esso si applicano invece i requisiti specificati al punto 4.4 della presente appendice.

3. REQUISITI DELL'APPARECCHIO DI CONTROLLO QUANDO È MONTATO UN ADATTATORE

I requisiti di cui ai successivi punti indicano come interpretare i requisiti del presente allegato quando viene utilizzato un adattatore. I pertinenti riferimenti numerici dei requisiti dell'allegato IC sono indicati tra parentesi.

ADA_005 L'apparecchio di controllo dei veicoli provvisti di adattatore deve essere conforme a tutte le disposizioni del presente allegato, salvo quando diversamente specificato nella presente appendice.

ADA_006 Quando è montato un adattatore, l'apparecchio di controllo comprende i cavi, l'adattatore (incluso il sensore di movimento) e una VU [01].

ADA_007 La funzione di rilevamento di anomalie e/o guasti dell'apparecchio di controllo è modificata come segue:

— l'anomalia «interruzione dell'alimentazione di energia» (power supply interruption) è attivata dalla VU, quando non è attiva la modalità di taratura, per qualsiasi interruzione di durata superiore a 200 millisecondi dell'alimentazione del sensore di movimento incorporato (79);

▼B

— l'anomalia «errore dei dati di movimento» (motion data error) è attivata dalla VU in caso di interruzione del normale flusso di dati tra il sensore di movimento incorporato e l'unità elettronica di bordo e/o nel caso di un errore di integrità o di autenticazione dei dati durante lo scambio di dati tra il sensore di movimento incorporato e la VU (83);

— l'anomalia «tentativi di violazione della sicurezza» (security breach attempt) è attivata dalla VU per ogni altra anomalia relativa alla sicurezza del sensore di movimento incorporato, quando non è attiva la modalità di taratura (85);

— l'indicazione guasto dell'«apparecchio di controllo» (recording equipment) è attivata dalla VU, quando non è attiva la modalità di taratura, per ogni guasto del sensore di movimento incorporato (88).

ADA_008 I guasti dell'adattatore individuabili dall'apparecchio di controllo sono quelli relativi al sensore di movimento incorporato [88].

ADA_009 La funzione di taratura della VU consente l'abbinamento automatico del sensore di movimento incorporato alla VU [202, 204].

4. REQUISITI DI COSTRUZIONE E FUNZIONAMENTO DELL'ADATTATORE

4.1. **Interfaccia e adattamento degli impulsi di velocità in entrata**

ADA_011 L'interfaccia di entrata dell'adattatore accetta impulsi di frequenza corrispondenti alla velocità del veicolo e alla distanza da esso percorsa. Le caratteristiche elettriche degli impulsi in ingresso sono: *TBD dal fabbricante*. Gli adeguamenti che possono essere apportati solo dal fabbricante dell'adattatore e dall'officina autorizzata che effettua il montaggio dell'adattatore devono consentire, se del caso, il corretto collegamento dell'input dell'adattatore al veicolo.

ADA_012 L'interfaccia di ingresso dell'adattatore deve essere in grado, se del caso, di moltiplicare o dividere gli impulsi di frequenza degli impulsi di velocità in entrata per un fattore fisso in modo da adeguare il segnale all'intervallo del fattore k definito dal presente allegato (da 4 000 a 25 000 impulsi/km). Il fattore fisso può essere programmato soltanto dal fabbricante dell'adattatore e dall'officina autorizzata che monta l'adattatore.

4.2. **Trasferimento degli impulsi in entrata al sensore di movimento incorporato**

ADA_013 Gli impulsi in entrata, eventualmente adattati come sopra specificato, sono trasferiti al sensore di movimento incorporato in modo tale che ogni impulso in entrata sia captato dal sensore di movimento.

4.3. **Sensore di movimento incorporato**

ADA_014 Il sensore di movimento incorporato è stimolato dagli impulsi trasferiti che gli permettono di generare dati di movimento che rappresentano con accuratezza il movimento del veicolo come se fosse meccanicamente collegato a una parte mobile dello stesso.

