To besedilo je zgolj informativne narave in nima pravnega učinka. Institucije Unije za njegovo vsebino ne prevzemajo nobene odgovornosti. Verodostojne različice zadevnih aktov, vključno z uvodnimi izjavami, so objavljene v Uradnem listu Evropske unije. Na voljo so na portalu EUR-Lex. Uradna besedila so neposredno dostopna prek povezav v tem dokumentu

►B

IZVEDBENA UREDBA KOMISIJE (EU) 2016/799

z dne 18. marca 2016

o izvajanju Uredbe (EU) št. 165/2014 Evropskega parlamenta in Sveta za določitev zahtev glede konstrukcije, preskušanja, namestitve, delovanja in popravila tahografov in njihovih sestavnih delov

(Besedilo velja za EGP)

(UL L 139, 26.5.2016, str. 1)

popravljena z:

►C1 Popravek, UL L 146, 3.6.2016, str. 31 (2016/799)
►C2 Popravek, UL L 27, 1.2.2017, str. 169 (2016/799)

▼B

IZVEDBENA UREDBA KOMISIJE (EU) 2016/799

z dne 18. marca 2016

o izvajanju Uredbe (EU) št. 165/2014 Evropskega parlamenta in Sveta za določitev zahtev glede konstrukcije, preskušanja, namestitve, delovanja in popravila tahografov in njihovih sestavnih delov

(Besedilo velja za EGP)

Člen 1

Predmet urejanja in področje uporabe

1. Ta uredba vsebuje določbe, potrebne za enotno uporabo naslednjih vidikov v zvezi s tahografi:

(a) zapisovanja položaja vozila v določenih trenutkih med voznikovim dnevnim delovnim časom;

(b) zgodnjega odkrivanja morebitnega prirejanja ali zlorabe pametnih tahografov na daljavo;

(c) vmesnika za povezavo z inteligentnimi prometnimi sistemi;

(d) upravnih in tehničnih zahtev v zvezi s postopki za homologacijo tahografov, vključno z varnostnimi mehanizmi.

2. Konstrukcija, preskušanje, namestitev, pregled, delovanje in popravilo pametnih tahografov in njihovih sestavnih delov so skladni s tehničnimi zahtevami iz Priloge 1C k tej Uredbi.

3. Konstrukcija, testiranje, namestitev, pregled, delovanje in popravilo tahografov, ki niso pametni tahografi, so še naprej skladni s Prilogo 1 ali Prilogo 1B k Uredbi Sveta (EGS) št. 3821/85 ([1]), kot je ustrezno.

4. V skladu s členom 10d Direktive 96/53/ES se prek opreme za zgodnje odkrivanje na daljavo za namene zgodnjega odkrivanja goljufij prenesejo tudi podatki o masi, ki jih izmeri oprema za tehtanje, nameščena v vozilu.

Člen 2

Opredelitve pojmov

Za namene te uredbe se uporabljajo opredelitve iz člena 2 Uredbe (EU) št. 165/2014.

Poleg tega se uporabljajo še naslednje opredelitve pojmov:

(1) „digitalni tahograf“ ali „tahograf prve generacije“ pomeni digitalni tahograf, ki ni pametni tahograf;

(2) „zunanja GNSS oprema“ pomeni opremo, ki vsebuje GNSS sprejemnik, kadar enota v vozilu ni ena sama enota, ter druge komponente, ki so potrebne za zaščito sporočanja podatkov o položaju drugim delom enote v vozilu;

([1]) Uredba Sveta (EGS) št. 3821/85 z dne 20. decembra 1985 o tahografu (nadzorni napravi) v cestnem prometu (UL L 370, 31.12.1985, str. 8).

▼B

(3) „opisna mapa“ pomeni popolno mapo v elektronski obliki ali na papirju, ki vsebuje vse informacije, ki jih proizvajalec ali njegov zastopnik sporoči homologacijskemu organu za namene homologacije tahografa ali njegovega dela, vključno s potrdili iz člena 12(3) Uredbe (EU) št. 165/2014, izvedbo preskusov, opredeljenih v Prilogi 1C k tej uredbi, ter skicami, fotografijami in drugimi relevantnimi dokumenti;

(4) „opisna dokumentacija“ pomeni opisno mapo v elektronski obliki ali na papirju, ki ji je priložen kakršen koli drug dokument, ki ga je med opravljanjem svojih nalog v opisno mapo dodal homologacijski organ, vključno – po zaključenem postopku homologacije – s certifikatom o ES-homologaciji tahografa ali njegovega sestavnega dela;

(5) „seznam opisne dokumentacije“ pomeni dokument, v katerem je navedena ustrezno oštevilčena vsebina opisne dokumentacije, tako da se prepoznajo vsi relevantni deli te dokumentacije. Oblika tega dokumenta omogoča razlikovanje med posameznimi fazami postopka ES-homologacije, vključno z datumi vseh pregledov in posodobitev dokumentacije;

(6) „oprema za zgodnje odkrivanje na daljavo“ pomeni opremo enote v vozilu, ki se uporablja za izvedbo usmerjenega cestnega nadzora;

(7) „pametni tahograf“ ali „tahograf druge generacije“ pomeni digitalni tahograf, ki izpolnjuje določbe členov 8, 9 in 10 Uredbe (EU) št. 165/2014 ter Priloge 1C k tej uredbi;

(8) „sestavni del tahografa“ ali „sestavni del“ pomeni katerega koli od naslednjih elementov: enoto v vozilu, tipalo gibanja, tahografsko kartico, tahografski vložek, zunanjo GNSS opremo in opremo za zgodnje odkrivanje na daljavo;

(9) „homologacijski organ“ pomeni organ države članice, ki je pristojen za izvedbo postopka homologacije tahografa ali njegovih sestavnih delov, postopka avtorizacije ter izdajo in, če je ustrezno, preklic certifikatov o homologaciji, ki deluje kot kontaktna točka za homologacijske organe drugih držav članic in ki zagotavlja, da proizvajalci izpolnjujejo svoje obveznosti v zvezi z zagotavljanjem skladnosti z zahtevami iz te uredbe.

Člen 3

Storitve, ki temeljijo na položaju

1. Proizvajalci zagotovijo, so pametni tahografi združljivi s storitvami za določanje položaja, zagotovljenimi prek sistema Galileo in sistema skupne evropske geostacionarne navigacijske storitve (EGNOS).

2. Poleg sistemov iz odstavka 1 lahko proizvajalci zagotavljajo tudi združljivost z drugimi satelitskimi navigacijskimi sistemi.

▼B

Člen 4

Postopek za homologacijo tahografa in njegovih sestavnih delov

1. Proizvajalec ali njegov zastopnik vlogo za homologacijo tahografa ali katerega koli njegovega sestavnega dela ali skupine sestavnih delov predložita homologacijskim organom, ki jih imenuje vsaka država članica. Vloga sestoji iz opisne mape, ki vsebuje informacije o vsakem od zadevnih sestavnih delov, vključno, če je ustrezno, s certifikati o homologaciji drugih sestavnih delov, ki so potrebni za dokončanje tahografa, in vsemi drugimi relevantnimi dokumenti.

2. Država članica podeli homologacijo za vsak tahograf, njegov sestavni del ali skupino sestavnih delov, ki je skladen z upravnimi in tehničnimi zahtevami iz člena 1(2) ali (3), kot je ustrezno. V tem primeru homologacijski organ vložniku izda certifikat o homologaciji, ki je skladen s predlogo, določeno v Prilogi II k tej uredbi.

3. Homologacijski organ lahko od proizvajalca ali njegovega zastopnika zahteva, naj predloži dodatne informacije.

4. Proizvajalec ali njegov zastopnik dasta homologacijskim organom in drugim subjektom, pristojnim za izdajo potrdil iz člena 12(3) Uredbe (EU) št. 165/2014, na voljo toliko tahografov ali njihovih sestavnih delov, kot je potrebno, da se omogoči zadovoljiva izvedba postopka homologacije.

5. Kadar proizvajalec ali njegov zastopnik zaprosi za homologacijo določenih sestavnih delov ali skupin sestavnih delov tahografa, homologacijskim organom zagotovi druge sestavne dele, ki so že homologirani, in druge dele, potrebne za konstrukcijo dokončanega tahografa, da navedeni organi lahko izvedejo potrebne preskuse.

Člen 5

Spremembe homologacij

1. Proizvajalec ali njegov zastopnik o vseh spremembah programske ali strojne opreme tahografa ali vrste materialov, uporabljenih pri njegovi izdelavi, ki so vpisane v opisni dokumentaciji, nemudoma obvestijo homologacijski organ, ki je podelil prvotno homologacijo, in vložijo vlogo za spremembo homologacije.

2. Homologacijski organ lahko glede na vrsto in značilnosti sprememb revidira ali razširi obstoječo homologacijo ali izda novo homologacijo.

„Revizija“ homologacije se opravi, kadar homologacijski organ meni, da so spremembe programske ali strojne opreme tahografa ali vrste materialov, uporabljenih pri njegovi izdelavi, majhne. V tem primeru homologacijski organ izda revidirane dokumente iz opisne dokumentacije ter v njih označi vnesene spremembe in datum njihovega sprejetja. Za izpolnitev te zahteve zadostuje konsolidirana različica posodobljene opisne dokumentacije, ki ji je priložen podroben opis vnesenih sprememb.

▼B

„Razširitev“ homologacije se opravi, kadar homologacijski organ meni, da so spremembe programske ali strojne opreme tahografa ali vrste materialov, uporabljenih pri njegovi izdelavi, obsežne. V takih primerih lahko zahteva, da se izvedejo novi preskusi, in o tem ustrezno obvesti proizvajalca ali njegovega zastopnika. Če so rezultati preskusov zadovoljivi, homologacijski organ izda revidiran certifikat o homologaciji, ki vsebuje sklicno številko podeljene razširitve. V certifikatu o homologaciji sta navedena razlog za razširitev in datum njegove izdaje.

3. V seznamu opisne dokumentacije je naveden datum najnovejše razširitve ali revizije homologacije ali datum najnovejše konsolidirane različice posodobljene homologacije.

4. Kadar bi bilo zaradi zahtevane spremembe homologiranega tahografa in njegovih sestavnih delov treba izdati novo varnostno potrdilo ali potrdilo o interoperabilnosti, je potrebna nova homologacija.

Člen 6

Začetek veljavnosti

Ta uredba začne veljati dvajseti dan po objavi v *Uradnem listu Evropske unije*.

Uporablja se od 2. marca 2016.

Vendar pa se priloge uporabljajo od 2. marca 2019, razen Priloge 16, ki se uporablja od 2. marca 2016.

Ta uredba je v celoti zavezujoča in se neposredno uporablja v vseh državah članicah.

▼B

PRILOGA I C

Zahteve glede konstrukcije, testiranja, namestitve in kontrolnih pregledov

UVOD	
1	OPREDELITVE POJMOV
2	SPLOŠNE ZNAČILNOSTI IN FUNKCIJE ZAPISOVALNE NAPRAVE
2.1	Splošne značilnosti
2.2	Funkcije
2.3	Načini delovanja
2.4	Varnost
3	ZAHTEVE GLEDE KONSTRUKCIJE IN FUNKCIONALNE ZAHTEVE ZA ZAPISOVALNE NAPRAVE
3.1	Spremljanje vstavljanja in izvlačenja kartic
3.2	Merjenje hitrosti, položaja in prevožene poti
3.2.1	Merjenje prevožene poti
3.2.2	Merjenje hitrosti
3.2.3	Merjenje položaja
3.3	Merjenje časa
3.4	Spremljanje voznikovih dejavnosti
3.5	Spremljanje stanja vožnje
3.6	Voznikovi vnosi
3.6.1	Vnos krajev, v katerih se dnevne delovne izmene začnejo in/ali končajo
3.6.2	Ročni vnos voznikovih dejavnosti in izrecna privolitev voznika za vmesnik z ITS
3.6.3	Vnos posebnih stanj
3.7	Upravljanje blokad s strani podjetja
3.8	Spremljanje nadzornih dejavnosti
3.9	Zaznavanje dogodkov in/ali napak
3.9.1	Dogodek „vstavitev neveljavne kartice“
3.9.2	Dogodek „navzkrižje med karticami“
3.9.3	Dogodek „časovno prekrivanje“
3.9.4	Dogodek „vožnja brez ustrezne kartice“
3.9.5	Dogodek „vstavitev kartice med vožnjo“
3.9.6	Dogodek „zadnja seja s kartico nepravilno zaključena“
3.9.7	Dogodek „prekoračitev hitrosti“
3.9.8	Dogodek „izpad napajanja“
3.9.9	Dogodek „napaka pri komuniciranju z opremo za komunikacijo na daljavo“
3.9.10	Dogodek „ni informacij o položaju s strani GNSS sprejemnika“

▼B

3.9.11	Dogodek „napaka pri komuniciranju z zunanjo GNSS opremo“
3.9.12	Dogodek „napaka v podatkih o gibanju“
3.9.13	Dogodek „navzkrižje v gibanju vozila“
3.9.14	Dogodek „poskus kršenja varnosti“
3.9.15	Dogodek „časovno navzkrižje“
3.9.16	Napaka „kartica“
3.9.17	Napaka „zapisovalna naprava“
3.10	Vgrajeni preskusi in samopreskusi
3.11	Branje iz pomnilnika podatkov
3.12	Zapisovanje in hranjenje podatkov v pomnilniku podatkov
3.12.1	Identifikacijski podatki naprave
3.12.1.1	Identifikacijski podatki enote v vozilu
3.12.1.2	Identifikacijski podatki tipala gibanja
3.12.1.3	Identifikacijski podatki globalnih satelitskih navigacijskih sistemov
3.12.2	Ključi in certifikati
3.12.3	Podatki o vstavljanju in izvleku vozniške kartice ali kartice servisne delavnice
3.12.4	Podatki o voznikovih dejavnostih
3.12.5	Kraji in položaji, kjer se dnevne delovne izmene začnejo in končajo in/ali kjer čas neprekinjene vožnje doseže 3 ure
3.12.6	Podatki števca prevožene poti
3.12.7	Podrobni podatki o hitrosti
3.12.8	Podatki o dogodkih
3.12.9	Podatki o napakah
3.12.10	Kalibracijski podatki
3.12.11	Podatki o nastavljanju časa
3.12.12	Podatki o nadzornih dejavnostih
3.12.13	Podatki o blokadah s strani podjetja
3.12.14	Podatki o prenosih podatkov
3.12.15	Podatki o posebnih stanjih
3.12.16	Podatki o tahografskih karticah
3.13	Branje s tahografskih kartic
3.14	Zapisovanje in shranjevanje podatkov na tahografske kartice
3.14.1	Zapisovanje in shranjevanje na tahografske kartice prve generacije
3.14.2	Zapisovanje in shranjevanje na tahografske kartice druge generacije
3.15	Prikazovanje
3.15.1	Privzeti prikaz
3.15.2	Opozorilni prikaz

▼B

3.15.3	Dostop do menijev
3.15.4	Drugi prikazi
3.16	Tiskanje
3.17	Opozorila
3.18	Prenos podatkov na zunanje medije
3.19	Komunikacija na daljavo za namen usmerjenega cestnega nadzora
3.20	Iznos podatkov na dodatne zunanje naprave
3.21	Kalibracija
3.22	Cestno preverjanje kalibracije
3.23	Nastavljanje časa
3.24	Delovne karakteristike
3.25	Materiali
3.26	Oznake
4	ZAHTEVE GLEDE KONSTRUKCIJE IN FUNKCIONALNE ZAHTEVE ZA TAHOGRAFSKE KARTICE
4.1	Vidni podatki
4.2	Varnost
4.3	Standardi
4.4	Okoljske in električne specifikacije
4.5	Hranjenje podatkov
4.5.1	Elementarne datoteke za identifikacijo in upravljanje kartic
4.5.2	Identifikacija kartice z integriranim vezjem
4.5.2.1	Identifikacija čipa
4.5.2.2	DIR (samo v tahografskih karticah druge generacije)
4.5.2.3	Informacija ATR (pogojno, samo v tahografskih karticah druge generacije)
4.5.2.4	Podaljšana informacija (pogojno, samo v tahografskih karticah druge generacije)
4.5.3	Vozniška kartica
4.5.3.1	Tahografska aplikacija (dostopna enotam v vozilu prve in druge generacije)
4.5.3.1.1	Identifikacija aplikacije
4.5.3.1.2	Ključi in certifikati
4.5.3.1.3	Identifikacija kartice
4.5.3.1.4	Identifikacija imetnika kartice
4.5.3.1.5	Prenos podatkov s kartice
4.5.3.1.6	Podatki o vozniškem dovoljenju
4.5.3.1.7	Podatki o dogodkih
4.5.3.1.8	Podatki o napakah
4.5.3.1.9	Podatki o voznikovih dejavnostih

▼B

4.5.3.1.10	Podatki o uporabljenih vozilih
4.5.3.1.11	Kraji, v katerih se dnevne delovne izmene začnejo in/ali končajo
4.5.3.1.12	Podatki o seji s kartico
4.5.3.1.13	Podatki o nadzornih dejavnostih
4.5.3.1.14	Podatki o posebnih stanjih
4.5.3.2	Tahografske aplikacije druge generacije (niso dostopne enotam v vozilu prve generacije)
4.5.3.2.1	Identifikacija aplikacije
4.5.3.2.2	Ključi in certifikati
4.5.3.2.3	Identifikacija kartice
4.5.3.2.4	Identifikacija imetnika kartice
4.5.3.2.5	Prenos podatkov s kartice
4.5.3.2.6	Podatki o vozniškem dovoljenju
4.5.3.2.7	Podatki o dogodkih
4.5.3.2.8	Podatki o napakah
4.5.3.2.9	Podatki o voznikovih dejavnostih
4.5.3.2.10	Podatki o uporabljenih vozilih
4.5.3.2.11	Kraji in položaji, v katerih se dnevne delovne izmene začnejo in/ali končajo
4.5.3.2.12	Podatki o seji s kartico
4.5.3.2.13	Podatki o nadzornih dejavnostih
4.5.3.2.14	Podatki o posebnih stanjih
4.5.3.2.15	Podatki o uporabljenih enotah v vozilu
4.5.3.2.16	Kraji, kjer čas neprekinjene vožnje doseže tri ure
4.5.4	Kartica servisne delavnice
4.5.4.1	Tahografska aplikacija (dostopna enotam v vozilu prve in druge generacije)
4.5.4.1.1	Identifikacija aplikacije
4.5.4.1.2	Ključi in certifikati
4.5.4.1.3	Identifikacija kartice
4.5.4.1.4	Identifikacija imetnika kartice
4.5.4.1.5	Prenos podatkov s kartice
4.5.4.1.6	Podatki o kalibraciji in nastavljanju časa
4.5.4.1.7	Podatki o dogodkih in napakah
4.5.4.1.8	Podatki o voznikovih dejavnostih
4.5.4.1.9	Podatki o uporabljenih vozilih
4.5.4.1.10	Podatki o začetku in/ali koncu dnevnih delovnih izmen
4.5.4.1.11	Podatki o seji s kartico
4.5.4.1.12	Podatki o nadzornih dejavnostih

▼B

4.5.4.1.13	Podatki o posebnih stanjih
4.5.4.2	Tahografske aplikacije druge generacije (niso dostopne enotam v vozilu prve generacije)
4.5.4.2.1	Identifikacija aplikacije
4.5.4.2.2	Ključi in certifikati
4.5.4.2.3	Identifikacija kartice
4.5.4.2.4	Identifikacija imetnika kartice
4.5.4.2.5	Prenos podatkov s kartice
4.5.4.2.6	Podatki o kalibraciji in nastavljanju časa
4.5.4.2.7	Podatki o dogodkih in napakah
4.5.4.2.8	Podatki o voznikovih dejavnostih
4.5.4.2.9	Podatki o uporabljenih vozilih
4.5.4.2.10	Podatki o začetku in/ali koncu dnevnih delovnih izmen
4.5.4.2.11	Podatki o seji s kartico
4.5.4.2.12	Podatki o nadzornih dejavnostih
4.5.4.2.13	Podatki o uporabljenih enotah v vozilu
4.5.4.2.14	Kraji, kjer čas neprekinjene vožnje doseže tri ure
4.5.4.2.15	Podatki o posebnih stanjih
4.5.5	Nadzorna kartica
4.5.5.1	Tahografska aplikacija (dostopna enotam v vozilu prve in druge generacije)
4.5.5.1.1	Identifikacija aplikacije
4.5.5.1.2	Ključi in certifikati
4.5.5.1.3	Identifikacija kartice
4.5.5.1.4	Identifikacija imetnika kartice
4.5.5.1.5	Podatki o nadzornih dejavnostih
4.5.5.2	Tahografske aplikacije druge generacije (G2) (niso dostopne enotam v vozilu prve generacije)
4.5.5.2.1	Identifikacija aplikacije
4.5.5.2.2	Ključi in certifikati
4.5.5.2.3	Identifikacija kartice
4.5.5.2.4	Identifikacija imetnika kartice
4.5.5.2.5	Podatki o nadzornih dejavnostih
4.5.6	Kartica podjetja
4.5.6.1	Tahografska aplikacija (dostopna enotam v vozilu prve in druge generacije)
4.5.6.1.1	Identifikacija aplikacije
4.5.6.1.2	Ključi in certifikati
4.5.6.1.3	Identifikacija kartice

▼B

4.5.6.1.4	Identifikacija imetnika kartice
4.5.6.1.5	Podatki o dejavnostih podjetja
4.5.6.2	Tahografske aplikacije druge generacije (G2) (niso dostopne enotam v vozilu prve generacije)
4.5.6.2.1	Identifikacija aplikacije
4.5.6.2.2	Ključi in certifikati
4.5.6.2.3	Identifikacija kartice
4.5.6.2.4	Identifikacija imetnika kartice
4.5.6.2.5	Podatki o dejavnostih podjetja
5	NAMESTITEV ZAPISOVALNE NAPRAVE
5.1	Namestitev
5.2	Namestitvena ploščica
5.3	Zapečatenje
6	PREVERJANJA, KONTROLNI PREGLEDI IN POPRAVILA
6.1	Pooblastitev izvajalcev namestitve, servisnih delavnic in proizvajalcev vozil
6.2	Preverjanje novih ali popravljenih instrumentov
6.3	Pregled namestitve
6.4	Redni kontrolni pregledi
6.5	Ugotavljanje napak
6.6	Popravila
7	IZDAJANJE KARTIC
8	HOMOLOGACIJA ZAPISOVALNE NAPRAVE IN TAHOGRAFSKIH KARTIC
8.1	Splošne točke
8.2	Potrdilo o varnosti
8.3	Potrdilo o funkcionalnosti
8.4	Potrdilo o interoperabilnosti
8.5	Certifikat o homologaciji
8.6	Izredni postopek: prva potrdila o interoperabilnosti za zapisovalne naprave in tahografske kartice druge generacije

UVOD

Sistem digitalnih tahografov prve generacije je bil uveden 1. maja 2006. V notranjem prometu se lahko uporablja do konca svoje uporabne dobe. V mednarodnem prometu pa morajo biti 15 let po začetku veljavnosti te uredbe Komisije vsa vozila opremljena s skladnim pametnim tahografom druge generacije, kot jih uvaja ta uredba.

V tej Prilogi so navedene zahteve v zvezi zapisovalnimi napravami druge generacije in tahografskimi karticami. Zapisovalne naprave druge generacije se bodo v vozila nameščale že od datuma njihove uvedbe, istočasno pa se bodo začele izdajati tudi tahografske kartice druge generacije.

Da bi se omogočila nemotena uvedba sistema tahografov druge generacije:

▼B

— so tahografske kartice druge generacije zasnovane tako, da se lahko uporabljajo tudi v enotah v vozilu prve generacije;

— se na datum uvedbe ne bo zahtevala nadomestitev tahografskih kartic prve generacije.

Tako bodo vozniki lahko obdržali svoje edinstvene vozniške kartice in jih uporabljali v obeh sistemih.

Vendar bo zapisovalne naprave druge generacije mogoče kalibrirati samo s karticami servisne delavnice druge generacije.

V tej prilogi so navedene vse zahteve v zvezi z interoperabilnostjo med sistemoma tahografov prve in druge generacije.

V Dodatku 15 so navedene vse dodatne podrobnosti o tem, kako se bo upravljal soobstoj obeh sistemov.

Seznam dodatkov:

Dodatek 1: SLOVAR PODATKOV

Dodatek 2: SPECIFIKACIJA TAHOGRAFSKIH KARTIC

Dodatek 3: PIKTOGRAMI

Dodatek 4: IZPISI

Dodatek 5: PRIKAZOVALNIK

Dodatek 6: ČELNI PRIKLJUČEK ZA KALIBRACIJO IN PRENOS PODATKOV

Dodatek 7: PROTOKOLI ZA PRENOS PODATKOV

Dodatek 8: KALIBRACIJSKI PROTOKOL

Dodatek 9: HOMOLOGACIJA IN SEZNAM MINIMALNIH ZAHTEVANIH PRESKUSOV

Dodatek 10: VARNOSTNE ZAHTEVE

Dodatek 11: SKUPNI VARNOSTNI MEHANIZMI

Dodatek 12: DOLOČANJE POLOŽAJA NA PODLAGI GLOBALNEGA SATELITSKEGA NAVIGACIJSKEGA SISTEMA (GNSS)

Dodatek 13: VMESNIK Z ITS

Dodatek 14: FUNKCIJA KOMUNIKACIJE NA DALJAVO

Dodatek 15: MIGRACIJA: UPRAVLJANJE SOOBSTOJA NAPRAV RAZLIČNIH GENERACIJ

Dodatek 16: PRETVORNIK ZA VOZILA KATEGORIJ M1 IN N1

1 OPREDELITVE POJMOV

V tej prilogi:

a) „aktivacija“ pomeni:

fazo, v kateri se vzpostavi vsestransko delovanje tahografa in se prek kartice servisne delavnice začnejo uporabljati vse funkcije, vključno z varnostnimi;

b) „avtentikacija“ pomeni:

funkcijo, namenjeno ugotavljanju in preverjanju priglašene identitete;

c) „avtentičnost“ pomeni:

lastnost, da informacija prihaja od vira, katerega identiteto je mogoče preveriti;

d) „vgrajeni preskus“ (BIT) pomeni:

preskuse, ki se izvedejo na zahtevo, sproži pa jih operater ali zunanja oprema;

▼B

e) „koledarski dan“ pomeni:

dan v razponu od 00.00 do 24.00. Vsi koledarski dnevi so vezani na čas UTC (usklajeni svetovni čas);

f) „kalibracija“ pametnega tahografa pomeni:

posodobitev ali potrditev parametrov vozila, ki se hranijo v pomnilniku podatkov. Parametri vozila vključujejo identifikacijo vozila (VIN, VRN in državo članico, v kateri je vozilo registrirano) in značilnosti vozila (w, k, l, velikosti pnevmatik, nastavitve naprave za omejevanje hitrosti (če obstaja), trenutni čas UTC, trenutno vrednost števca prevožene poti); med kalibracijo zapisovalne naprave se v pomnilnik podatkov shranijo tudi vrste in identifikatorji vseh nameščenih relevantnih pečatov;

kakršnakoli posodobitev ali potrditev samo časa UTC se šteje kot nastavljanje časa in ne kot kalibracija, če ni v nasprotju z zahtevo 409;

za kalibracijo zapisovalne naprave je potrebna kartica servisne delavnice;

g) „številka kartice“ pomeni:

niz 16 alfanumeričnih znakov, ki nedvoumno identificira tahografsko kartico v državi članici. Številka kartice vključuje indeks zaporedja kartice (če obstaja), indeks nadomestitve kartice in indeks podaljšanja kartice;

kartica je zato nedvoumno identificirana s kodo države izdajateljice in številko kartice;

h) „indeks zaporedja kartice“ pomeni:

štirinajsti alfanumerični znak v številki kartice, ki služi za razlikovanje med karticami, izdanimi podjetju, servisni delavnici ali nadzornemu organu, ki je upravičen do prejema več tahografskih kartic. Podjetje, servisna delavnica ali nadzorni organ je nedvoumno identificiran s prvimi trinajstimi znaki številke kartice;

i) „indeks podaljšanja kartice“ pomeni:

šestnajsti alfanumerični znak v številki kartice, ki se poveča za eno ob vsaki obnovitvi tahografske kartice;

j) „indeks nadomestitve kartice“ pomeni:

petnajsti alfanumerični znak v številki kartice, ki se poveča za eno ob vsaki nadomestitvi tahografske kartice;

k) „značilni koeficient vozila“ pomeni:

število, ki označuje vrednost izhodnega signala, ki ga odda tisti del vozila, ki vozilo povezuje z zapisovalno napravo (izhodna gred menjalnika ali kolesna os vozila), ko vozilo prevozi razdaljo enega kilometra, ki se meri pod standardnimi preskusnimi pogoji, kot so opredeljeni v zahtevi 414 spodaj. Značilni koeficient je izražen v impulzih na kilometer (w = … imp/km);

l) „kartica podjetja“ pomeni:

tahografsko kartico, ki jo organi države članice izdajo prevoznemu podjetju, ki mora upravljati z vozili, opremljenimi s tahografom; ta kartica identificira prevozno podjetje in omogoča prikazovanje, prenos in izpis podatkov, shranjenih v tahografu, ki jih je zaklenilo to prevozno podjetje;

▼B

m) „konstanta zapisovalne naprave“ pomeni:

število, ki označuje vrednost vhodnega signala, potrebnega za prikaz in zapis prevožene poti enega kilometra; ta konstanta je izražena v impulzih na kilometer (k = … imp/km);

n) „čas neprekinjene vožnje“ izračuna zapisovalna naprava, kot sledi ([1]):

čas neprekinjene vožnje se izračuna kot dosedanji skupni čas vožnje določenega voznika od konca njegovega zadnjega obdobja RAZPOLOŽLJIVOSTI, obdobja ODMORA/POČITKA ali NEZNANEGA ([2]) obdobja, dolgega 45 minut ali več (to obdobje je bilo lahko razdeljeno v več obdobij v skladu z Uredbo (ES) št. 561/2006 Evropskega parlamenta in Sveta ([3])). V izračunu se po potrebi upoštevajo pretekle dejavnosti, shranjene na vozniški kartici. Če voznik ni vstavil svoje kartice, izračun temelji na zapisih v pomnilniku podatkov za sedanje obdobje, ko v ustrezni reži ni bila vstavljena nobena kartica;

o) „nadzorna kartica“ pomeni:

tahografsko kartico, ki jo organi države članice izdajo pristojnemu nacionalnemu nadzornemu organu; ta kartica identificira nadzorni organ in neobvezno tudi inšpektorja ter omogoča dostop do branja, izpisa in/ali prenosa podatkov, ki so shranjeni v pomnilniku podatkov ali na vozniških karticah in neobvezno na karticah servisnih delavnic.

Omogoča tudi dostop do funkcije cestnega preverjanja kalibracije in do podatkov, shranjenih v bralniku komunikacije za zgodnje odkrivanje na daljavo;

p) „skupni čas odmorov“ izračuna zapisovalna naprava, kot sledi ([1]):

skupni čas odmorov od vožnje določenega voznika se izračuna kot dosedanji skupni čas obdobij RAZPOLOŽLJIVOSTI ali ODMORA/POČITKA ali NEZNANIH ([2]) obdobij, dolgih 15 minut ali več, od konca njegovega zadnjega obdobja RAZPOLOŽLJIVOSTI, obdobja ODMORA/POČITKA ali NEZNANEGA ([2]) obdobja, dolgega 45 minut ali več (to obdobje je bilo lahko razdeljeno v več obdobij v skladu z Uredbo (ES) št. 561/2006).

V izračunu se po potrebi upoštevajo pretekle dejavnosti, shranjene na vozniški kartici. Ne upoštevajo se morebitna neznana obdobja negativnega trajanja (čas začetka neznanega obdobja > čas konca neznanega obdobja) zaradi časovnega prekrivanja med dvema različnima zapisovalnima napravama.

([1]) Ta način izračuna časa neprekinjene vožnje in skupnega časa odmorov služi za to, da zapisovalna naprava izračuna podatke za opozorilo o prekoračitvi časa neprekinjene vožnje. Ne služi kot podlaga za pravno razlago teh časov. Če te opredelitve zaradi posodobitev druge zadevne zakonodaje postanejo zastarele, se lahko namesto njih za izračun časa neprekinjene vožnje in skupnega časa odmorov uporabijo drugi načini.

([2]) NEZNANO obdobje pomeni obdobje, v katerem vozniška kartica ni vstavljena v zapisovalno napravo in za katero ni nikakršnega ročnega vnosa voznikove dejavnosti.

([3]) Uredba (ES) št. 561/2006 Evropskega parlamenta in Sveta z dne 15. marca 2006 o usklajevanju določene socialne zakonodaje v zvezi s cestnim prometom in spremembi uredb Sveta (EGS) št. 3821/85 in (ES) št. 2135/98 ter razveljavitvi Uredbe Sveta (EGS) št. 3820/85 (UL L 102, 11.4.2006, str. 1).

▼B

Če voznik ni vstavil svoje kartice, izračun temelji na zapisih v pomnilniku podatkov za sedanje obdobje, ko v ustrezni reži ni bila vstavljena nobena kartica;

q) „pomnilnik podatkov“ pomeni:

elektronsko napravo za hranjenje podatkov, vgrajeno v zapisovalno napravo;

r) „digitalni podpis“ pomeni:

podatke, dodane bloku podatkov, ali kriptografsko transformacijo tega bloka podatkov, ki prejemniku omogočajo dokazati avtentičnost in celovitost bloka podatkov;

s) „prenos podatkov“ pomeni:

kopiranje, skupaj z digitalnim podpisom, dela ali celotnega niza datotek, shranjenih na pomnilniku podatkov enote v vozilu ali v spominu tahografske kartice, pod pogojem, da ta postopek ne spremeni ali zbriše shranjenih podatkov.

Proizvajalci pametnih tahografskih enot v vozilu in proizvajalci naprav, zasnovanih in namenjenih za prenos podatkovnih datotek, sprejmejo vse primerne ukrepe, s katerimi zagotovijo, da prevozna podjetja ali vozniki take podatke lahko prenesejo s kar najmanjšo izgubo časa.

Prenos datoteke s podrobnimi podatki o hitrosti morda ni potreben za zagotavljanje skladnosti z Uredbo (ES) št. 561/2006, lahko pa se uporabi za druge namene, na primer za preiskavo ob nesrečah;

t) „vozniška kartica“ pomeni:

tahografsko kartico, ki jo organi države članice izdajo določenemu vozniku; ta kartica identificira voznika in omogoča shranjevanje podatkov o voznikovih dejavnostih;

u) „dejanski obseg koles“ pomeni:

povprečje razdalj, ki jih prevozi vsako posamezno pogonsko kolo vozila (kolo, ki premika vozilo) med enim polnim obratom. Meritev teh razdalj se opravi pod standardnimi preskusnimi pogoji, kot so opredeljeni v zahtevi 414, rezultati pa so izraženi kot „l = … mm“. Proizvajalec vozila lahko nadomesti merjenje teh razdalj s teoretičnim izračunom, v katerem upošteva porazdelitev mase med osmi pri praznem vozilu v normalnem delovanju ([1]). Metoda takšnega teoretičnega izračuna mora biti potrjena s strani pristojnega organa države članice še pred aktivacijo tahografa.

v) „dogodek“ pomeni:

nenormalno delovanje, ki ga zazna pametni tahograf, do katerega lahko pride zaradi poskusa goljufije;

w) „zunanja GNSS oprema“ pomeni:

opremo, ki vsebuje GNSS sprejemnik, kadar enota v vozilu ni ena sama enota, ter druge sestavne dele, ki so potrebni za zaščito sporočanja podatkov o položaju drugim delom enote v vozilu;

([1]) Uredba Komisije (EU) št. 1230/2012 z dne 12. decembra 2012 o izvajanju Uredbe (ES) št. 661/2009 Evropskega parlamenta in Sveta glede zahtev za homologacijo za mase in mere motornih vozil in njihovih priklopnikov ter o spremembi Direktive 2007/46/ES Evropskega parlamenta in Sveta (UL L 353, 21.12.2012, str. 31), kot je bila nazadnje spremenjena.

▼B

x) „napaka“ pomeni:

nenormalno delovanje, ki ga zazna pametni tahograf, do katerega lahko pride zaradi nepravilnega delovanja ali okvare opreme;

y) „GNSS sprejemnik“ pomeni:

elektronsko napravo, ki sprejema in digitalno obdeluje signale enega ali več globalnih satelitskih navigacijskih sistemov (GNSS) in tako zagotovi informacije o položaju, hitrosti in času;

z) „namestitev“ pomeni:

vgradnjo tahografa v vozilo;

aa) „interoperabilnost“ pomeni:

zmožnost sistemov ter osnovnih poslovnih procesov za izmenjavo podatkov ter informacij;

bb) „vmesnik“ pomeni:

napravo med sistemi, ki omogoča njihovo medsebojno povezovanje in komuniciranje;

cc) „položaj“ pomeni:

zemljepisne koordinate vozila v danem trenutku;

dd) „tipalo gibanja“ pomeni:

del tahografa, ki daje signal, ustrezen hitrosti in/ali prevoženi poti vozila;

ee) „neveljavna kartica“ pomeni:

kartico, ki je zaznana kot kartica z napako ali pri kateri začetna avtentikacija ni bila uspešna ali kateri se veljavnost še ni začela oziroma je že potekla;

ff) „odprti standard“ pomeni:

standard iz dokumenta o specifikaciji standardov, ki je na voljo brezplačno ali po nominalni ceni in vsakomur dovoljuje kopiranje, širjenje ali brezplačno uporabo ali uporabo proti nominalnemu plačilu;

gg) „zunaj področja uporabe“ pomeni:

stanje, v katerem po določbah Uredbe Sveta (ES) št. 561/2006 uporaba zapisovalne naprave ni potrebna;

hh) „prekoračitev hitrosti“ pomeni:

prekoračitev odobrene najvišje hitrosti vozila, opredeljeno kot poljubno več kakor 60 sekund dolgo obdobje, v katerem izmerjena hitrost vozila presega omejitev, nastavljeno na napravi za omejevanje hitrosti vozila, ki jo določa Direktiva Sveta 92/6/EGS ([1]), kot je bila nazadnje spremenjena;

ii) „redni kontrolni pregledi“ pomenijo:

skupek del, opravljenih z namenom preverjanja, ali tahograf deluje pravilno, ali njegove nastavitve ustrezajo parametrom vozila in ali so na tahograf morda pritrjene naprave za prirejanje;

([1]) Direktiva Sveta 92/6/EGS z dne 10. februarja 1992 o vgradnji in uporabi naprav za omejevanje hitrosti za določene kategorije motornih vozil v Skupnosti (UL L 57, 2.3.1992, str. 27).