ADA_015 I dati di identificazione del sensore di movimento incorporato sono utilizzati dalla VU per identificare l'adattatore [95].

▼B

ADA_016 Si considera che i dati di montaggio contenuti nel sensore di movimento incorporato rappresentino i dati di montaggio dell'adattatore [122].

4.4. **Requisiti di sicurezza**

ADA_017 L'alloggiamento dell'adattatore deve essere progettato in modo che non sia possibile aprirlo. Esso deve essere sigillato in modo da consentire di individuare agevolmente i tentativi di manomissione fisica (ad esempio mediante ispezione visiva, cfr. ADA_035). I sigilli devono soddisfare gli stessi requisiti dei sigilli dei sensori di movimento [da 398 a 406].

ADA_018 Non deve essere possibile asportare dall'adattatore il sensore di movimento incorporato senza manomettere il o i sigilli dell'alloggiamento dell'adattatore o il sigillo apposto tra l'alloggiamento del sensore e quello dell'adattatore (cfr. ADA_034).

ADA_019 L'adattatore garantisce che i dati di movimento possano essere elaborati e ricavati soltanto in base all'input dell'adattatore.

4.5. **Caratteristiche prestazionali**

ADA_020 L'adattatore deve essere completamente funzionale nell'intervallo di temperatura definito dal fabbricante.

ADA_021 L'adattatore deve essere in grado di funzionare correttamente nel campo di umidità compreso tra 10 % e 90 % [214].

ADA_021 L'adattatore deve essere protetto contro sovratensione, inversione di polarità dell'alimentazione e corto circuiti [216].

ADA_023 L'adattatore:

— deve reagire a un campo magnetico che disturba il rilevamento dei dati di movimento del veicolo. In queste circostanze, l'unità elettronica di bordo del veicolo registra e memorizza un guasto del sensore [88]; oppure

— deve disporre di un elemento di rilevazione protetto dai campi magnetici o immune agli stessi [217].

ADA_024 L'adattatore deve essere conforme al regolamento internazionale UNECE n. 10 concernente la compatibilità elettromagnetica e deve essere protetto contro le scariche elettrostatiche e i transitori [218].

4.6. **Materiali**

ADA_025 L'adattatore deve essere conforme al grado di protezione *(TBD dal fabbricante in funzione della posizione di montaggio)* [220, 221].

ADA_026 L'alloggiamento dell'adattatore deve essere di colore giallo.

4.7. **Contrassegni**

ADA_027 Sull'adattatore deve essere affissa una targhetta segnaletica indicante:

— nome e indirizzo del fabbricante dell'adattatore;

— il codice componente del fabbricante e l'anno di fabbricazione dell'adattatore;

— il marchio di omologazione del tipo di adattatore o del tipo di apparecchio di controllo che comprende l'adattatore;

— la data in cui è stato montato l'adattatore;

▼B

— il numero di identificazione del veicolo su cui è stato montato.

ADA_028 La targhetta segnaletica deve riportare inoltre le seguenti informazioni (se non sono direttamente leggibili all'esterno del sensore di movimento incorporato):

— nome del fabbricante del sensore di movimento incorporato;

— il codice componente del fabbricante e l'anno di fabbricazione del sensore di movimento incorporato;

— il marchio di omologazione del sensore di movimento incorporato.

5. MONTAGGIO DELL'APPARECCHIO DI CONTROLLO QUANDO È UTILIZZATO UN ADATTATORE

5.1. **Montaggio**

ADA_029 Gli adattatori destinati al montaggio sui veicoli devono essere installati esclusivamente dai costruttori dei veicoli o dalle officine autorizzate, abilitati a montare, attivare e tarare i tachigrafi digitali e intelligenti.

ADA_030 Le officine abilitate che effettuano il montaggio dell'adattatore regolano l'interfaccia di ingresso e selezionano il rapporto di divisione del segnale di ingresso (se applicabile).

ADA_031 Le officine abilitate che effettuano il montaggio dell'adattatore appongono i sigilli sull'alloggiamento dello stesso.

ADA_032 L'adattatore è montato quanto più vicino possibile alla parte del veicolo che gli fornisce gli impulsi in entrata.

ADA_033 I cavi per l'alimentazione dell'adattatore devono essere di colore rosso (polo positivo) e nero (terra).

5.2. **Sigilli**

ADA_034 Per quanto riguarda i sigilli, si applicano i seguenti requisiti:

— l'alloggiamento dell'adattatore deve essere sigillato (cfr. ADA_017);

— l'alloggiamento del sensore incorporato deve essere sigillato all'alloggiamento dell'adattatore, salvo nei casi in cui non sia possibile rimuovere il sensore incorporato senza rompere il o i sigilli dell'alloggiamento dell'adattatore (cfr. ADA_018);

— l'alloggiamento dell'adattatore deve essere sigillato al veicolo;

— il collegamento tra l'adattatore e l'apparecchiatura che gli fornisce gli impulsi in entrata deve essere sigillato alle due estremità (nella misura in cui ciò sia ragionevolmente possibile).

6. VERIFICHE, CONTROLLI E RIPARAZIONI

6.1. **Controlli periodici**

ADA_035 Quando viene utilizzato un adattatore, ogni ispezione periodica dell'apparecchio di controllo (ispezione periodica conforme ai requisiti da [409] a [413] dell'allegato 1C) deve verificare che:

— l'adattatore rechi i pertinenti marchi di omologazione;

— i sigilli sull'adattatore e sui suoi collegamenti siano integri;

▼B

— l'adattatore sia montato come indicato sulla targhetta di montaggio;

— l'adattatore sia montato come specificato dal fabbricante dell'adattatore e/o dal costruttore del veicolo;

— il montaggio dell'adattatore sia autorizzato per il veicolo oggetto di ispezione.

ADA_036 Tali controlli devono prevedere una taratura e una sostituzione dei sigilli indipendentemente dal loro stato.

7. OMOLOGAZIONE DELL'APPARECCHIO DI CONTROLLO QUANDO È UTILIZZATO UN ADATTATORE

7.1. **Prescrizioni generali**

ADA_037 L'apparecchio di controllo deve essere presentato all'omologazione completo e munito dell'adattatore [425].

ADA_038 Qualsiasi adattatore può essere presentato all'omologazione in quanto tale o come componente dell'apparecchio di controllo.

ADA_039 Tale omologazione deve includere prove funzionali dell'adattatore. I risultati positivi di ciascuna di queste prove vanno riportati su un apposito certificato [426].

7.2. **Certificato funzionale**

ADA_040 Al fabbricante dell'adattatore viene rilasciato un certificato funzionale relativo all'adattatore o all'apparecchio di controllo comprendente un adattatore solo se tutte le seguenti prove funzionali minime hanno dato esito positivo.

N.	Prova	Descrizione	Requisiti applicabili
1.	**Esame amministrativo**		
1.1	Documentazione	Validità della documentazione dell'adattatore	
2.	**Controllo visivo**		
2.1.	Conformità dell'adattatore con la documentazione		
2.2.	Identificazione/marcatura dell'adattatore		ADA_027, ADA_028
2.3	Materiali dell'adattatore		dal [219] al [223] ADA_026
2.4.	Sigilli		ADA_017, ADA_018, ADA_034
3.	**Prove funzionali**		
3.1	Trasferimento degli impulsi di velocità al sensore di movimento incorporato		ADA_013

▼B

N.	Prova	Descrizione	Requisiti applicabili
3.2	Interfaccia e adattamento degli impulsi di velocità in entrata		ADA_011, ADA_012
3.3	Precisione della misurazione del movimento		da [30] a [35], [217]
4.	**Prove ambientali**		
4.1	Risultati delle prove fabbricante	Risultati delle prove ambientali del fabbricante	ADA_020, ADA_021, ADA_022, ADA_024
5.	**EMC**		
5.1	Emissioni irradiate e sensibilità ai disturbi	Verifica della conformità con la direttiva 2006/28/CE	ADA_024
5.2	Risultati delle prove fabbricante	Risultati delle prove ambientali del fabbricante	ADA_024