▼B

jj) „tiskalnik“ pomeni:

del zapisovalne naprave, ki omogoča izpisovanje shranjenih podatkov;

kk) „komunikacija za zgodnje odkrivanje na daljavo“ pomeni:

komunikacijo med opremo za zgodnje odkrivanje na daljavo in bralnikom komunikacije za zgodnje odkrivanje na daljavo med usmerjenim cestnim nadzorom z namenom odkrivanja morebitnega prirejanja ali zlorabe zapisovalnih naprav na daljavo;

ll) „oprema za komunikacijo na daljavo“ pomeni:

opremo enote v vozilu, ki se uporablja za izvedbo usmerjenega cestnega nadzora;

mm) „bralnik komunikacije za zgodnje odkrivanje na daljavo“ pomeni:

sistem, ki ga uporabljajo inšpektorji za usmerjeni cestni nadzor;

nn) „podaljšanje“ pomeni:

izdajo nove tahografske kartice, ko obstoječi tahografski kartici poteče veljavnost ali je zaradi nepravilnega delovanja vrnjena pristojnemu izdajatelju. Pri podaljšanju kartice je z gotovostjo znano, da ne obstajata hkrati dve veljavni kartici;

oo) „popravilo“ pomeni:

kakršno koli popravilo tipala gibanja ali enote v vozilu ali kabla, pri katerem je potreben odklop napajanja, njegov odklop od drugih delov tahografa ali odpiranje tipala gibanja ali enote v vozilu;

pp) „nadomestitev kartice“ pomeni:

izdajo tahografske kartice za nadomestitev obstoječe kartice, ki je bila prijavljena kot izgubljena, ukradena ali nepravilno delujoča in ni bila vrnjena pristojnemu izdajatelju. Z nadomestitvijo kartice je vedno povezano tveganje hkratnega obstoja dveh veljavnih kartic;

qq) „varnostno certificiranje“ pomeni:

proces certificiranja, ki ga opravi certifikacijski organ na podlagi skupnih meril, za zagotovitev, da obravnavana zapisovalna naprava (ali njen del) ali tahografska kartica izpolnjuje varnostne zahteve, opredeljene v ustreznih profilih zaščite;

rr) „samopreskus“ pomeni:

preskus, ki ga zapisovalna naprava ciklično in samodejno izvaja za odkrivanje napak;

ss) „merjenje časa“ pomeni:

stalni digitalni zapis usklajenega univerzalnega datuma in časa (UTC);

tt) „nastavljanje časa“ pomeni:

samodejno nastavljanje tekočega časa v rednih presledkih in v okviru maksimalnega odstopanja ene minute ali nastavljanje med kalibracijo;

uu) „velikost pnevmatike“ pomeni:

oznako mer pnevmatik (zunanjih pogonskih koles) v skladu z Direktivo 92/23/EGS ([1]), kot je bila nazadnje spremenjena;

([1]) Direktiva Sveta 92/23/EGS z dne 31. marca 1992 o pnevmatikah za motorna vozila in priklopnike ter njihovi vgradnji (UL L 129, 14.5.1992, str. 95).

▼B

vv) „identifikacija vozila“ pomeni:

številke, ki identificirajo vozilo: registrsko številko vozila (VRN) z oznako države, v kateri je vozilo registrirano, in identifikacijsko številko vozila (VIN) ([1]);

ww) v izračunih, ki jih opravlja zapisovalna naprava, „teden“ pomeni:

obdobje od 00:00 UTC v ponedeljek do 24:00 UTC v nedeljo;

xx) „kartica servisne delavnice“ pomeni:

tahografsko kartico, ki jo organi države članice izdajo imenovanemu osebju proizvajalca tahografa, izvajalcu namestitve, proizvajalcu vozil ali servisni delavnici, odobrenim v navedeni državi članici; ta kartica identificira imetnika kartice in omogoča testiranje, kalibracijo in aktivacijo tahografov in/ali prenos podatkov iz njih;

yy) „pretvornik“ pomeni:

napravo, ki neprestano daje signal, ki ustreza hitrosti vozila in/ali prevoženi poti, ter ni naprava, ki se uporablja za neodvisno zaznavanje gibanja, in:

— se namešča in uporablja samo v vozilih tipov M1 in N1 (kakor so opredeljena v Prilogi II k Direktivi 2007/46/ES Evropskega parlamenta in Sveta ([2]), kot je bila nazadnje spremenjena), ki so se začela uporabljati po 1. maju 2006,

— se namesti, če namestitev druge vrste obstoječega tipala gibanja, ki sicer je v skladu z določbami te priloge in njenih dodatkov 1 do 15, mehansko ni mogoča,

— se namesti med enoto v vozilu in mestom, kjer vgrajena tipala ali drugi vmesniki proizvajajo impulze hitrosti/razdalje,

— se z vidika enote v vozilu pretvornika vede enako, kot če bi bilo tipalo gibanja, ki je v skladu z določbami te priloge in njenih dodatkov 1 do 16, povezano z enoto v vozilu;

uporaba takega pretvornika v navedenih tipih vozil omogoča namestitev in pravilno uporabo enote v vozilu, ki je skladna z zahtevami iz te priloge;

za navedena vozila pametni tahograf vključuje kable, pretvornik in enoto v vozilu;

([1]) Direktiva Sveta z dne 18. decembra 1975 o približevanju zakonodaje držav članic o predpisanih tablicah in oznakah za motorna in priklopna vozila ter njihovi namestitvi in načinu pritrditve (UL L 24, 30.1.1976, str. 1).

([2]) Direktiva 2007/46/ES Evropskega parlamenta in Sveta z dne 5. septembra 2007 o vzpostavitvi okvira za odobritev motornih in priklopnih vozil ter sistemov, sestavnih delov in samostojnih tehničnih enot, namenjenih za taka vozila (Okvirna direktiva) (UL L 263, 9.10.2007, str. 1).

▼B

zz) „celovitost podatkov“ pomeni:

točnost in doslednost shranjenih podatkov, o kateri je mogoče sklepati ob odsotnosti kakršnih koli odklonov v podatkih med dvema posodobitvama podatkovnega zapisa. Celovitost podatkov pomeni, da so podatki natančna kopija izvirne različice, tj. da v postopku zapisovanja na tahografsko kartico in prebiranja s te kartice ali druge za to namenjene opreme ali med prenosom preko katerega koli komunikacijskega kanala niso bili poškodovani;

aaa) „zasebnost podatkov“ pomeni:

splošne tehnične ukrepe, sprejete za zagotavljanje ustreznega izvajanja načel iz Direktive 95/46/ES Evropskega parlamenta in Sveta ([1]) z dne 24. oktobra 1995 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter načel iz Direktive 2002/58/ES Evropskega parlamenta in Sveta ([2]);

bbb) „sistem pametnih tahografov“ pomeni:

zapisovalno napravo, tahografske kartice ter vso opremo, ki je z njimi v neposredni ali posredni interakciji med njihovo konstrukcijo, namestitvijo, uporabo, testiranjem in nadzorom, kot so kartice, bralnik komunikacij na daljavo in vsa druga oprema za prenos in analizo podatkov, kalibracijo, ustvarjanje, upravljanje in uvedbo varnostnih elementov itd.;

ccc) „datum uvedbe“:

36 mesecev po začetku veljavnosti podrobnih določb iz člena 11 Uredbe (EU) št. 165/2014 Evropskega parlamenta in Sveta ([3]).

Vozila, prvič registrirana po tem datumu:

— *so opremljena s tahografom, povezanim s storitvijo za določanje položaja, ki temelji na satelitskem navigacijskem sistemu,*

— *so sposobna pristojnim nadzornim organom sporočiti podatke, ki jih potrebujejo za izvedbo usmerjenega cestnega nadzora, medtem ko se vozilo giblje, in*

— *so lahko opremljena s standardiziranimi vmesniki, ki v delovnem načinu na zunanji napravi omogočajo uporabo podatkov, ki jih je zapisal ali izdelal tahograf;*

ddd) „profil zaščite“ pomeni:

dokument, ki se uporablja kot del postopka certificiranja na podlagi skupnih meril in omogoča uvedbo neodvisnih specifikacij varnostnih zahtev na področju zagotavljanja informacijske varnosti;

([1]) Direktiva Evropskega parlamenta in Sveta 95/46/ES z dne 24. oktobra 1995 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov (UL L 281, 23.11.1995, str. 31).

([2]) Direktiva 2002/58/ES Evropskega parlamenta in Sveta z dne 12. julija 2002 o obdelavi osebnih podatkov in varstvu zasebnosti na področju elektronskih komunikacij (Direktiva o zasebnosti in elektronskih komunikacijah) (UL L 201, 31.7.2002, str. 37).

([3]) Uredba (EU) št. 165/2014 Evropskega parlamenta in Sveta z dne 4. februarja 2014 o tahografih v cestnem prometu, razveljavitvi Uredbe Sveta (EGS) št. 3821/85 o tahografu (nadzorni napravi) v cestnem prometu in spremembi Uredbe (ES) št. 561/2006 Evropskega parlamenta in Sveta o usklajevanju določene socialne zakonodaje v zvezi s cestnim prometom (UL L 60, 28.2.2014, str. 1).

▼B

eee) „točnost GNSS“:

z vidika zapisovanja položaja, pridobljenega prek globalnega satelitskega navigacijskega sistema (GNSS), s tahografi pomeni vrednost napake pri določanju horizontalnega položaja (HDOP), izračunano kot minimalno vrednost HDOP, pridobljeno od razpoložljivih sistemov GNSS.

2 SPLOŠNE ZNAČILNOSTI IN FUNKCIJE ZAPISOVALNE NAPRAVE

2.1 **Splošne značilnosti**

Naloge zapisovalne naprave so zapisovanje, hranjenje, prikaz, tiskanje in iznos podatkov, povezanih z voznikovimi dejavnostmi.

Vsako vozilo, opremljeno z zapisovalno napravo v skladu z določbami iz te priloge, mora biti opremljeno s prikazovalnikom hitrosti in števcem prevožene poti. Ti funkciji sta lahko vključeni v sami zapisovalni napravi.

(1) Zapisovalna naprava obsega kable, tipalo gibanja in enoto v vozilu.

(2) Vmesnik med tipali gibanja in enoto v vozilu je skladen z zahtevami iz Dodatka 11.

(3) Enota v vozilu je povezana z globalnim(-i) satelitskim(-i) navigacijskim(-i) sistemom(-i), kot je določeno v Dodatku 12.

(4) Enota v vozilu komunicira z bralniki komunikacije za zgodnje odkrivanje na daljavo, kot je določeno v Dodatku 14.

(5) Enota v vozilu lahko vključuje vmesnik z ITS, kot je določeno v Dodatku 13.

Zapisovalna naprava je lahko povezana z drugimi napravami prek dodatnih vmesnikov in/ali prek neobveznega vmesnika z ITS.

(6) Nobena odobrena ali neodobrena vključitev v zapisovalno napravo ali priključitev nanjo kakršne koli funkcije ali ene ali več naprav ne sme posegati ali odpreti možnosti za poseganje v pravilno in varno delovanje zapisovalne naprave ali kršiti določb te uredbe.

Uporabniki se zapisovalni napravi identificirajo s tahografskimi karticami.

(7) Zapisovalna naprava uporabniku omogoča selektiven dostop do podatkov in funkcij glede na vrsto in/ali identiteto uporabnika.

Zapisovalna naprava zapisuje in shranjuje podatke v svoj pomnilnik podatkov, v opremo za komunikacijo na daljavo in na tahografske kartice.

To poteka v skladu z Direktivo 95/46/ES z dne 24. oktobra 1995 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ([1]), Direktivo 2002/58/ES Evropskega parlamenta in Sveta z dne 12. julija 2002 o obdelavi osebnih podatkov in varstvu zasebnosti na področju elektronskih komunikacij ([2]) ter členom 7 Uredbe (EU) št. 165/2014.

([1]) UL L 281, 23.11.1995, str. 31.
([2]) UL L 201, 31.7.2002, str. 37.

▼B

2.2 **Funkcije**

(8) Zapisovalna naprava zagotavlja naslednje funkcije:

— spremljanje vstavljanja in izvlačenja kartic,

— merjenje hitrosti, prevožene poti in položaja,

— merjenje časa,

— spremljanje voznikovih dejavnosti,

— spremljanje stanja vožnje,

— zapisovanje voznikovih ročnih vnosov:

— vnos krajev, v katerih se dnevne delovne izmene začnejo in/ali zaključijo,

— ročni vnos voznikovih dejavnosti,

— vnos posebnih stanj,

— upravljanje blokad s strani podjetja,

— spremljanje nadzornih dejavnosti,

— zaznavanje dogodkov in/ali napak,

— vgrajene preskuse in samopreskuse,

— branje iz pomnilnika podatkov,

— zapisovanje in shranjevanje v pomnilniku podatkov,

— branje s tahografskih kartic,

— zapisovanje in shranjevanje na tahografske kartice,

— prikazovanje,

— tiskanje,

— opozarjanje,

— prenos podatkov na zunanje medije,

— komunikacijo na daljavo za namen usmerjenega cestnega nadzora,

— iznos podatkov na dodatne naprave,

— kalibracijo,

— cestno preverjanje kalibracije,

— nastavljanje časa.

2.3 **Načini delovanja**

(9) Zapisovalna naprava omogoča štiri načine delovanja:

— delovni način,

— nadzorni način,

— kalibracijski način,

— način dela v podjetju.

(10) Zapisovalna naprava se preklopi v naslednji način delovanja glede na veljavne tahografske kartice, vstavljene v vmesniške naprave za kartice. Za določitev načina delovanja ni pomembno, v katero generacijo spada uporabljena tahografska kartica, pomembno je le, da je veljavna. Prva generacija kartic servisne delavnice se vedno šteje za neveljavno, če je vstavljena v drugo generacijo enote v vozilu.

▼B

Način delovanja		Voznikova reža				
		Ni kartice	Vozniška kartica	Nadzorna kartica	Kartica servisne delavnice	Kartica podjetja
Sovoznikova reža	Ni kartice	delovni	delovni	nadzorni	kalibracijski	delo v podjetju
	Vozniška kartica	delovni	delovni	nadzorni	kalibracijski	delo v podjetju
	Nadzorna kartica	nadzorni	nadzorni	nadzorni (*)	delovni	delovni
	Kartica servisne delavnice	kalibracijski	kalibracijski	delovni	kalibracijski (*)	delovni
	Kartica podjetja	delo v podjetju	delo v podjetju	delovni	delovni	delo v podjetju (*)

(*) V teh stanjih zapisovalna naprava uporablja le tahografsko kartico, vstavljeno v voznikovo režo.

(11) Zapisovalna naprava vstavljene neveljavne kartice ignorira, pri čemer omogoča le prikaz, tiskanje ali prenos podatkov s kartice, ki ji je potekla veljavnost.

(12) Vse funkcije, naštete v poglavju 2.2, delujejo v katerem koli načinu delovanja, pri čemer veljajo naslednje izjeme:

— funkcija kalibracije je dostopna le v kalibracijskem načinu,

— funkcija cestnega preverjanja kalibracije je dostopna le v nadzornem načinu,

— funkcija upravljanja blokad s strani podjetja je dostopna le v načinu dela v podjetju,

— funkcija spremljanja nadzornih dejavnosti deluje le v nadzornem načinu,

— funkcija prenosa podatkov ni dostopna v delovnem načinu (razen če je v zahtevi 193 določeno drugače), z izjemo prenosa podatkov z voznikove kartice, ko v enoto v vozilu ni vstavljena nobena druga vrsta kartice.

(13) Zapisovalna naprava lahko iznaša katere koli podatke na prikazovalnik, tiskalnik ali vmesnike z zunanjimi napravami, pri čemer veljajo naslednje izjeme:

— v delovnem načinu je izbrisan vsak osebni identifikacijski podatek (priimek in ime(-na)), različen od teh podatkov na vstavljeni tahografski kartici, in delno izbrisana (izbrisana vsaka liha številka od leve proti desni) številka kartice, različna od vstavljene tahografske kartice,

— v načinu dela v podjetju je možno iznašanje podatkov, povezanih z voznikom (zahteve 102, 105 in 108), le za obdobja, za katera ni blokade ali ki jih ni blokiralo nobeno drugo podjetje (kot je identificirano s prvimi 13 številkami številke kartice podjetja),

— kadar v zapisovalno napravo ni vstavljena nobena kartica, je mogoče podatke, povezane z voznikom, iznašati le za tekoči dan in za predhodnih osem koledarskih dni,

— osebni podatki iz enote v vozilu se ne iznašajo preko njenega vmesnika z ITS, razen če voznik, na katerega se podatki navezujejo, v to izrecno privoli,

▼B

— običajno obdobje veljavnosti za delovanje enot v vozilu je 15 let, z začetkom na dan izdaje potrdil zanje, vendar se enote v vozilu lahko uporabljajo nadaljnje 3 mesece, in sicer izključno za namen prenosa podatkov.

2.4 **Varnost**

Cilji varnosti sistema so zaščita pomnilnika podatkov s tem, da preprečuje nepooblaščene dostope do podatkov in nepooblaščeno manipuliranje z njimi ter da zaznava poskuse takih posegov, zaščita celovitosti in pristnosti podatkov, izmenjanih med tipalom gibanja in enoto v vozilu, zaščita celovitosti in pristnosti podatkov, izmenjanih med zapisovalno napravo in tahografskimi karticami, zaščita celovitosti in pristnosti podatkov, izmenjanih med zapisovalno napravo in zunanjo GNSS opremo, zaščita zaupnosti, celovitosti in pristnosti podatkov, izmenjanih za namen nadzora prek komunikacije za zgodnje odkrivanje na daljavo, ter preverjanje celovitosti in pristnosti prenesenih podatkov.

(14) Za zagotovitev varnosti sistema naslednji sestavni deli izpolnjujejo varnostne zahteve, določene v zadevnih profilih zaščite, kot je določeno v Dodatku 10:

— enota v vozilu,

— tahografska kartica,

— tipalo gibanja,

— zunanja GNSS oprema (ta profil je potreben in se uporablja samo za različice z zunanjo GNSS opremo).

3 ZAHTEVE GLEDE KONSTRUKCIJE IN FUNKCIONALNE ZAHTEVE ZA ZAPISOVALNE NAPRAVE

3.1 **Spremljanje vstavljanja in izvlačenja kartic**

(15) Zapisovalna naprava spremlja stanje vmesniških naprav za kartice, da zazna vstavitve in izvleke kartic.

(16) Po vstavitvi kartice zapisovalna naprava ugotovi, ali je vstavljena kartica veljavna tahografska kartica, in, če je, identificira vrsto in generacijo kartice.

Če je v zapisovalno napravo že bila vstavljena kartica z enako številko kartice ali višjim indeksom podaljšanja kartice, se kartica obravnava kot neveljavna.

Če je v zapisovalno napravo že bila vstavljena kartica z enako številko kartice in indeksom podaljšanja, vendar z višjim indeksom nadomestitve kartice, se kartica obravnava kot neveljavna.

(17) Tahografske kartice prve generacije zapisovalna naprava obravnava kot neveljavne, potem ko servisna delavnica odpravi možnost uporabe tahografskih kartic prve generacije v skladu z Dodatkom 15 (zahteva MIG003).

(18) Kartice servisne delavnice prve generacije, ki se vstavijo v zapisovalno napravo druge generacije, se obravnavajo kot neveljavne.

▼B

(19) Zapisovalna naprava je zasnovana tako, da se po pravilni vstavitvi tahografske kartice v vmesniško napravo za kartice ta zaskoči v vstavljenem položaju.

(20) Sprostitev tahografskih kartic je mogoča le, ko je vozilo ustavljeno in so potrebni podatki že shranjeni na kartici. Za sprostitev kartice je potreben aktiven poseg uporabnika.

3.2 **Merjenje hitrosti, položaja in prevožene poti**

(21) Tipalo gibanja (ki je lahko vgrajeno v pretvornik) je najpomembnejši vir za meritve hitrosti in prevožene poti.

(22) Ta funkcija na podlagi impulzov, ki jih generira tipalo gibanja, neprekinjeno meri in po potrebi posreduje vrednosti števca prevožene poti, ki ustrezajo celotni prevoženi poti vozila.

(23) Ta funkcija na podlagi impulzov, ki jih generira tipalo gibanja, neprekinjeno meri in po potrebi posreduje hitrost vozila.

(24) Funkcija merjenja hitrosti posreduje tudi informacijo, ali se vozilo premika ali pa je ustavljeno. Da se vozilo premika, velja, kakor hitro funkcija od tipala gibanja prejme več kakor 1 imp/s najmanj pet sekund zaporedoma; v nasprotnem primeru velja, da je vozilo ustavljeno.

(25) Napravi za prikaz hitrosti (merilnik hitrosti) in celotne prevožene poti (števec prevožene poti), nameščeni v katero koli vozilo, opremljeno zapisovalno napravo, skladno z določbami iz te uredbe, izpolnjujeta zahteve glede največjih dovoljenih odstopanj (glej poglavji 3.2.1 in 3.2.2), določenih v tej prilogi.

(26) Za odkrivanje prirejanja podatkov v zvezi z gibanjem so informacije, ki jih posreduje tipalo gibanja, potrjene tudi na podlagi informacij v zvezi z gibanjem vozila, pridobljenih preko GNSS sprejemnika, in po potrebi na podlagi informacij iz drugih virov, neodvisnih od tipala gibanja.

(27) Ta funkcija meri položaj vozila, s čimer omogoči samodejno zapisovanje:

— položajev, kjer voznik in/ali sovoznik začne svojo dnevno delovno izmeno,

— položajev, kjer čas neprekinjene vožnje voznika doseže večkratnik treh ur,

— položajev, kjer voznik in/ali sovoznik konča svojo delovno izmeno.

3.2.1 *Merjenje prevožene poti*

(28) Prevožena pot se lahko meri na enega od naslednjih načinov:

— s seštevanjem vseh premikov vozila naprej in nazaj, ali

— z upoštevanjem samo premikov vozila naprej.

(29) Zapisovalna naprava meri razdalje v območju od 0 do 9 999 999,9 km.

▼B

(30) Razdalja je izmerjena v okviru naslednjih dovoljenih odstopanj (razdalje najmanj 1 000 m):

— ± 1 % pred namestitvijo,

— ± 2 % ob namestitvi in ob rednih kontrolnih pregledih,

— ± 4 % med uporabo.

(31) Ločljivost izmerjene razdalje je enaka ali boljša od 0,1 km.

3.2.2 *Merjenje hitrosti*

(32) Zapisovalna naprava meri hitrosti v območju od 0 do 220 km/h.

(33) Za zagotovitev največjega dovoljenega odstopanja prikazane hitrosti ± 6 km/h med uporabo in ob upoštevanju:

— največjega dovoljenega odstopanja ± 2 km/h zaradi odstopanj vhodnih podatkov (odstopanja pnevmatik …) ter

— največjega dovoljenega odstopanja meritev ± 1 km/h med namestitvijo in ob rednih kontrolnih pregledih

zapisovalna naprava pri hitrostih med 20 in 180 km/h in pri značilnih koeficientih vozila med 4 000 in 25 000 imp/km meri hitrost v okviru največjega dovoljenega odstopanja ± 1 km/h (pri stalni hitrosti).

Opomba: Ločljivost naprave za hranjenje podatkov v podatke o hitrosti, ki jih hrani zapisovalna naprava, vnese še dodatno največje dovoljeno odstopanje ± 0,5 km/h.

(34) V 2 sekundah po končani spremembi hitrosti, ki se je spreminjala s hitrostjo do 2 m/s^2, se hitrost spet meri pravilno in v okviru normalnih največjih dovoljenih odstopanj.

(35) Hitrost se meri z ločljivostjo, enako ali boljšo od 1 km/h.

3.2.3 *Merjenje položaja*

(36) Zapisovalna naprava meri absolutni položaj vozila s pomočjo GNSS sprejemnika.

(37) Absolutni položaj se meri s koordinatami zemljepisne širine in dolžine v stopinjah in minutah, in sicer z ločljivostjo 1/10 minute.

3.3 **Merjenje časa**

(38) Funkcija merjenja časa meri čas neprekinjeno in navaja UTC čas in datum v digitalni obliki.

(39) UTC čas in datum se uporabljata za datiranje podatkov v zapisovalni napravi (zapisi, izmenjave podatkov) in za vse izpise, opisane v Dodatku 4 „Izpisi“.

(40) Za prikaz lokalnega časa je mogoče spreminjati zamik časa za prikaz v polurnih korakih. Drugačni zamiki, razen negativnih in pozitivnih večkratnikov pol ure, niso dovoljeni.

(41) V homologacijskih preskusnih pogojih je časovno odstopanje v mejah ± 2 sekundi na dan, ob odsotnosti kakršnega koli nastavljanja časa.

▼B

(42) Čas se meri z ločljivostjo, enako ali boljšo od 1 sekunde.

(43) Merjenje časa v homologacijskih preskusnih pogojih poteka neodvisno od izklopa zunanjega napajanja, če je ta izklop krajši od 12 mesecev.

3.4 **Spremljanje voznikovih dejavnosti**

(44) Ta funkcija neprekinjeno in ločeno nadzira dejavnosti enega voznika in enega sovoznika.

(45) Voznikove dejavnosti so: VOŽNJA, DELO, RAZPOLOŽLJIVOST ali ODMOR/POČITEK.

(46) Voznik in/ali sovoznik ima možnost ročne izbire dejavnosti DELO, RAZPOLOŽLJIVOST ali ODMOR/POČITEK.

(47) Kadar se vozilo premika, se za voznika samodejno izbere dejavnost VOŽNJA, za sovoznika pa dejavnost RAZPOLOŽLJIVOST.

(48) Ko se vozilo ustavi, se za voznika samodejno izbere dejavnost DELO.

(49) Za prvo spremembo dejavnosti v dejavnost POČITEK ali RAZPOLOŽLJIVOST v času 120 sekund od samodejne spremembe v dejavnost DELO zaradi ustavitve vozila velja, da je nastopila v trenutku, ko se je vozilo ustavilo (kar lahko prekliče prvotno spremembo v dejavnost DELO).

(50) Ta funkcija posreduje spremembe dejavnosti funkcijam zapisovanja z ločljivostjo ene minute.

(51) Če je v minuti neposredno pred določeno koledarsko minuto in v minuti neposredno za njo registrirana dejavnost VOŽNJA, ta minuta v celoti šteje kot minuta VOŽNJE.

(52) Koledarska minuta, ki v skladu z zahtevo 051 ne šteje kot minuta VOŽNJE, v celoti velja kot minuta tiste dejavnosti, ki je v tej minuti neprekinjeno trajala najdlje (ali zadnje od enako dolgih najdlje trajajočih dejavnosti).

(53) Ta funkcija tudi neprekinjeno spremlja čas neprekinjene vožnje in skupni čas odmorov voznika.

3.5 **Spremljanje stanja vožnje**

(54) Ta funkcija neprekinjeno in samodejno spremlja stanje vožnje.

(55) Stanje vožnje POSADKA je izbrano, kadar sta v napravi vstavljeni dve veljavni vozniški kartici, v vseh ostalih primerih pa je izbrano stanje vožnje POSAMEZNIK.

3.6 **Voznikovi vnosi**

3.6.1 *Vnos krajev, v katerih se dnevne delovne izmene začnejo in/ali končajo*

(56) Ta funkcija omogoča vnos krajev, kjer se po navedbah voznika in/ali sovoznika njegova/njuna dnevna delovna izmena začne in/ali konča.

▼B

(57) Kraji so opredeljeni kot država, po potrebi pa še dodatno kot regija, vnese in potrdi pa se jih ročno.

(58) Ob izvleku vozniške kartice (ali kartice servisne delavnice) zapisovalna naprava (so)voznika pozove k vnosu „kraja, kjer se konča dnevna delovna izmena“.

(59) Voznik nato vnese trenutni kraj vozila, ki se šteje za začasni vnos.

(60) Kraje začetka in/ali konca dnevnih delovnih izmen je mogoče vnašati z ukazi v menijih. Če se v eni koledarski minuti opravi več kot en tak vnos, se ohrani samo zapis zadnjega vnosa kraja začetka in zadnjega vnosa kraja konca, opravljen v tem času.

3.6.2 *Ročni vnos voznikovih dejavnosti in izrecna privolitev voznika za vmesnik z ITS*

(61) Takoj po vstavitvi vozniške kartice (ali kartice servisne delavnice), in le tedaj, zapisovalna naprava omogoči ročni vnos dejavnosti. Pri ročnih vnosih dejavnosti se uporabijo lokalne vrednosti časa in datuma časovnega pasu (zamik UTC), ki je trenutno nastavljen za enoto v vozilu.

Po vstavitvi vozniške kartice ali kartice servisne delavnice se imetnika kartice opomni na:

— datum in čas njegovega zadnjega izvleka kartice,

— neobvezno: lokalni zamik časa, ki je trenutno nastavljen za enoto v vozilu.

Ob prvi vstavitvi vozniške kartice ali kartice servisne delavnice, ki enoti v vozilu še ni poznana, se imetnika kartice vpraša, ali privoljuje v iznos osebnih podatkov, povezanih s tahografom, preko neobveznega vmesnika z ITS.

Privolitev voznika oziroma servisne delavnice je možno kadar koli aktivirati ali deaktivirati z ukazi v meniju, pod pogojem, da je vozniška kartica oziroma kartica servisne delavnice vstavljena.

Mogoč je vnos dejavnosti z naslednjimi omejitvami:

— vrste dejavnosti so DELO, RAZPOLOŽLJIVOST ali ODMOR/POČITEK;

— čas začetka in konca za vsako dejavnost je izključno v okviru obdobja od zadnjega izvleka do sedanje vstavitve kartice;

— dejavnosti se med seboj ne smejo časovno prekrivati.

Po potrebi so ročni vnosi mogoči ob prvi vstavitvi še neuporabljene vozniške kartice (ali kartice servisne delavnice).

▼B

Postopek za ročni vnos dejavnosti vključuje toliko zaporednih korakov, kot je potrebnih za nastavitev vrste, časa začetka in časa konca vsake dejavnosti. Za kateri koli del časovnega obdobja med zadnjim izvlekom in sedanjo vstavitvijo kartice ima imetnik kartice možnost, da ne določi nobene dejavnosti.

Med ročnimi vnosi, povezanimi z vstavitvijo kartice, in če je primerno, ima imetnik kartice možnost, da vnese:

— kraj, kjer se je končala prejšnja dnevna delovna izmena, v povezavi z ustreznim časom (s tem se prepiše vpis ob zadnjem izvleku kartice),

— kraj, kjer se začne trenutna dnevna delovna izmena, v povezavi z ustreznim časom.

Če imetnik kartice z možnostjo ročnega vnosa, povezanega z vstavitvijo kartice, ne vnese nobenega kraja, kjer se začne ali konča dnevna delovna izmena, se to šteje kot izjava, da se njegova delovna izmena od zadnjega izvleka kartice ni spremenila. Z naslednjim vnosom kraja, kjer se je končala prejšnja dnevna delovna izmena, se prepiše začasni vnos, vpisan med zadnjim izvlekom kartice.

Če se vnese kraj, se zapiše na ustrezno tahografsko kartico.

Ročni vnosi se prekinejo, če:

— se kartica izvleče, ali

— se vozilo premika in je kartica v voznikovi reži.

Dovoljene so dodatne prekinitve, npr. zaradi izteka časa po določenem obdobju uporabnikove nedejavnosti. Če so ročni vnosi prekinjeni, zapisovalna naprava sprejme kot veljavne vse že popolno vnesene kraje in dejavnosti (z nedvoumnim krajem in časom ali vrsto, časom začetka in časom konca dejavnosti).

Če se med ročnim vnašanjem dejavnosti za prej vstavljeno kartico vstavi druga vozniška kartica ali kartica servisne delavnice, je mogoče pred začetkom ročnih vnosov za drugo kartico dokončati ročne vnose za prej vstavljeno kartico.

Imetnik kartice ima možnost vstaviti ročne vnose po naslednjem minimalnem postopku:

— Ročni vnos dejavnosti, v časovnem zaporedju, v obdobju od zadnjega izvleka do sedanje vstavitve kartice.

— Čas začetka prve dejavnosti se nastavi na čas izvleka kartice. Za vsak naknadni vnos je čas začetka vnaprej nastavljen tako, da neposredno sledi koncu prejšnjega vnosa. Za vsako dejavnost se izbere vrsta in čas zaključka dejavnosti.

▼B

Postopek je zaključen, ko se čas zaključka ročno vnesene dejavnosti pokrije s časom vstavitve kartice. Nato lahko zapisovalna naprava imetniku kartice omogoči, da do potrditve vnosa s posebnim ukazom še spreminja podatke ročno vnesenih dejavnosti. Po tej potrditvi niso dovoljene nobene takšne spremembe več.

3.6.3 *Vnos posebnih stanj*

(62) Zapisovalna naprava vozniku omogoča vnos naslednjih dveh posebnih stanj v realnem času:

— „ZUNAJ PODROČJA UPORABE“ (začetek, konec) in

— „PREVOZ S TRAJEKTOM/VLAKOM“ (začetek, konec).

Stanje „PREVOZ S TRAJEKTOM/VLAKOM“ ni možno, kadar je odprto stanje „ZUNAJ PODROČJA UPORABE“.

Odprto stanje „ZUNAJ PODROČJA UPORABE“ zapisovalna naprava samodejno zapre, če voznik vstavi ali izvleče svojo kartico.

Odprto stanje „ZUNAJ PODROČJA UPORABE“ preprečuje naslednje dogodke in opozorila:

— vožnjo brez ustrezne kartice,

— opozorila, povezana s časom neprekinjene vožnje.

Označevalnik za začetek PREVOZA S TRAJEKTOM/VLAKOM se nastavi pred izključitvijo motorja na trajektu/vlaku.

Odprto stanje PREVOZ S TRAJEKTOM/VLAKOM se mora zapreti, ko se zgodi eden od naslednjih dogodkov:

— voznik ročno konča PREVOZ S TRAJEKTOM/VLAKOM,

— voznik izvleče svojo kartico.

Odprto stanje PREVOZ S TRAJEKTOM/VLAKOM se zapre, ko v skladu s pravili iz Uredbe (ES) št. 561/2006 ni več veljavno.

3.7 **Upravljanje blokad s strani podjetja**

(63) Ta funkcija omogoča upravljanje blokad, ki jih nastavi podjetje za omejitev lastnega dostopa do podatkov v načinu dela v podjetju.

(64) Blokade s strani podjetja sestavljata datum/čas začetka (vklop blokade) in datum/čas konca (izklop blokade), povezana z identifikacijo podjetja, kot je navedena v številki kartice podjetja (ob vklopu blokade).

(65) Blokade je mogoče vklapljati in izklapljati le v realnem času.

(66) Blokado lahko izklopi le podjetje, katerega blokada je vključena (kot je identificirano v prvih 13 številkah številke kartice podjetja) ali

(67) blokada se izklopi samodejno, ko svojo blokado vključi drugo podjetje.

▼B

(68) Če določeno podjetje vključi svojo blokado, prejšnja blokada pa je bila vklopljena za isto podjetje, se šteje, da prejšnja blokada ni bila izklopljena, pač pa ostane vklopljena še naprej.

3.8 **Spremljanje nadzornih dejavnosti**

(69) Ta funkcija spremlja dejavnosti PRIKAZOVANJA, TISKANJA, VU (enota v vozilu) in PRENOS podatkov ter CESTNO PREVERJANJE KALIBRACIJE v nadzornem načinu.

(70) Ta funkcija v nadzornem načinu spremlja tudi dejavnost NADZORA PREKORAČITVE HITROSTI. Velja, da se je nadzor prekoračitve hitrosti izvedel, kadar se v nadzornem načinu pošlje obvestilo „prekoračitev hitrosti“ na tiskalnik ali na prikazovalnik ali kadar so se iz pomnilnika podatkov VU prenesli podatki o „dogodkih in napakah“.

3.9 **Zaznavanje dogodkov in/ali napak**

(71) Ta funkcija zaznava naslednje dogodke in/ali napake:

3.9.1 *Dogodek „vstavitev neveljavne kartice“*

(72) Ta dogodek se sproži ob vstavitvi kakršne koli neveljavne kartice, ob vstavitvi vozniške kartice, ki je že bila zamenjana, in/ali ob poteku veljavnosti vstavljene veljavne kartice.

3.9.2 *Dogodek „navzkrižje med karticami“*

(73) Ta dogodek se sproži ob nastopu katere koli od kombinacij veljavnih kartic, označenih z X v naslednji preglednici:

Navzkrižje med karticami		Voznikova reža				
		Ni kartice	Vozniška kartica	Nadzorna kartica	Kartica servisne delavnice	Kartica podjetja
Sovoznikova reža	Ni kartice					
	Vozniška kartica				X	
	Nadzorna kartica			X	X	X
	Kartica servisne delavnice		X	X	X	X
	Kartica podjetja			X	X	X

3.9.3 *Dogodek „časovno prekrivanje“*

(74) Ta dogodek se sproži, kadar je s kartice prebrani datum/čas zadnjega izvleka vozniške kartice poznejši od tekočega datuma/časa zapisovalne naprave, v katero je kartica vstavljena.

3.9.4 *Dogodek „vožnja brez ustrezne kartice“*

(75) Ta dogodek se sproži ob nastopu katere koli od kombinacij tahografskih kartic, označenih z X v naslednji preglednici, ko se voznikova dejavnost preklopi v VOŽNJO ali ob kakršnikoli spremembi načina delovanja v času, ko je voznikova dejavnost VOŽNJA:

▼B

Vožnja brez ustrezne kartice		Voznikova reža				
		Brez kartice (ali neveljavna kartica)	Vozniška kartica	Nadzorna kartica	Kartica servisne delavnice	Kartica podjetja
Sovoznikova reža	Brez kartice (ali neveljavna kartica)	X		X		X
	Vozniška kartica	X		X	X	X
	Nadzorna kartica	X	X	X	X	X
	Kartica servisne delavnice	X	X	X		X
	Kartica podjetja	X	X	X	X	X

3.9.5 *Dogodek „vstavitev kartice med vožnjo“*

(76) Ta dogodek se sproži ob vstavitvi tahografske kartice v katerokoli režo med tem, ko je voznikova dejavnost VOŽNJA.

3.9.6 *Dogodek „zadnja seja s kartico nepravilno zaključena“*

(77) Ta dogodek se sproži, če zapisovalna naprava ob vstavitvi kartice zazna, da prejšnja seja s kartico ni bila zaključena pravilno glede na določbe iz poglavja 3.1 (kartica je bila izvlečena pred shranitvijo vseh potrebnih podatkov nanjo). Ta dogodek sprožijo samo vozniške kartice in kartice servisne delavnice.

3.9.7 *Dogodek „prekoračitev hitrosti“*

(78) Ta dogodek se sproži ob vsaki prekoračitvi hitrosti.

3.9.8 *Dogodek „izpad napajanja“*

(79) Ta dogodek se sproži, če naprava ni v kalibracijskem ali nadzornem načinu ter izpad napajanja tipala gibanja in/ali enote v vozilu traja več kot 200 milisekund. Prag izpada opredeli proizvajalec. Prehodni izpad napajanja ob zagonu motorja vozila ne sproži tega dogodka.

3.9.9 *Dogodek „napaka pri komuniciranju z opremo za komunikacijo na daljavo“*

(80) Ta dogodek se sproži, **kadar naprava ni v kalibracijskem načinu**, če oprema za komunikacijo na daljavo po več kot treh poskusih ne potrdi uspešnega prejema podatkov, poslanih na daljavo iz vozila.