▼C1

ALLEGATO II

MARCHIO E SCHEDA DI OMOLOGAZIONE

I. MARCHIO DI OMOLOGAZIONE

1. Il marchio di omologazione è composto:

a) da un rettangolo, all'interno del quale si trova la lettera «e» seguita da un numero distintivo o da una lettera distintiva del paese che ha rilasciato l'omologazione, come segue:

Belgio	6,
Bulgaria	34,
Repubblica ceca	8,
Danimarca	18,
Germania	1,
Estonia	29,
Irlanda	24,
Grecia	23,
Spagna	9,
Francia	2,
Croazia	25,
Italia	3,
Cipro	CY,
Lettonia	32,
Lituania	36,
Lussemburgo	13,
Ungheria	7,
Malta	MT,
Paesi Bassi	4,
Austria	12,
Polonia	20,
Portogallo	21,
Romania	19,
Slovenia	26,
Slovacchia	27,
Finlandia	17,
Svezia	5,
Regno Unito	11,

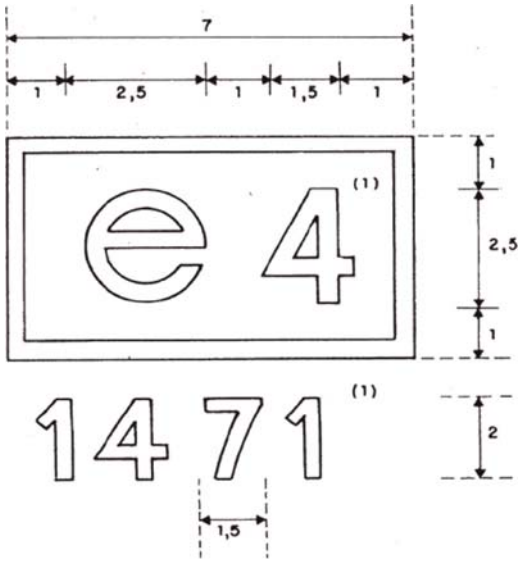
e

b) da un numero di omologazione corrispondente al numero della scheda di omologazione compilata per il prototipo dell'apparecchio di controllo o del foglio di registrazione o al numero di una carta tachigrafica, posto in una posizione qualsiasi in prossimità di tale rettangolo.

▼C1

2. Il marchio di omologazione è apposto sulla targhetta segnaletica di ciascun apparecchio, su ciascun foglio di registrazione e su ogni carta tachigrafica. Esso deve essere indelebile e rimanere sempre ben leggibile.

3. Le dimensioni del marchio di omologazione disegnate di seguito ([1]) sono espresse in millimetri e rappresentano dei minimi. Si devono rispettare i rapporti fra queste dimensioni.



([1]) Queste cifre sono riportate unicamente a titolo indicativo.

▼C1

II. SCHEDA DI OMOLOGAZIONE DEI TACHIGRAFI ANALOGICI

Lo Stato membro che ha rilasciato l'omologazione, rilascia al richiedente una scheda di omologazione, il cui modello è riprodotto di seguito. Per la notifica agli altri Stati membri delle omologazioni rilasciate o eventualmente revocate, ciascuno Stato membro deve utilizzare copie di tale scheda.

SCHEDA DI OMOLOGAZIONE

Nome dell'amministrazione competente .....

Notifica concernente ([1]):

— l'omologazione di un tipo di apparecchio di controllo

— la revoca dell'omologazione di un tipo di apparecchio di controllo

— l'omologazione di un modello di foglio di registrazione

— la revoca dell'omologazione di un modello di foglio di registrazione

Omologazione n.:

.....