3.9.10 *Dogodek „ni informacij o položaju s strani GNSS sprejemnika“*

(81) Ta dogodek se sproži, **kadar naprava ni v kalibracijskem načinu**, če sprejemnik GNSS (zunanji ali notranji) po več kot treh urah skupnega časa vožnje ni zagotovil informacij o položaju.

3.9.11 *Dogodek „napaka pri komuniciranju z zunanjo GNSS opremo“*

(82) Ta dogodek se sproži, **kadar naprava ni v kalibracijskem načinu**, če med tem, ko se vozilo premika, pride do prekinitve komunikacije med zunanjo GNSS opremo in enoto v vozilu, ki neprekinjeno traja več kot 20 minut.

▼B

3.9.12 *Dogodek „napaka v podatkih o gibanju“*

(83) Ta dogodek se sproži, **kadar naprava ni v kalibracijskem načinu**, če pride do prekinitve normalnega pretoka podatkov med tipalom gibanja in enoto v vozilu in/ali napake v celovitosti ali avtentikaciji podatkov pri prenosu podatkov med tipalom gibanja in enoto v vozilu.

3.9.13 *Dogodek „navzkrižje v gibanju vozila“*

(84) Ta dogodek se sproži, **kadar naprava ni v kalibracijskem načinu**, če informacije o gibanju vozila, izračunane na podlagi podatkov iz tipala gibanja, nasprotujejo informacijam o gibanju vozila, pridobljenih prek notranje ali zunanje GNSS opreme, in, če je ustrezno, podatkom iz drugih, neodvisnih virov, kot je določeno v Dodatku 12. Ta dogodek se ne sproži med prevozom s trajektom/vlakom, stanjem ZUNAJ PODROČJA UPORABE ali kadar informacije o položaju s strani GNSS sprejemnika niso na voljo.

3.9.14 *Dogodek „poskus kršenja varnosti“*

(85) Ta dogodek se sproži, kadar naprava ni v kalibracijskem načinu, ob kateremkoli dogodku, ki vpliva na varnost tipala gibanja in/ali enote v vozilu in/ali zunanje GNSS opreme, kot je določena v Dodatku 10.

3.9.15 *Dogodek „časovno navzkrižje“*

(86) Ta dogodek se sproži, **kadar naprava ni v kalibracijskem načinu**, če enota v vozilu med časom, ki ga beleži oprema za merjenje časa enote v vozilu, in časom, ki ga posreduje GNSS sprejemnik, zazna odstopanje, daljše od 1 minute. Ta dogodek se zapiše skupaj z internim časom enote v vozilu in ga spremlja samodejno nastavljanje časa. Po sproženju dogodka časovnega navzkrižja enota v vozilu 12 ur ne sproži drugih dogodkov časovnega navzkrižja. Ta dogodek se ne sproži, kadar GNSS sprejemnik v zadnjih 30 dneh ni mogel odkriti veljavnega GNSS signala. Ko so informacije o položaju prek GNSS sprejemnika spet na voljo, se opravi samodejna nastavitev časa.

3.9.16 *Napaka „kartica“*

(87) Ta napaka se sproži ob napaki na tahografski kartici med delovanjem.

3.9.17 *Napaka „zapisovalna naprava“*

(88) Ta napaka se sproži, kadar zapisovalna naprava ni v kalibracijskem načinu, ob kateri koli od naslednjih napak:

— notranja napaka VU,

— napaka na tiskalniku,

— napaka na prikazovalniku,

— napaka pri prenosu podatkov,

— napaka na tipalu,

— napaka na GNSS sprejemniku ali zunanji GNSS opremi,

— napaka na opremi za komunikacijo na daljavo.

▼B

3.10 **Vgrajeni preskusi in samopreskusi**

(89) Zapisovalna naprava sama zaznava napake z izvajanjem vgrajenih preskusov in samopreskusov v skladu z naslednjo preglednico:

Preskušani podsestav	Samopreskus	Vgrajeni preskus
Programska oprema		Celovitost
Pomnilnik podatkov	Dostop	Dostop, celovitost podatkov
Vmesniške naprave za kartice	Dostop	Dostop
Tipkovnica		Ročno preverjanje
Tiskalnik	(določi proizvajalec)	Izpis
Prikazovalnik		Vizualni pregled
Prenos podatkov (se izvaja samo med prenašanjem podatkov)	Pravilno delovanje	
Tipalo	Pravilno delovanje	Pravilno delovanje
Oprema za komunikacijo na daljavo	Pravilno delovanje	Pravilno delovanje
GNSS oprema	Pravilno delovanje	Pravilno delovanje

3.11 **Branje iz pomnilnika podatkov**

(90) Zapisovalna naprava je zmožna brati vse podatke, shranjene v njenem pomnilniku podatkov.

3.12 **Zapisovanje in hranjenje podatkov v pomnilniku podatkov**

Za namen tega odstavka velja naslednje:

— „365 dni“ pomeni 365 koledarskih dni povprečnih voznikovih dejavnosti v vozilu. Povprečna dejavnost na dan na vozilo je opredeljena kot najmanj šest voznikov ali sovoznikov, šest ciklov vstavitve in izvleka kartice ter 256 sprememb dejavnosti. „365 dni“ torej vključuje najmanj 2 190 (so)voznikov, 2 190 ciklov vstavitve in izvleka kartice in 93 440 sprememb dejavnosti;

— povprečno število položajev na dan pomeni vsaj 6 položajev, kjer se začne dnevna delovna izmena, 6 položajev, kjer čas neprekinjene vožnje voznika doseže večkratnik treh ur, in 6 položajev, kjer se dnevna delovna izmena konča, tako da „365 dni“ vključuje najmanj 6 570 položajev;

— časi so zapisani z ločljivostjo ene minute, če ni predpisano drugače;

— vrednosti števca prevožene poti so zapisane z ločljivostjo enega kilometra;

— hitrosti so zapisane z ločljivostjo 1 km/h;

— položaji (zemljepisne širine in dolžine) so zapisani v stopinjah in minutah, in sicer z ločljivostjo 1/10 minute, ob upoštevanju ustrezne točnosti GNSS in časa pridobitve.

▼B

(91) Na podatke, shranjene v pomnilniku podatkov, v homologacijskih preskusnih pogojih ne vpliva izklop zunanjega napajanja, če je ta izklop krajši od dvanajst mesecev. Poleg tega na podatke, shranjene v zunanji opremi za komunikacijo na daljavo, kot je opredeljeno v Dodatku 14, ne vpliva izklop napajanja, krajši od 28 dni.

(92) Zapisovalna naprava je zmožna v svoj pomnilnik podatkov implicitno ali eksplicitno zapisati in shraniti naslednje podatke:

3.12.1 *Identifikacijski podatki naprave*

3.12.1.1 Identifikacijski podatki enote v vozilu

(93) Zapisovalna naprava je zmožna v svojem pomnilniku podatkov hraniti naslednje identifikacijske podatke enote v vozilu:

— ime proizvajalca,

— naslov proizvajalca,

— kataloško številko,

— serijsko številko,

— generacijo VU,

— zmožnost uporabe tahografskih kartic prve generacije,

— številko različice programske opreme,

— datum namestitve različice programske opreme,

— leto izdelave opreme,

— homologacijsko številko.

(94) Identifikacijske podatke enote v vozilu enkrat za vselej zapiše in shrani njen proizvajalec, razen podatkov povezanih s programsko opremo, in homologacijske številke, ki se lahko spremenijo ob nadgradnji programske opreme, ter zmožnosti uporabe tahografskih kartic prve generacije.

3.12.1.2 Identifikacijski podatki tipala gibanja

(95) Tipalo gibanja je zmožno v svojem pomnilniku hraniti naslednje identifikacijske podatke:

— ime proizvajalca,

— serijsko številko,

— homologacijsko številko.

— identifikator vgrajenega varnostnega dela (npr. številko vgrajenega čipa/procesorja),

— identifikator operacijskega sistema (npr. številko različice programske opreme).

(96) Identifikacijske podatke tipala gibanja vanj enkrat za vselej zapiše in shrani njegov proizvajalec.

(97) Enota v vozilu je zmožna v svoj hranilnik podatkov zapisati in shraniti naslednje podatke v zvezi z 20 najnovejšimi povezavami s tipali gibanja (če je na isti dan opravljenih več povezav, se shranita le prva in zadnja povezava, opravljena tistega dne).

▼B

Za vsako od teh povezav se zapišejo naslednji podatki:

— identifikacijski podatki tipala gibanja:

— serijska številka,

— homologacijska številka;

— podatki povezave tipala gibanja:

— datum povezave.

3.12.1.3 Identifikacijski podatki globalnih satelitskih navigacijskih sistemov

(98) Zunanja GNSS oprema je zmožna v svojem pomnilniku hraniti naslednje identifikacijske podatke:

— ime proizvajalca,

— serijsko številko,

— homologacijsko številko.

— identifikator vgrajenega varnostnega dela (npr. številko vgrajenega čipa/procesorja),

— identifikator operacijskega sistema (npr. številko različice programske opreme).

(99) Identifikacijske podatke zunanje GNSS opreme vanjo enkrat za vselej zapiše in shrani njen proizvajalec.

(100) Enota v vozilu je zmožna v svojem hranilniku podatkov zapisati in shraniti naslednje podatke v zvezi z 20 najnovejšimi povezavami zunanje GNSS opreme (če je na isti dan opravljenih več povezav, se shranita le prva in zadnja povezava, opravljeni tistega dne).

Za vsako od teh povezav se zapišejo naslednji podatki:

— identifikacijski podatki zunanje GNSS opreme:

— serijska številka,

— homologacijska številka;

— podatki povezave zunanje GNSS opreme:

— datum povezave.

3.12.2 *Ključi in certifikati*

(101) Zapisovalna naprava je zmožna hraniti več različnih kriptografskih ključev in certifikatov, kot je določeno v delih A in B Dodatka 11.

3.12.3 *Podatki o vstavljanju in izvleku vozniške kartice ali kartice servisne delavnice*

(102) Za vsak cikel vstavljanja in izvleka vozniške kartice ali kartice servisne delavnice v napravo zapisovalna naprava v svoj pomnilnik podatkov zapiše in shrani naslednje podatke:

— priimek in ime(na) imetnika kartice, kot so shranjeni na kartici,

— številko kartice, državo izdajateljico in datum poteka veljavnosti, kot so shranjeni na kartici,

— generacijo kartice,

▼B

— datum in čas vstavitve,

— vrednost števca prevožene poti ob vstavitvi kartice,

— režo, v katero je kartica vstavljena,

— datum in čas izvleka,

— vrednost števca prevožene poti ob izvleku kartice,

— naslednje podatke o prejšnjem vozilu, ki ga je uporabljal voznik, kot so shranjeni na kartici:

— registrsko številko vozila in državo, v kateri je registrirano,

— generacijo enote v vozilu (če je na voljo),

— datum in čas izvleka kartice,

— označevalnik, ki kaže, ali je imetnik kartice ob vstavitvi ročno vnesel svoje dejavnosti ali ne.

(103) Pomnilnik podatkov je zmožen hraniti te podatke najmanj 365 dni.

(104) Ko se pomnilnik zapolni s podatki, se novi podatki prepišejo čez najstarejše podatke.

3.12.4 *Podatki o voznikovih dejavnostih*

(105) Zapisovalna naprava ob vsaki spremembi voznikove/sovoznikove dejavnosti in/ali ob vsaki spremembi stanja vožnje in/ali ob vsaki vstavitvi ali izvleku vozniške kartice ali kartice servisne delavnice v svojem pomnilniku podatkov zapiše in shrani naslednje podatke:

— stanje vožnje (POSADKA, POSAMEZNIK),

— režo (VOZNIK, SOVOZNIK),

— stanje kartice v ustrezni reži (VSTAVLJENA, NI VSTAVLJENA),

— dejavnost (VOŽNJA, RAZPOLOŽLJIVOST, DELO, ODMOR/POČITEK),

— datum in čas spremembe.

VSTAVLJENA pomeni, da je v reži vstavljena veljavna vozniška kartica ali kartica servisne delavnice. NI VSTAVLJENA pomeni nasprotno, tj. da v reži ni vstavljena veljavna vozniška kartica ali kartica servisne delavnice (npr. vstavljena je kartica podjetja ali pa v reži ni kartice).

Podatki o dejavnostih, ki jih ročno vnese voznik, se ne zapišejo v pomnilnik podatkov.

(106) Pomnilnik podatkov je zmožen podatke o voznikovih dejavnostih hraniti najmanj 365 dni.

(107) Ko se pomnilnik zapolni s podatki, se novi podatki prepišejo čez najstarejše podatke.

▼B

3.12.5 *Kraji in položaji, kjer se dnevne delovne izmene začnejo in končajo in/ali kjer čas neprekinjene vožnje doseže 3 ure*

(108) Zapisovalna naprava v svoj pomnilnik podatkov zapiše in shrani:

— kraje in položaje, kjer voznik in/ali sovoznik začne svojo dnevno delovno izmeno,

— položaje, kjer čas neprekinjene vožnje voznika doseže večkratnik treh ur,

— kraje in položaje, kjer voznik in/ali sovoznik konča svojo dnevno delovno izmeno.

(109) Kadar v takšnih trenutkih položaja vozila ni mogoče določiti preko GNSS sprejemnika, zapisovalna naprava uporabi zadnji zabeleženi položaj in z njim povezana datum in čas.

(110) Skupaj z vsakim krajem ali položajem zapisovalna naprava v svoj pomnilnik podatkov zapiše in shrani:

— številko in državo izdajateljico (so)vozniške kartice,

— generacijo kartice,

— datum in čas vnosa,

— vrsto vnosa (čas začetka, konca ali doseženih 3 ur neprekinjene vožnje),

— povezane točnost, datum in čas GNSS, če je ustrezno,

— vrednost števca prevožene poti.

(111) Pomnilnik podatkov je zmožen podatke o krajih in položajih, kjer se dnevne delovne izmene začnejo in končajo in/ali kjer čas neprekinjene vožnje doseže 3 ure, hraniti najmanj 365 dni.

(112) Ko se pomnilnik zapolni s podatki, se novi podatki prepišejo čez najstarejše podatke.

3.12.6 *Podatki števca prevožene poti*

(113) Zapisovalna naprava v svoj pomnilnik podatkov vsak koledarski dan ob polnoči zapiše vrednost števca prevožene poti in ustrezajoči datum.

(114) Pomnilnik podatkov je zmožen ob polnoči zapisane vrednosti števca prevožene poti hraniti najmanj 365 dni.

(115) Ko se pomnilnik zapolni s podatki, se novi podatki prepišejo čez najstarejše podatke.

3.12.7 *Podrobni podatki o hitrosti*

(116) Zapisovalna naprava v svoj pomnilnik podatkov zapiše in shrani trenutno hitrost vozila ter ustrezajoči datum in čas vsako sekundo najmanj zadnjih 24 ur gibanja vozila.

3.12.8 *Podatki o dogodkih*

Za namen tega pododstavka velja, da se čas zapisuje z ločljivostjo 1 sekunde.

(117) Zapisovalna naprava v svoj pomnilnik podatkov zapiše in shrani naslednje podatke za vsak zaznani dogodek po naslednjih pravilih shranjevanja:

▼B

Dogodek	Pravila shranjevanja	Podatki, ki se zapišejo za vsak dogodek
Vstavitev neveljavne kartice	— 10 najnovejših dogodkov.	— Datum in čas dogodka, — vrsta, številka, država izdajateljica in generacija kartic(e), s katero je dogodek nastopil, — število podobnih dogodkov v danem dnevu.
Navzkrižje med karticami	— 10 najnovejših dogodkov.	— Datum in čas začetka dogodka, — datum in čas konca dogodka, — vrsta, številka, država izdajateljica in generacija kartic, s katerima je navzkrižje nastopilo.
Vožnja brez ustrezne kartice	— Najdaljši dogodek za vsakega od 10 zadnjih dni nastopov dogodkov, — 5 najdaljših dogodkov v zadnjih 365 dneh.	— Datum in čas začetka dogodka, — datum in čas konca dogodka, — vrsta, številka, država izdajateljica in generacija katere koli kartice, vstavljene ob začetku in/ali koncu dogodka, — število podobnih dogodkov v danem dnevu.
Vstavitev kartice med vožnjo	— Zadnji dogodek za vsakega od 10 zadnjih dni nastopov dogodkov.	— Datum in čas dogodka, — vrsta, številka, država izdajateljica in generacija kartic, — število podobnih dogodkov v danem dnevu.
Zadnja seja s kartico nepravilno zaključena	— 10 najnovejših dogodkov.	— Datum in čas vstavitve kartice, — vrsta, številka, država izdajateljica in generacija kartic, — podatki zadnje seje, prebrani s kartice: — datum in čas vstavitve kartice, — registrska številka vozila, država članica registracije in generacija enote v vozilu.
Prekoračitev hitrosti (1)	— Najresnejši dogodek za vsakega od 10 zadnjih dni nastopov dogodkov (tj. tisti z najvišjo povprečno hitrostjo), — 5 najresnejših dogodkov v zadnjih 365 dneh, — prvi dogodek, ki je nastopil po zadnji kalibraciji.	— Datum in čas začetka dogodka, — datum in čas konca dogodka, — najvišja hitrost, izmerjena med dogodkom, — aritmetična sredina hitrosti, izmerjenih med dogodkom, — vrsta, številka, država izdajateljica in generacija vozniške kartice (če je ustrezno), — število podobnih dogodkov v danem dnevu.

▼B

Dogodek	Pravila shranjevanja	Podatki, ki se zapišejo za vsak dogodek
Izpad napajanja (2)	— Najdaljši dogodek za vsakega od 10 zadnjih dni nastopov dogodkov, — 5 najdaljših dogodkov v zadnjih 365 dneh.	— Datum in čas začetka dogodka, — datum in čas konca dogodka, — vrsta, številka, država izdajateljica in generacija katere koli kartice, vstavljene ob začetku in/ali koncu dogodka, — število podobnih dogodkov v danem dnevu.
Napaka pri komuniciranju z opremo za komunikacijo na daljavo	— Najdaljši dogodek za vsakega od 10 zadnjih dni nastopov dogodkov, — 5 najdaljših dogodkov v zadnjih 365 dneh.	— Datum in čas začetka dogodka, — datum in čas konca dogodka, — vrsta, številka, država izdajateljica in generacija katere koli kartice, vstavljene ob začetku in/ali koncu dogodka, — število podobnih dogodkov v danem dnevu.
Ni informacij o položaju s strani GNSS sprejemnika	— Najdaljši dogodek za vsakega od 10 zadnjih dni nastopov dogodkov, — 5 najdaljših dogodkov v zadnjih 365 dneh.	— Datum in čas začetka dogodka, — datum in čas konca dogodka, — vrsta, številka, država izdajateljica in generacija katere koli kartice, vstavljene ob začetku in/ali koncu dogodka, — število podobnih dogodkov v danem dnevu.
Napaka v podatkih o gibanju	— Najdaljši dogodek za vsakega od 10 zadnjih dni nastopov dogodkov, — 5 najdaljših dogodkov v zadnjih 365 dneh.	— Datum in čas začetka dogodka, — datum in čas konca dogodka, — vrsta, številka, država izdajateljica in generacija katere koli kartice, vstavljene ob začetku in/ali koncu dogodka, — število podobnih dogodkov v danem dnevu.
Navzkrižje v gibanju vozila	— Najdaljši dogodek za vsakega od 10 zadnjih dni nastopov dogodkov, — 5 najdaljših dogodkov v zadnjih 365 dneh.	— Datum in čas začetka dogodka, — datum in čas konca dogodka, — vrsta, številka, država izdajateljica in generacija katere koli kartice, vstavljene ob začetku in/ali koncu dogodka, — število podobnih dogodkov v danem dnevu.
Poskus kršenja varnosti	— 10 najnovejših dogodkov za vsako vrsto dogodka.	— Datum in čas začetka dogodka, — datum in čas konca dogodka (če je ustrezno), — vrsta, številka, država izdajateljica in generacija katere koli kartice, vstavljene ob začetku in/ali koncu dogodka, — vrsta dogodka.

▼B

Dogodek	Pravila shranjevanja	Podatki, ki se zapišejo za vsak dogodek
Časovno navzkrižje	— Najdaljši dogodek za vsakega od 10 zadnjih dni nastopov dogodkov, — 5 najdaljših dogodkov v zadnjih 365 dneh.	— Datum in čas zapisovalne naprave, — datum in čas GNSS, — vrsta, številka, država izdajateljica in generacija katere koli kartice, vstavljene ob začetku in/ali koncu dogodka, — število podobnih dogodkov v danem dnevu.

(1) Zapisovalna naprava v svoj pomnilnik podatkov zapiše in shrani tudi:

— datum in čas zadnjega NADZORA PREKORAČITVE HITROSTI,

— datum in čas prve prekoračitve hitrosti po tem NADZORU PREKORAČITVE HITROSTI,

— število dogodkov prekoračitve hitrosti od zadnjega NADZORA PREKORAČITVE HITROSTI.

(2) Ti podatki se lahko zapišejo le ob ponovni vzpostavitvi napajanja, časi pa so lahko znani na minuto natančno.

3.12.9 *Podatki o napakah*

Za namen tega pododstavka velja, da se čas zapisuje z ločljivostjo 1 sekunde.

(118) Zapisovalna naprava v svoj pomnilnik podatkov poskusi zapisati in shraniti naslednje podatke za vsako zaznano napako po naslednjih pravilih shranjevanja:

Napaka	Pravila shranjevanja	Podatki, ki se zapišejo za vsako napako
Napaka „kartica“	— 10 najnovejših napak na vozniški kartici.	— Datum in čas začetka napake, — datum in čas konca napake, — vrsta, številka, država izdajateljica in generacija kartic.
Napaka „zapisovalna naprava“	— 10 najnovejših napak za vsako vrsto napake, — prva napaka po zadnji kalibraciji.	— Datum in čas začetka napake, — datum in čas konca napake, — vrsta napake, — vrsta, številka, država izdajateljica in generacija katere koli kartice, vstavljene ob začetku in/ali koncu napake.

3.12.10 *Kalibracijski podatki*

(119) Zapisovalna naprava v svoj pomnilnik podatkov zapiše in shrani podatke, povezane z:

— znanimi kalibracijskimi parametri ob aktivaciji,

▼B

— prvo kalibracijo po njeni aktivaciji,

— njeno prvo kalibracijo v vozilu (kot ga identificira VIN), v katerem je nameščena zdaj,

— 20 najnovejšimi kalibracijami (če se na isti koledarski dan opravi več kalibracij, se shranijo le podatki za prvo in zadnjo kalibracijo v tem dnevu).

(120) Za vsako od teh kalibracij se zapišejo naslednji podatki:

— namen kalibracije (aktivacija, prva namestitev, namestitev, redni kontrolni pregled),

— ime in naslov servisne delavnice,

— številka kartice servisne delavnice, država izdajateljica in datum poteka veljavnosti kartice,

— identifikacija vozila,

— posodobljeni ali potrjeni parametri: w, k, l, velikosti pnevmatik, nastavitev naprave za omejevanje hitrosti, števec prevožene poti (stare in nove vrednosti), datum in čas (stare in nove vrednosti),

— vrste in identifikatorji vseh nameščenih pečatov.

(121) Poleg tega zapisovalna naprava v svoj pomnilnik podatkov zapiše in shrani svojo zmožnost uporabe tahografskih kartic prve generacije (ali je ta možnost še vedno aktivirana ali ne).

(122) Tipalo gibanja v svoj pomnilnik zapiše in shrani naslednje podatke o namestitvi tipala gibanja:

— prvo povezavo z VU (datum, čas, homologacijsko številko VU, serijsko številko VU),

— zadnjo povezavo z VU (datum, čas, homologacijsko številko VU, serijsko številko VU).

(123) Zunanja GNSS oprema v svoj pomnilnik zapiše in shrani naslednje podatke o namestitvi zunanje GNSS opreme:

— prvo povezavo z VU (datum, čas, homologacijsko številko VU, serijsko številko VU),

— zadnjo povezavo z VU (datum, čas, homologacijsko številko VU, serijsko številko VU).

3.12.11 *Podatki o nastavljanju časa*

(124) Zapisovalna naprava v svoj pomnilnik podatkov zapiše in shrani podatke, povezane z nastavljanji časa, opravljenimi v kalibracijskem načinu zunaj rednih kalibracij (opredelitev pojma f), in sicer:

— najnovejše nastavljanje časa,

— 5 največjih nastavljanj časa.

(125) Za vsako od teh nastavljanj časa se zapišejo naslednji podatki:

— datum in čas, stara vrednost,

— datum in čas, nova vrednost,

— ime in naslov servisne delavnice,

— številka kartice servisne delavnice, država izdajateljica, generacija in datum poteka veljavnosti kartice.

▼B

3.12.12 *Podatki o nadzornih dejavnostih*

(126) Zapisovalna naprava v svoj pomnilnik podatkov zapiše in shrani naslednje podatke, povezane z 20 najnovejšimi nadzornimi dejavnostmi:

— datum in čas nadzora,

— številko nadzorne kartice, državo izdajateljico in generacijo kartice,

— vrsto nadzora (prikazovanje in/ali tiskanje in/ali prenos podatkov iz VU in/ali prenos podatkov s kartice in/ali cestno preverjanje kalibracije).

(127) Pri prenosu podatkov se zapiše tudi prvi in zadnji dan obdobja, za katerega so podatki preneseni.

3.12.13 *Podatki o blokadah s strani podjetja*

(128) Zapisovalna naprava v svoj pomnilnik podatkov zapiše in shrani naslednje podatke, povezane z 255 najnovejšimi blokadami s strani podjetja:

— datum in čas vklopa blokade,

— datum in čas izklopa blokade,

— številko kartice podjetja, državo izdajateljico in generacijo kartice,

— ime in naslov podjetja.

Podatki, ki so bili prej blokirani z blokado, ki je bila zaradi zgoraj navedene omejitve odstranjena iz pomnilnika, se obravnavajo kot da niso blokirani.

3.12.14 *Podatki o prenosih podatkov*

(129) Zapisovalna naprava v načinu dela v podjetju ali v kalibracijskem načinu v svoj pomnilnik podatkov zapiše in shrani naslednje podatke, povezane z zadnjim prenosom podatkov iz pomnilnika podatkov na zunanje medije:

— datum in čas prenosa,

— številko kartice podjetja ali servisne delavnice, državo izdajateljico in generacijo kartice,

— ime podjetja ali servisne delavnice.

3.12.15 *Podatki o posebnih stanjih*

(130) Zapisovalna naprava v svoj pomnilnik podatkov zapiše in shrani naslednje podatke, povezane s posebnimi stanji:

— datum in čas vnosa,

— vrsto posebnega stanja.

(131) Zapisovalna naprava je zmožna hraniti podatke o posebnih stanjih najmanj 365 dni (ob predpostavki, da se povprečno odpre in zapre po eno posebno stanje na dan). Ko se pomnilnik zapolni s podatki, se novi podatki prepišejo čez najstarejše podatke.

3.12.16 *Podatki o tahografskih karticah*

(132) Zapisovalna naprava je zmožna zapisati in shraniti naslednje podatke, povezane z različnimi tahografskimi karticami, ki so bile uporabljene v enoti v vozilu:

— številko in serijsko številko tahografske kartice,

— proizvajalca tahografske kartice,

▼B

— vrsto tahografske kartice,

— različico kartografske kartice.

(133) Zapisovalna naprava je zmožna hraniti najmanj 88 takih zapisov.

3.13 **Branje s tahografskih kartic**

(134) Zapisovalna naprava je zmožna s tahografskih kartic prve in druge generacije, če je ustrezno, prebrati potrebne podatke za:

— identifikacijo vrste kartice, imetnika kartice, prej uporabljenega vozila, datuma in časa zadnjega izvleka kartice in takrat izbrane dejavnosti,

— preverjanje, ali je bila zadnja seja s kartico pravilno zaključena,

— izračun časa neprekinjene vožnje voznika, skupnega časa odmorov in skupnega časa vožnje v preteklem in tekočem tednu,

— tiskanje zahtevanih izpisov, ki se navezujejo na podatke, zapisane na vozniški kartici,

— prenos podatkov z vozniške kartice na zunanje medije.

Ta zahteva velja le za tahografske kartice prve generacije, če je servisna delavnica odpravila možnost njihove uporabe.

(135) V primeru napake pri branju zapisovalna naprava še do trikrat poskusi izvesti isti ukaz za branje, če vsi ti ponovni poskusi spodletijo, pa proglasi, da ima kartica napako in je neveljavna.

3.14 **Zapisovanje in shranjevanje podatkov na tahografske kartice**

3.14.1 *Zapisovanje in shranjevanje na tahografske kartice prve generacije*

(136) Pod pogojem, da servisna delavnica ni odpravila možnosti uporabe tahografskih kartic prve generacije, zapisovalna naprava zapiše in shrani podatke na točno tak način, kot bi to naredila zapisovalna naprava prve generacije.

(137) Zapisovalna naprava takoj po vstavitvi kartice nastavi „podatke o seji s kartico“ na vozniški kartici ali kartici servisne delavnice.

(138) Zapisovalna naprava posodobi podatke, shranjene na veljavni vozniški kartici, kartici servisne delavnice in/ali nadzorni kartici, z vsemi podatki, ki se navezujejo na obdobje, v katerem je kartica vstavljena, in ki zadevajo imetnika kartice. Podatki, shranjeni na teh karticah, so določeni v poglavju 4.

(139) Zapisovalna naprava posodobi podatke o voznikovih dejavnostih in krajih (kot je določeno v poglavjih 4.5.3.1.9 in 4.5.3.1.11), shranjene na vozniških karticah in/ali karticah servisnih delavnic, s podatki o dejavnostih in krajih, ki jih ročno vnese imetnik kartice.

(140) Dogodki, ki niso opredeljeni za zapisovalne naprave prve generacije, se ne shranjujejo na vozniške kartice in kartice servisnih delavnic.

▼B

(141) Posodabljanje podatkov na tahografskih karticah poteka tako, da se po potrebi in ob upoštevanju dejanske zmogljivosti pomnilnika kartice, najnovejši podatki zapišejo čez najstarejše podatke.

(142) V primeru napake pri zapisovanju zapisovalna naprava še do trikrat poskusi izvesti isti ukaz za zapisovanje, če vsi ti ponovni poskusi spodletijo, pa proglasi, da ima kartica napako in je neveljavna.

(143) Pred sprostitvijo vozniške kartice in po shranitvi vseh potrebnih podatkov nanjo zapisovalna naprava ponastavi „podatke o seji s kartico“.

3.14.2 *Zapisovanje in shranjevanje na tahografske kartice druge generacije*

(144) Tahografske kartice druge generacije vključujejo dve različni aplikaciji – prvo, ki je popolnoma enaka kot aplikacija TACHO na tahografskih karticah prve generacije, in drugo, aplikacijo „TACHO_G2“, kot je določena v poglavju 4 in Dodatku 2.

(145) Zapisovalna naprava takoj po vstavitvi kartice nastavi „podatke o seji s kartico“ na vozniški kartici ali kartici servisne delavnice.

(146) Zapisovalna naprava posodobi podatke, shranjene na obeh aplikacijah veljavne vozniške kartice, kartice servisne delavnice in/ali nadzorne kartice, z vsemi podatki, ki se navezujejo na obdobje, v katerem je kartica vstavljena, in ki zadevajo imetnika kartice. Podatki, shranjeni na teh karticah, so določeni v poglavju 4.

(147) Zapisovalna naprava posodobi podatke o krajih voznikovih dejavnosti in položajih (kot je določeno v poglavjih 4.5.3.1.9, 4.5.3.1.11, 4.5.3.2.9 in 4.5.3.2.11), shranjene na voznikih karticah in/ali karticah servisnih delavnic, s podatki o dejavnostih in krajih, ki jih ročno vnese imetnik kartice.

(148) Posodabljanje podatkov na tahografskih karticah poteka tako, da se po potrebi in ob upoštevanju dejanske zmogljivosti pomnilnika kartice, najnovejši podatki zapišejo čez najstarejše podatke.

(149) V primeru napake pri zapisovanju zapisovalna naprava še do trikrat poskusi izvesti isti ukaz za zapisovanje, če vsi ti ponovni poskusi spodletijo, pa proglasi, da ima kartica napako in je neveljavna.

(150) Pred sprostitvijo vozniške kartice in po shranitvi vseh potrebnih podatkov na obe aplikaciji kartice, zapisovalna naprava ponastavi „podatke o seji s kartico“.

3.15 **Prikazovanje**

(151) Prikazovalnik obsega najmanj 20 znakov.

(152) Znak na prikazovalniku je najmanj 5 mm visok in 3,5 mm širok.

(153) Prikazovalnik podpira znake, opredeljene v poglavju 4 Dodatka 1 „Nabori znakov“. Prikazovalnik lahko uporablja poenostavljene glife (npr. lahko so opuščeni znaki za naglase, male črke so lahko prikazane kot velike črke).

▼B

(154) Prikazovalnik je ustrezno osvetljen, vendar ne sme slepiti uporabnika.

(155) Prikazi so vidni zunaj zapisovalne naprave.

(156) Zapisovalna naprava je zmožna prikazovati:

— privzete podatke,

— podatke, povezane z opozorili,

— podatke, povezane z dostopom do menijev,

— druge podatke po zahtevah uporabnika.

Zapisovalna naprava lahko prikazuje tudi druge podatke, pod pogojem, da je te dodatne podatke mogoče jasno ločiti od zgoraj predpisanih podatkov.

(157) Prikazovalnik zapisovalne naprave uporablja piktograme ali kombinacije piktogramov, naštete v Dodatku 3. Prikazovalnik lahko podpira tudi dodatne piktograme ali kombinacije piktogramov, pod pogojem, da jih je mogoče jasno ločiti od zgoraj navedenih piktogramov ali kombinacij piktogramov.

(158) Med gibanjem vozila je prikazovalnik ves čas vključen.

(159) Zapisovalna naprava lahko samodejno izklopi ali omogoča ročni izklop prikazovalnika, kadar vozilo miruje.

Oblika prikaza je predpisana v Dodatku 5.

3.15.1 *Privzeti prikaz*

(160) Če ni potreben prikaz nobenih drugih podatkov, zapisovalna naprava po privzetem dogovoru prikazuje naslednje informacije:

— lokalni čas (seštevek časa UTC in zamika časa, ki ga je nastavil voznik),

— način delovanja,

— trenutno dejavnost voznika in trenutno dejavnost sovoznika,

— informacije v zvezi z voznikom:

— če je njegova trenutna dejavnost VOŽNJA, njegov trenutni čas neprekinjene vožnje in njegov trenutni skupni čas odmorov,

— če njegova trenutna dejavnost ni VOŽNJA, dosedanji čas te dejavnosti (od takrat, ko je to dejavnost izbral) in njegov trenutni skupni čas odmorov.

(161) Prikaz podatkov o vsakem od njiju (vozniku oz. sovozniku) je jasen, enostaven in nedvoumen. Če ni mogoče istočasno prikazovati informacij o vozniku in sovozniku, zapisovalna naprava po privzetem dogovoru prikazuje informacije, ki se navezujejo na voznika, in uporabniku omogoča tudi izbiro prikaza informacij o sovozniku.

(162) Če širina prikazovalnika po privzetem dogovoru ne omogoča prikaza načina delovanja, zapisovalna naprava za kratek čas prikaže novi način po vsaki spremembi načina.

▼B

(163) Zapisovalna naprava po vstavitvi kartice za kratek čas prikaže ime imetnika kartice.

(164) Kadar je odprto stanje „ZUNAJ PODROČJA UPORABE“ ali TRAJEKT/VLAK, mora privzeti prikaz kazati tudi ustrezni piktogram tega stanja (sprejemljivo je, da v tem primeru ni mogoče istočasno prikazovati tudi tekoče voznikove dejavnosti).

3.15.2 *Opozorilni prikaz*

(165) Zapisovalna naprava prikazuje opozorilne informacije predvsem s piktogrami, predpisanimi v Dodatku 3, po potrebi dopolnjenimi z dodatnimi številsko kodiranimi informacijami. Dodan je lahko tudi besedni opis opozorila v voznikovem izbranem jeziku.

3.15.3 *Dostop do menijev*

(166) Zapisovalna naprava zagotavlja potrebne ukaze za premikanje skozi sestav menijev.

3.15.4 *Drugi prikazi*

(167) Na zahtevo je možno izbrati naslednje prikaze:

— datum in čas UTC ter zamik lokalnega časa,

— vsebino katerega koli od šestih tiskanih izpisov v enaki obliki, kakršno imajo sami izpisi,

— čas neprekinjene vožnje in skupni čas odmorov voznika,

— čas neprekinjene vožnje in skupni čas odmorov sovoznika,

— skupni čas vožnje voznika v prejšnjem in tekočem tednu,

— skupni čas vožnje sovoznika v prejšnjem in tekočem tednu;

neobvezno:

— dosedanji čas sovoznikove dejavnosti (od takrat, ko je to dejavnost izbral),

— skupni čas vožnje voznika v tekočem tednu,

— skupni čas vožnje sovoznika v tekoči dnevni delovni izmeni,

— skupni čas vožnje voznika v tekoči dnevni delovni izmeni.

(168) Prikaz vsebine tiskanih izpisov je zaporeden, po vrsticah. Če je širina prikazovalnika manjša od 24 znakov, se uporabniku zagotovi popolna informacija z ustrezno rešitvijo (prikaz v več vrsticah, drsno premikanje …).

Vrstice tiskanega izpisa, namenjene ročnemu vpisu podatkov, so lahko na prikazovalniku izpuščene.

▼B

3.16 **Tiskanje**

(169) Zapisovalna naprava je zmožna tiskati informacije iz svojega pomnilnika podatkov in/ali tahografskih kartic v naslednjih sedmih oblikah izpisov:

— dnevni izpis voznikovih dejavnosti s kartice,

— dnevni izpis voznikovih dejavnosti iz enote v vozilu,

— izpis dogodkov in napak s kartice,

— izpis dogodkov in napak iz enote v vozilu,

— izpis tehničnih podatkov,

— izpis prekoračenj hitrosti,

— zgodovina podatkov na tahografski kartici za zadevno enoto v vozilu (glej poglavje 3.12.16).

Oblika in vsebina teh izpisov je podrobno določena v Dodatku 4.

Na koncu izpisov so lahko vključeni še dodatni podatki.

Zapisovalna naprava lahko omogoča še druge izpise, če jih je mogoče jasno ločiti od zgoraj navedenih sedmih izpisov.

(170) „Dnevni izpis voznikovih dejavnosti s kartice“ in „izpis dogodkov in napak s kartice“ sta mogoča le, kadar je v zapisovalno napravo vstavljena vozniška kartica ali kartica servisne delavnice. Pred začetkom tiskanja zapisovalna naprava posodobi podatke, shranjene na zadevni kartici.

(171) Za izvedbo „dnevnega izpisa voznikovih dejavnosti s kartice“ ali „izpisa dogodkov in napak s kartice“ zapisovalna naprava:

— samodejno izbere vozniško kartico ali kartico servisne delavnice, če je vstavljena samo ena od teh kartic, ali

— omogoči izbiro izvorne kartice z ustreznim ukazom ali izbere kartico v voznikovi reži, če sta v zapisovalno napravo vstavljeni dve taki kartici.