1. Marchio o denominazione commerciale .....
2. Denominazione del tipo o del modello .....
3. Denominazione del costruttore .....
4. Indirizzo del costruttore .....
5. Data di presentazione per l'omologazione .....
6. Laboratorio di prova .....
7. Data e numero della/e prova/e .....
8. Data dell'omologazione .....
9. Data della revoca dell'omologazione .....
10. Tipo/i di apparecchi di controllo nel/i quale/i il foglio è destinato ad essere utilizzato
11. Luogo .....
12. Data .....
13. Documenti illustrativi allegati .....
14. Osservazioni (compresa la posizione dei sigilli, ove applicabile)

(Firma)

([1]) Cancellare le diciture non pertinenti.

▼C1

III. SCHEDA DI OMOLOGAZIONE DEI TACHIGRAFI DIGITALI

Lo Stato membro che ha rilasciato l'omologazione, rilascia al richiedente una scheda di omologazione, il cui modello è riprodotto di seguito. Per la notifica agli altri Stati membri delle omologazioni rilasciate o eventualmente revocate, ciascuno Stato membro deve utilizzare copie di tale scheda.

SCHEDA DI OMOLOGAZIONE DEI TACHIGRAFI DIGITALI

Nome dell'amministrazione competente .....

Notifica concernente ([1]):

☐ omologazione di: ☐ revoca dell'omologazione di:

☐ modello di apparecchio di controllo

☐ componente dell'apparecchio di controllo ([2])

☐ una carta del conducente

☐ una carta dell'officina

☐ una carta dell'azienda

☐ una carta dell'agente di controllo

Omologazione n.:

.....

1. Marchio di fabbrica o denominazione commerciale.....
2. Nome del modello.....
3. Denominazione del costruttore.....
4. Indirizzo del costruttore.....
5. Presentato all'omologazione il.....
6. Laboratorio/i.....
7. Data e numero del verbale di prova.....
8. Data dell'omologazione.....
9. Data della revoca dell'omologazione.....
10. Modello di apparecchio/i di controllo con cui il componente è destinato ad essere utilizzato
11. Luogo.....
12. Data.....
13. Documenti illustrativi allegati.....
14. Osservazioni (compresa la posizione dei sigilli, ove applicabile)

(Firma)

([1]) Barrare le caselle appropriate.
([2]) Specificare il componente oggetto della notifica.

▼C1

IV. SCHEDA DI OMOLOGAZIONE DEI TACHIGRAFI INTELLIGENTI

Lo Stato membro che ha rilasciato l'omologazione, rilascia al richiedente una scheda di omologazione, il cui modello è riprodotto di seguito. Per la notifica agli altri Stati membri delle omologazioni rilasciate o eventualmente revocate, ciascuno Stato membro deve utilizzare copie di tale scheda.

SCHEDA DI OMOLOGAZIONE DEI TACHIGRAFI INTELLIGENTI

Nome dell'amministrazione competente .....

Notifica concernente ([1]):

☐ omologazione di: ☐ revoca dell'omologazione di:

☐ modello di apparecchio di controllo

☐ componente dell'apparecchio di controllo ([2])

☐ una carta del conducente

☐ una carta dell'officina

☐ una carta dell'azienda

☐ una carta dell'agente di controllo

Omologazione n.:

.....

1. Marchio di fabbrica o denominazione commerciale .....
2. Nome del modello .....
3. Denominazione del costruttore .....
4. Indirizzo del costruttore .....
5. Presentato all'omologazione il .....
6. a) Laboratorio di prova per la certificazione funzionale .....
   b) Laboratorio di prova per la certificazione della sicurezza .....
   c) Laboratorio di prova per la certificazione dell'interoperabilità .....
7. a) Data e numero del certificato funzionale .....
   b) Data e numero del certificato di sicurezza .....
   c) Data e numero del certificato di interoperabilità .....
8. Data dell'omologazione .....
9. Data della revoca dell'omologazione .....
10. Modello di apparecchio/i di controllo con cui il componente è destinato ad essere utilizzato
11. Luogo .....
12. Data .....
13. Documenti illustrativi allegati .....
14. Osservazioni (compresa la posizione dei sigilli, ove applicabile)

(Firma)

([1]) Barrare le caselle appropriate.
([2]) Specificare il componente oggetto della notifica.