(172) Tiskalnik omogoča tiskanje 24 znakov v vrstici.

(173) Znak na prikazovalniku je najmanj 2,1 mm visok in 1,5 mm širok.

(174) Tiskalnik podpira znake, opredeljene v poglavju 4 Dodatka 1 „Nabori znakov“.

(175) Tiskalniki imajo zadostno ločljivost, da je mogoče nedvoumno branje izpisov.

(176) Izpisi morajo pri normalni vlažnosti (10–90 %) in temperaturi ohraniti svoje mere in zapis.

(177) Homologirani papir za zapisovalno napravo ima ustrezno homologacijsko oznako in oznake vrst zapisovalnih naprav, za katere je namenjen.

▼B

(178) V normalnih pogojih hranjenja (glede osvetlitve, vlažnosti in temperature) izpisi ostanejo jasno berljivi in prepoznavni vsaj dve leti.

(179) Izpisi so skladni najmanj s preskusnimi specifikacijami iz Dodatka 9.

(180) Prav tako je tem dokumentom mogoče dodati z roko napisane dopise, kot je podpis voznika.

(181) Ko uporabnik vstavi nov papir, zapisovalna naprava nadaljuje tiskanje od začetka izpisa ali pa nadaljuje tiskanje od tam, kjer je bilo prekinjeno, pri čemer nedvoumno označi, na kateri prej natisnjeni del se nadaljevanje navezuje.

3.17 **Opozorila**

(182) Zapisovalna naprava voznika opozori, kakor hitro zazna dogodek in/ali napako.

(183) Opozorilo na izpad napajanja je lahko naknadno, po ponovni vzpostavitvi napajanja.

(184) Zapisovalna naprava na presežen najdaljši dovoljeni čas neprekinjene vožnje voznika opozori 15 minut vnaprej in v trenutku, ko ta dogodek nastopi.

(185) Opozorilo je vizualno. Vizualno opozorilo je lahko dopolnjeno tudi z zvočnim opozorilom.

(186) Vizualna opozorila so taka, da jih uporabnik jasno zazna, so znotraj voznikovega vidnega polja ter so jasno berljiva podnevi in ponoči.

(187) Prikazovalnik vizualnih opozoril je lahko vgrajen v zapisovalni napravi in/ali nameščen posebej.

(188) Če je nameščen posebej, je označen s simbolom „T“.

(189) Opozorila trajajo najmanj 30 sekund, če jih uporabnik vmes ne potrdi s pritiskom na določeno tipko ali kombinacijo tipk na zapisovalni napravi. Ta prva potrditev ne zbriše prikaza vzroka opozorila, navedenega v naslednjem odstavku.

(190) Vzrok opozorila se prikaže na zapisovalni napravi in ostane viden, dokler ga uporabnik ne potrdi s pritiskom na določeno tipko na zapisovalni napravi ali ukazom.

(191) Dodatna opozorila so dovoljena, če jih voznik ne more zamenjati z zgoraj opredeljenimi opozorili.

3.18 **Prenos podatkov na zunanje medije**

(192) Zapisovalna naprava je zmožna na zahtevo prenašati podatke iz svojega pomnilnika ali z vozniške kartice na zunanji pomnilniški medij preko priključka za kalibracijo/prenos podatkov. Pred začetkom prenosa zapisovalna naprava posodobi podatke, shranjene na zadevni kartici.

▼B

(193) Poleg tega lahko kot neobvezno funkcijo zapisovalna naprava v katerem koli načinu delovanja omogoča prenos podatkov tudi preko drugega priključka podjetju, ki se avtenticira na tem kanalu. Za tak prenos se uporabljajo dostopne pravice, ki veljajo v načinu dela v podjetju.

(194) Pri prenosu se noben shranjeni podatek ne spremeni ali izbriše.

(195) Električni vmesnik priključka za kalibracijo/prenos podatkov je predpisan v Dodatku 6.

(196) Protokoli za prenos podatkov so predpisani v Dodatku 7.

3.19 **Komunikacija na daljavo za namen usmerjenega cestnega nadzora**

(197) Ko je električni kontakt vozila vključen, enota v vozilu vsakih 60 sekund v opremo za komunikacijo na daljavo shrani najnovejše podatke, potrebne za namen usmerjenega cestnega nadzora. Takšni podatki so šifrirani in podpisani, kot je predpisano v Dodatku 11 in Dodatku 14.

(198) Podatki, ki se preverjajo na daljavo, so bralnikom komunikacij na daljavo na voljo z brezžičnim komuniciranjem, kot je predpisano v Dodatku 14.

(199) Podatki, potrebni za usmerjeni cestni nadzor, se navezujejo na:

— zadnji poskus kršenja varnosti,

— najdaljši izpad napajanja,

— napako na tipalu,

— napako v podatkih o gibanju,

— navzkrižje v gibanju vozila,

— vožnjo brez veljavne kartice,

— vstavitev kartice med vožnjo,

— podatke o nastavljanju časa,

— podatke o kalibraciji, vključno z datumoma dveh najnovejših shranjenih kalibracij,

— registrsko številka vozila,

— hitrost, ki jo zapiše tahograf.

3.20 **Iznos podatkov na dodatne zunanje naprave**

(200) Zapisovalne naprave so lahko opremljene tudi s standardiziranimi vmesniki, ki v delovnem ali kalibracijskem načinu omogočajo uporabo podatkov, ki jih je zapisal ali pripravil tahograf, z zunanjo opremo.

Neobvezni vmesnik z ITS je predpisan in standardiziran v Dodatku 13. Vzporedno s tem lahko delujejo tudi drugi podobni vmesniki, pod pogojem, da v celoti izpolnjujejo zahteve iz Dodatka 13 glede obveznih podatkov, varnosti in voznikove privolitve.

Za podatke ITS, ki so na voljo prek navedenega vmesnika, veljajo naslednje zahteve:

— ti podatki so niz izbranih obstoječih podatkov iz slovarja podatkov tahografa (Dodatek 1),

▼B

— podniz teh izbranih podatkov je označen kot „osebni podatki“,

— podniz „osebni podatki“ je na voljo samo, če je aktivirano preverljivo soglasje voznika, da njegovi osebni podatki lahko zapustijo omrežje vozila,

— privolitev voznika je možno kadar koli aktivirati ali deaktivirati z ukazi v meniju, pod pogojem, da je vstavljena vozniška kartica,

— niz in podniz podatkov se preneseta prek brezžičnega protokola Bluetooth v polmeru voznikove kabine, s hitrostjo osveževanja ene minute,

— povezava zunanje naprave z vmesnikom z ITS se zaščiti z namensko in naključno določeno kodo PIN, sestavljeno iz vsaj 4 števk, ki je zapisana in posredovana preko prikazovalnika vsake od enot v vozilu,

— prisotnost vmesnika z ITS v nobenem primeru ne sme motiti ali vplivati na pravilno delovanje in varnost enote v vozilu.

Poleg niza izbranih obstoječih podatkov, ki štejejo za minimalni seznam, se lahko iznesejo tudi drugi podatki, pod pogojem, da ne štejejo za osebne podatke.

Zapisovalna naprava obvesti drugo zunanjo opremo o voznikovi privolitvi.

Ko je električni kontakt vozila vključen, se ti podatki oddajajo ves čas.

(201) Tahografi so lahko še naprej opremljeni z vmesnikom serijske povezave, kot je predpisan v Prilogi 1B k Uredbi Sveta (EGS) št. 3821/85, kot je bila nazadnje spremenjena, da se zagotovi združljivost s starejšo opremo. Kljub temu je v primeru, da se prenašajo osebni podatki, potrebno voznikovo soglasje.

3.21 **Kalibracija**

(202) Funkcija kalibracije omogoča:

— samodejno povezavo tipala gibanja in VU,

— samodejno povezavo zunanje GNSS opreme z VU, če je ustrezno,

— digitalno prilagoditev konstante zapisovalne naprave (k) značilnemu koeficientu vozila (w),

— nastavitev tekočega časa v okviru obdobja veljavnosti vstavljene kartice servisne delavnice,

— nastavitev tekoče vrednosti števca prevožene poti,

— posodobitev identifikacijskih podatkov tipala gibanja, shranjenih v pomnilniku podatkov,

— če je ustrezno, posodobitev identifikacijskih podatkov zunanje GNSS opreme, shranjenih v pomnilniku podatkov,

▼B

— posodobitev vrst in identifikatorjev vseh nameščenih pečatov,

— posodobitev ali potrditev drugih parametrov, poznanih zapisovalni napravi: identifikacije vozila, w, l, mere pnevmatik in nastavitve naprave za omejevanje hitrosti, če je ustrezno.

(203) Poleg tega funkcija kalibracije omogoča odpravo možnosti uporabe tahografskih kartic prve generacije v zapisovalni napravi, če so izpolnjeni pogoji iz Dodatka 15.

(204) Povezovanje tipala gibanja z VU obsega najmanj:

— posodobitev namestitvenih podatkov tipala gibanja, ki jih hrani tipalo gibanja (po potrebi),

— kopiranje potrebnih identifikacijskih podatkov tipala gibanja iz tipala gibanja v pomnilnik podatkov VU.

(205) Povezovanje zunanje GNSS opreme z VU obsega najmanj:

— posodobitev namestitvenih podatkov zunanje GNSS opreme, ki jih hrani zunanja GNSS oprema (po potrebi),

— kopiranje potrebnih identifikacijskih podatkov zunanje GNSS opreme, vključno z njeno serijsko številko, iz zunanje GNSS opreme v pomnilnik podatkov VU.

Povezovanju sledi preverjanje GNSS informacij o položaju.

(206) Funkcija kalibracije podpira vnos potrebnih podatkov prek priključka za kalibracijo/prenos podatkov v skladu s kalibracijskim protokolom, opredeljenim v Dodatku 8. Funkcija kalibracije lahko vnos podatkov omogoča tudi prek drugih priključkov.

3.22 **Cestno preverjanje kalibracije**

(207) Funkcija cestnega preverjanja kalibracije omogoča odčitanje serijske številke tipala gibanja (ki je lahko zapisano v pretvorniku) ali zunanje GNSS opreme (če je ustrezno), ki je v času zahtevka priključen(a) na enoto v vozilu.

(208) Te podatke je mogoče prebrati najmanj na prikazovalniku enote v vozilu s pomočjo ukazov v menijih.

(209) Funkcija cestnega preverjanja kalibracije omogoča tudi izbiro V/I načina kalibracijske V/I signalne linije, kot je določeno v Dodatku 6, prek vmesnika linije K. To se opravi s funkcijo ECUAdjustmentSession, kot je določena v oddelku 7 Dodatka 8 „Upravljanje preskusnih impulzov – funkcionalna enota za upravljanje vhodov/izhodov“.

3.23 **Nastavljanje časa**

(210) Funkcija nastavljanja časa omogoča samodejno nastavljanje trenutnega časa. Zapisovalna oprema za nastavljanje časa uporablja dva vira: notranjo uro VU in GNSS sprejemnik.

▼B

(211) Nastavitev časa notranje ure VU se opravlja samodejno, v največ 12-urnih presledkih. Če po preteku tega roka GNSS signal ni na voljo, se nastavitev opravi takoj, ko VU dobi dostop do veljavnega časa, ki ga posreduje GNSS sprejemnik, v skladu s stanjem električnega kontakta vozila. Referenčni čas za samodejno nastavljanje časa na notranji uri VU se izpelje na podlagi podatka iz GNSS sprejemnika. Če trenutni čas od informacije o času, ki jo posreduje GNSS sprejemnik, odstopa za več kot eno (1) minuto, se sproži dogodek „časovno navzkrižje“.

(212) Funkcija nastavljanja časa omogoča tudi namensko nastavljanje trenutnega časa v kalibracijskem načinu.

3.24 **Delovne karakteristike**

(213) Enota v vozilu in zunanja GNSS oprema sta v celoti funkcionalni v temperaturnem območju od – 20 °C do 70 °C, tipalo gibanja pa v temperaturnem območju od – 40 °C do 135 °C. Vsebina pomnilnika podatkov se ohrani pri temperaturah do – 40 °C.

(214) Tahograf je v celoti funkcionalen v območju vlažnosti od 10 % do 90 %.

(215) Pečati, ki se uporabljajo v pametnih tahografih, vzdržijo enake pogoje kot tisti, ki veljajo za dele tahografa, na katere so nameščeni.

(216) Zapisovalna naprava je zaščitena pred prenapetostjo, zamenjavo polarnosti napajanja in kratkimi stiki.

(217) Tipala gibanja:

— bodisi reagirajo na magnetna polja, ki motijo zaznavanje gibanja vozila. V takšnih okoliščinah enota v vozilu zapiše in shrani napako na tipalu (zahteva 88);

— bodisi imajo tipalni element, ki je zaščiten pred magnetnimi polji ali je zanje neobčutljiv.

(218) Zapisovalna naprava in zunanja GNSS oprema sta skladni z mednarodnim predpisom UN ECE R10 in sta zaščiteni pred elektrostatičnimi razelektritvami in prehodnimi pojavi.

3.25 **Materiali**

(219) Vsi sestavni deli zapisovalne naprave so izdelani iz ustrezno obstojnih in mehansko trdnih materialov s stabilnimi električnimi in magnetnimi lastnostmi.

(220) Vsi notranji deli opreme so v normalnih pogojih uporabe zaščiteni pred vlago in prahom.

(221) Enota v vozilu in zunanja GNSS naprava imata stopnjo zaščite IP 40, tipalo gibanja pa stopnjo zaščite IP 64 po standardu IEC 60529:1989, vključno z A1:1999 in A2:2013.

(222) Zapisovalna naprava je skladna z ustreznimi tehničnimi specifikacijami glede ergonomije.

▼B

(223) Zapisovalna naprava je zaščitena pred nenamernimi poškodbami.

3.26 **Oznake**

(224) Če zapisovalna naprava prikazuje vrednost števca prevožene poti in hitrost vozila, se na prikazovalniku izpišejo naslednji podatki:

— poleg prikazane vrednosti prevožene poti je zapisana enota za merjenje razdalje „km“,

— poleg prikazane vrednosti hitrosti je oznaka „km/h“.

Zapisovalna naprava lahko omogoča tudi preklop na prikaz hitrosti v miljah na uro; pri takem prikazu je poleg vrednosti hitrosti enota za merjenje hitrosti „mph“. Zapisovalna naprava lahko omogoča tudi preklop na prikaz prevožene poti v miljah; pri takem prikazu je poleg vrednosti razdalje enota za merjenje razdalje „mi“.

(225) Na vsako samostojno nameščeno enoto zapisovalne naprave je pritrjena označevalna ploščica z naslednjimi podatki:

— ime in naslov proizvajalca opreme,

— proizvajalčeva kataloška številka in leto proizvodnje,

— serijska številka opreme,

— homologacijska oznaka za vrsto opreme.

(226) Če prostor fizično ne omogoča prikaza vseh zgoraj omenjenih podatkov, označevalna ploščica prikazuje vsaj: proizvajalčevo ime ali logotip in kataloško številko dela opreme.

4 ZAHTEVE GLEDE KONSTRUKCIJE IN FUNKCIONALNE ZAHTEVE ZA TAHOGRAFSKE KARTICE

4.1 **Vidni podatki**

Prednja stran vsebuje:

(227) besedi(-e) „vozniška kartica“ ali „nadzorna kartica“ ali „kartica servisne delavnice“ ali „kartica podjetja“ glede na vrsto kartice, natisnjeni(-e) z velikimi tiskanimi črkami v uradnem jeziku države izdajateljice kartice.

(228) ime države članice, ki je kartico izdala (neobvezno).

(229) oznako države članice, ki je kartico izdala, natisnjeno v negativu v modrem pravokotniku in obkroženo z 12 rumenimi zvezdami. Oznake so naslednje:

B	Belgija	LV	Latvija
BG	Bolgarija	L	Luksemburg
CZ	Češka	LT	Litva
CY	Ciper	M	Malta
DK	Danska	NL	Nizozemska
D	Nemčija	A	Avstrija
EST	Estonija	PL	Poljska

▼B

GR	Grčija	P RO SK SLO	Portugalska Romunija Slovaška Slovenija
E	Španija	FIN	Finska
F HR H	Francija Hrvaška Madžarska	S	Švedska
IRL	Irska	UK	Združeno kraljestvo
I	Italija		

(230) podatke, posebej značilne za izdano kartico, oštevilčene, kot je prikazano spodaj:

	Vozniška kartica	Nadzorna kartica	Kartica podjetja ali servisne delavnice
1.	priimek voznika	ime nadzornega organa	ime podjetja ali servisne delavnice
2.	ime(-na) voznika	priimek inšpektorja (če je ustrezno)	priimek imetnika kartice (če je ustrezno)
3.	rojstni datum voznika	ime(-na) inšpektorja (če je ustrezno)	ime(-na) imetnika kartice (če je ustrezno)
4.a	datum začetka veljavnosti kartice		
4.b	datum izteka veljavnosti kartice		
4.c	ime organa, ki je kartico izdal (lahko je natisnjeno na hrbtni strani)		
4.d	drugačna številka od tiste pod številko 5 za upravne namene (neobvezno)		
5.a	številka vozniškega dovoljenja (na datum izdaje vozniške kartice)	—	—
5.b	številka kartice		
6.	fotografija voznika	fotografija inšpektorja (neobvezno)	fotografija izvajalca namestitve (neobvezno)
7.	podpis imetnika (neobvezno)		
8.	običajno prebivališče ali poštni naslov imetnika (neobvezno)	poštni naslov nadzornega organa	poštni naslov podjetja ali servisne delavnice

(231) datumi se zapišejo v obliki „dd/mm/llll“ ali „dd.mm.llll“ (dan, mesec, leto).

Hrbtna stran vsebuje:

(232) razlago za oštevilčene navedbe na prednji strani kartice;

▼B

(233) z izrecnim pisnim soglasjem imetnika se lahko dodajo tudi informacije, ki niso povezane z upravljanjem kartice, navedba takšnih podatkov pa na noben način ne vpliva na uporabo modela kot tahografske kartice.

(234) Tahografske kartice so natisnjene na ozadjih z naslednjimi prevladujočimi barvami:

— vozniška kartica: bela,

— nadzorna kartica: modra,

— kartica servisne delavnice: rdeča,

— kartica podjetja: rumena.

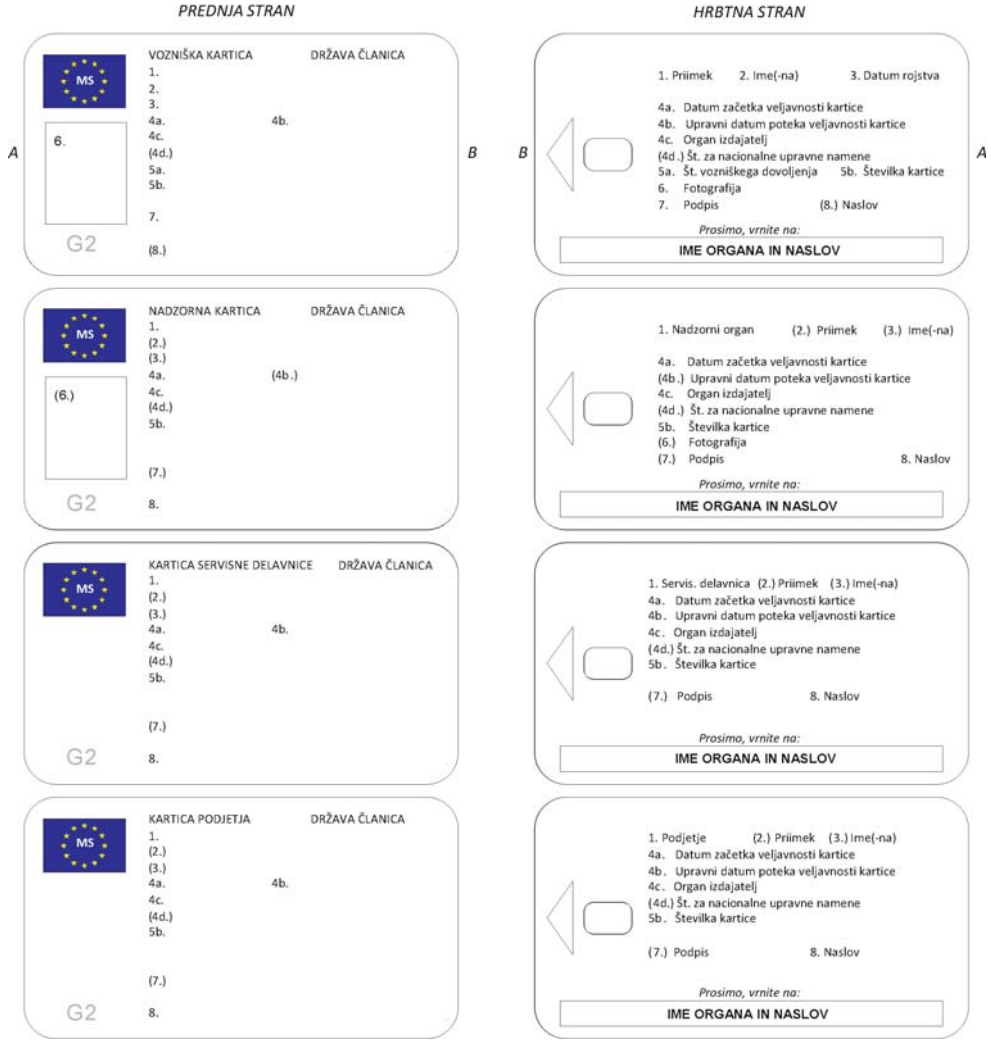
(235) Telo tahografske kartice je zaščiteno pred ponarejanjem in nepooblaščenimi posegi vsaj z naslednjimi zaščitami:

— varnostni vzorec ozadja s finimi giljošami in mavričnim tiskom,

— v območju fotografije se varnostni vzorec ozadja in fotografija prekrivata,

— vsaj ena dvobarvna črta v mikrotisku.

TAHOGRAFSKE KARTICE, KI USTREZAJO VZORCU SKUPNOSTI



▼B

(236) Po posvetu s Komisijo lahko država članica brez poseganja v druge določbe te priloge uporabi dodatne barve ali oznake, npr. nacionalne simbole in elemente zaščite.

(237) Začasne kartice iz člena 26(4) Uredbe (EU) št. 165/2014 so skladne z določbami iz te priloge.

4.2 **Varnost**

Cilji varnosti sistema so zaščita celovitosti in avtentičnosti podatkov, izmenjanih med karticami in zapisovalno napravo, zaščita celovitosti in avtentičnosti podatkov, prenesenih s kartic, s tem, da se dovoljuje določene operacije pisanja na kartice samo zapisovalni napravi, dešifriranje nekaterih podatkov, izključitev vsake možnosti ponarejanja podatkov, shranjenih na karticah, preprečitev nepooblaščenih posegov in zaznavanje kakršnega koli poskusa takega posega.

(238) Za zagotovitev varnosti sistema tahografske kartice izpolnjujejo varnostne zahteve, opredeljene v dodatkih 10 in 11.

(239) Tahografske kartice so berljive z drugo opremo, npr. osebnimi računalniki.

4.3 **Standardi**

(240) Tahografske kartice so skladne z naslednjimi standardi:

— ISO/IEC 7810 Identifikacijski dokumenti – Fizične lastnosti,

— ISO/IEC 7816 Identifikacijski dokumenti – Kartice z integriranim vezjem:

  — 1. del: Fizične lastnosti

  — 2. del: Mere in položaj kontaktov (ISO/IEC 7816-2:2007),

  — 3. del: Električni vmesnik in protokoli prenosa (ISO/IEC 7816-3:2006),

  — 4. del: Organizacija, varovanje in ukazi za izmenjavo (ISO/IEC 7816-4:2013 + Cor. 1:2014),

  — 6. del: Panožni podatkovni elementi za izmenjavo (ISO/IEC 7816-6:2004 + Cor. 1:2006),

  — 8. del: Ukazi za varnostne operacije (ISO/IEC 7816-8:2004).

— Tahografske kartice se testirajo v skladu s standardom ISO/IEC 10373-3:2010 Identifikacijski dokumenti – Preskusne metode – 3. del: Kartice z integriranim vezjem s kontakti in povezane vmesniške naprave.

4.4 **Okoljske in električne specifikacije**

(241) Tahografske kartice so zmožne pravilno delovati v vseh podnebnih pogojih, ki jih običajno lahko srečamo na ozemlju Skupnosti, in najmanj v temperaturnem območju od – 25 °C do + 70 °C z občasnimi temperaturnimi konicami do + 85 °C, pri čemer „občasno“ pomeni ne več kot 4 ure hkrati in skupaj ne več kot stokrat v dobi uporabe kartice.

(242) Kartice so zmožne pravilno delovati v območju vlažnosti od 10 % do 90 %.

▼B

(243) Tahografske kartice so ob uporabi v okviru predpisanih okoljskih in električnih specifikacij zmožne pravilno delovati pet let.

(244) Tahografske kartice so med delovanjem skladne s predpisom ECE R10 o elektromagnetni združljivosti in so zaščitene pred elektrostatičnimi razelektritvami.

4.5 **Hranjenje podatkov**

Za namen tega odstavka velja naslednje:

— časi so zapisani z ločljivostjo ene minute, če ni predpisano drugače;

— vrednosti števca prevožene poti so zapisane z ločljivostjo enega kilometra;

— hitrosti so zapisane z ločljivostjo 1 km/h;

— položaji (zemljepisne širine in dolžine) so zapisani v stopinjah in minutah, in sicer z ločljivostjo 1/10 minute.

Funkcije, ukazi in logične strukture tahografskih kartic, s katerimi se izpolnijo zahteve glede hranjenja podatkov, so predpisani v Dodatku 2.

Če ni določeno drugače, je hranjenje podatkov na tahografskih karticah organizirano tako, da v primeru, ko bi bila ob zapisu določenih podatkov presežena predvidena velikost pomnilnika, novi podatki nadomestijo najstarejše shranjene podatke.

(245) Ta člen določa minimalne zmogljivosti pomnilnika kartice za različne aplikativne podatkovne datoteke. Tahografske kartice so zmožne zapisovalni napravi posredovati podatke o dejanskih zmogljivostih teh podatkovnih datotek.

(246) Vsi dodatni podatki, ki so lahko shranjeni na tahografski kartici, v zvezi z drugimi aplikacijami, s katerimi je kartica lahko povezana, se hranijo v skladu z Direktivo 95/46/ES, Direktivo 2002/58/ES Evropskega parlamenta in Sveta ter členom 7 Uredbe (EU) št. 165/2014.

(247) Vsaka glavna datoteka (MF) vsake tahografske kartice vsebuje do pet elementarnih datotek (EF) za upravljanje kartice in identifikacijo aplikacij in čipov ter dve namenski datoteki:

— DF Tachograph, ki vsebuje aplikacijo, dostopno enotam v vozilu prve generacije, vsebujejo pa jo tudi tahografske kartice prve generacije,

— DF Tachograph_G2, ki vsebuje aplikacijo, dostopno samo enotam v vozilu druge generacije, vsebujejo pa jo samo tahografske kartice prve generacije.

Podrobnosti strukture tahografskih kartic so v celoti opredeljene v Dodatku 2.

4.5.1 *Elementarne datoteke za identifikacijo in upravljanje kartic*

4.5.2 *Identifikacija kartice z integriranim vezjem*

(248) Tahografske kartice so zmožne hraniti naslednje identifikacijske podatke pametne kartice:

— zaustavitev notranje ure,

▼B

— serijsko številko kartice (vključno s proizvodnimi podatki),

— homologacijsko številko kartice,

— identifikacijo (ID) personalizatorja kartice,

— identifikacijo (ID) vgraditelja čipa,

— identifikator integriranega vezja (IC).

4.5.2.1 Identifikacija čipa

(249) Tahografske kartice so zmožne hraniti naslednje identifikacijske podatke integriranega vezja (IC):

— serijsko številko IC,

— proizvodne podatke IC.

4.5.2.2 DIR (samo v tahografskih karticah druge generacije)

(250) Tahografska kartica je zmožna hraniti podatkovne objekte za identifikacijo aplikacij iz Dodatka 2.

4.5.2.3 Informacija ATR (pogojno, samo v tahografskih karticah druge generacije)

(251) Tahografske kartice so zmožne hraniti naslednji podaljšani podatkovni objekt:

— če tahografska kartica podpira podaljšana podatkovna polja, podaljšani podatkovni objekt, kot je določen v Dodatku 2.

4.5.2.4 Podaljšana informacija (pogojno, samo v tahografskih karticah druge generacije)

(252) Tahografske kartice so zmožne hraniti naslednje podaljšane podatkovne objekte:

— če tahografska kartica podpira podaljšana podatkovna polja, podaljšane podatkovne objekte, kot so določeni v Dodatku 2.

4.5.3 *Vozniška kartica*

4.5.3.1 Tahografska aplikacija (dostopna enotam v vozilu prve in druge generacije)

4.5.3.1.1 Identifikacija aplikacije

(253) Vozniška kartica je zmožna hraniti naslednje identifikacijske podatke aplikacije:

— identifikacijo tahografske aplikacije,

— vrsto identifikacije tahografske kartice.

4.5.3.1.2 Ključi in certifikati

(254) Vozniška kartica je zmožna hraniti več različnih kriptografskih ključev in certifikatov, kot je določeno v delu A Dodatka 11.

▼B

4.5.3.1.3 Identifikacija kartice

(255) Vozniška kartica je zmožna hraniti naslednje identifikacijske podatke kartice:

— številko kartice,

— državo izdajateljico, ime organa izdajatelja, datum izdaje,

— datum začetka veljavnosti kartice, datum poteka veljavnosti kartice.

4.5.3.1.4 Identifikacija imetnika kartice

(256) Vozniška kartica je zmožna hraniti naslednje identifikacijske podatke imetnika kartice:

— priimek imetnika kartice,

— ime(-na) imetnika kartice,

— datum rojstva,

— izbrani jezik.

4.5.3.1.5 Prenos podatkov s kartice

(257) Vozniška kartica je zmožna hraniti naslednje podatke o prenosih podatkov s kartice:

— datum in čas zadnjega prenosa podatkov s kartice (za druge namene kot nadzor).

(258) Vozniška kartica je zmožna hraniti en tak zapis.

4.5.3.1.6 Podatki o vozniškem dovoljenju

(259) Vozniška kartica je zmožna hraniti naslednje podatke o vozniškem dovoljenju:

— državo izdajateljico, ime organa izdajatelja,

— številko vozniškega dovoljenja (na dan izdaje kartice).

4.5.3.1.7 Podatki o dogodkih

Za namen tega pododstavka velja, da se čas shranjuje z ločljivostjo 1 sekunde.

(260) Vozniška kartica je zmožna hraniti podatke, povezane z naslednjimi dogodki, ki jih zazna zapisovalna naprava v času, ko je kartica vstavljena:

— časovno prekrivanje (kjer je vzrok dogodka ta kartica),

— vstavitev kartice med vožnjo (kjer pri dogodku nastopa ta kartica),

— zadnja seja s kartico nepravilno zaključena (kjer pri dogodku nastopa ta kartica),

— izpad napajanja,

— napaka v podatkih o gibanju,

— poskusi kršenja varnosti.

(261) Vozniška kartica je zmožna hraniti naslednje podatke o teh dogodkih:

— kodo dogodka,

— datum in čas začetka dogodka (ali vstavitve kartice, če je dogodek ob tem času že v teku),

▼B

— datum in čas konca dogodka (ali izvleka kartice, če je dogodek ob tem času že v teku),

— registrsko številko vozila, v katerem je dogodek nastopil, in državo, v kateri je vozilo registrirano.

Opomba: pri dogodku „časovno prekrivanje“:

— datum in čas začetka dogodka pomeni datum in čas izvleka kartice iz prejšnjega vozila,

— datum in čas konca dogodka pomeni datum in čas vstavitve kartice v trenutno vozilo,

— podatki o vozilu se nanašajo na trenutno vozilo, v katerem je dogodek nastopil.

Opomba: Pri dogodku „zadnja seja s kartico nepravilno zaključena“:

— datum in čas začetka dogodka sta datum in čas vstavitve kartice pri seji, ki ni bila pravilno zaključena,

— datum in čas konca dogodka sta datum in čas vstavitve kartice pri seji, v kateri je bil dogodek zaznan (tj. trenutni seji),

— podatki o vozilu se nanašajo na vozilo, v katerem seja ni bila pravilno zaključena.

(262) Vozniška kartica je zmožna hraniti podatke o šestih najnovejših dogodkih vsake vrste (tj. skupaj 36 dogodkih).

4.5.3.1.8 Podatki o napakah

Za namen tega pododstavka velja, da se čas zapisuje z ločljivostjo 1 sekunde.

(263) Vozniška kartica je zmožna hraniti podatke, povezane z naslednjimi napakami, ki jih zazna zapisovalna naprava v času, ko je kartica vstavljena:

— napaka kartice (kjer pri dogodku nastopa ta kartica),

— napaka na zapisovalni napravi.

(264) Vozniška kartica je zmožna hraniti naslednje podatke o teh napakah:

— kodo napake,

— datum in čas začetka napake (ali vstavitve kartice, če je napaka ob tem času že v teku),

— datum in čas konca napake (ali izvleka kartice, če je napaka ob tem času že v teku),

— registrsko številko vozila, v katerem se je napaka zgodila, in državo, v kateri je vozilo registrirano.

(265) Vozniška kartica je zmožna hraniti podatke o dvanajstih najnovejših napakah vsake vrste (tj. skupaj 24 napakah).

▼B

4.5.3.1.9 Podatki o voznikovih dejavnostih

(266) Vozniška kartica je za vsak koledarski dan, na katerega je bila kartica uporabljena ali za katerega je voznik dejavnosti vnesel ročno, zmožna hraniti naslednje podatke:

— datum,

— števec dni prisotnosti (ki se poveča za eno ob vsakem takem novem koledarskem dnevu),

— celotno dolžino poti, ki jo je voznik prevozil na ta dan,

— stanje voznika ob 00.00,

— ob vsaki voznikovi spremembi dejavnosti in/ali spremembi stanja vožnje in/ali ob vsaki vstavitvi/izvleku kartice:

— stanje vožnje (POSADKA, POSAMEZNIK),

— režo (VOZNIK, SOVOZNIK),

— stanje kartice (VSTAVLJENA, NI VSTAVLJENA),

— dejavnost (VOŽNJA, RAZPOLOŽLJIVOST, DELO, ODMOR/POČITEK),

— čas spremembe.

(267) Pomnilnik podatkov na vozniški kartici je zmožen hraniti podatke o voznikovih dejavnostih najmanj 28 dni (povprečna voznikova dejavnost je opredeljena kot 93 sprememb dejavnosti na dan).

(268) Podatki iz zahtev 261, 264 in 266 so shranjeni tako, da je mogoče poizvedovanje po dejavnostih iz pomnilnika v zaporedju njihovih nastopov, tudi v primerih časovnih prekrivanj.

4.5.3.1.10 Podatki o uporabljenih vozilih

(269) Vozniška kartica je za vsak koledarski dan, na katerega je bila uporabljena, in za vsako obdobje uporabe določenega vozila na ta dan (obdobje uporabe vključuje vse cikle vstavitve/izvleka kartice v vozilu z vidika kartice), zmožna hraniti naslednje podatke:

— datum in čas prve uporabe vozila (tj. prve vstavitve kartice v tem obdobju uporabe vozila ali čas 00.00, če je ob tem času uporaba vozila že v teku),

— vrednost števca prevožene poti ob tem času,

— datum in čas zadnje uporabe vozila (tj. zadnjega izvleka kartice v tem obdobju uporabe vozila ali čas 23.59, če je ob tem času uporaba vozila še v teku),

▼B

— vrednost števca prevožene poti ob tem času,

— registrsko številko vozila in državo, v kateri je registrirano.

(270) Vozniška kartica je zmožna hraniti najmanj 84 takih zapisov.

4.5.3.1.11 Kraji, v katerih se dnevne delovne izmene začnejo in/ali končajo

(271) Vozniška kartica je zmožna hraniti naslednje podatke v zvezi s kraji začetka in/ali konca dnevnih delovnih izmen, ki jih vnese voznik:

— datum in čas vnosa (ali datum/čas, povezan z vnosom, kadar je vnos opravljen s postopkom ročnega vnosa),

— vrsto vnosa (začetek ali konec, stanje vnosa),

— vneseno državo in regijo,

— vrednost števca prevožene poti.

(272) Pomnilnik podatkov na vozniški kartici je zmožen hraniti najmanj 42 parov takih zapisov.

4.5.3.1.12 Podatki o seji s kartico

(273) Vozniška kartica je zmožna hraniti naslednje podatke o vozilu, v katerem je bila odprta trenutna seja s to kartico:

— datum in čas odprtja seje (tj. vstavitve kartice) z ločljivostjo ene sekunde,

— registrsko številko vozila in državo, v kateri je registrirano.

4.5.3.1.13 Podatki o nadzornih dejavnostih

(274) Vozniška kartica je zmožna hraniti naslednje podatke, povezane z nadzornimi dejavnostmi:

— datum in čas nadzora,

— številko in državo izdajateljico nadzorne kartice,

— vrsto nadzora (prikazovanje in/ali tiskanje in/ali prenos podatkov iz VU in/ali prenos podatkov s kartice (gl. opombo)),

— v primeru prenosa podatkov obdobje, za katerega so podatki preneseni,

— registrsko številko vozila, v zvezi s katerim je bil izveden nadzor, in državo, v kateri je vozilo registrirano.

Opomba: Prenos podatkov s kartice se zabeleži le, če poteka preko zapisovalne naprave.

(275) Vozniška kartica je zmožna hraniti en tak zapis.

4.5.3.1.14 Podatki o posebnih stanjih

(276) Vozniška kartica je zmožna hraniti naslednje podatke, povezane s posebnimi stanji, vnesenimi v času, ko je bila kartica vstavljena (v katerikoli reži):

— datum in čas vnosa,

— vrsto posebnega stanja.

▼B

(277) Vozniška kartica je zmožna hraniti najmanj 56 takih zapisov.

4.5.3.2 Tahografske aplikacije druge generacije (niso dostopne enotam v vozilu prve generacije)

4.5.3.2.1 Identifikacija aplikacije

(278) Vozniška kartica je zmožna hraniti naslednje identifikacijske podatke aplikacije:

— identifikacijo tahografske aplikacije,

— vrsto identifikacije tahografske kartice.

4.5.3.2.2 Ključi in certifikati

(279) Vozniška kartica je zmožna hraniti več različnih kriptografskih ključev in certifikatov, kot je določeno v delu B Dodatka 11.

4.5.3.2.3 Identifikacija kartice

(280) Vozniška kartica je zmožna hraniti naslednje identifikacijske podatke kartice:

— številko kartice,

— državo izdajateljico, ime organa izdajatelja, datum izdaje,

— datum začetka veljavnosti kartice, datum poteka veljavnosti kartice.

4.5.3.2.4 Identifikacija imetnika kartice

(281) Vozniška kartica je zmožna hraniti naslednje identifikacijske podatke imetnika kartice:

— priimek imetnika kartice,

— ime(-na) imetnika kartice,

— datum rojstva,

— izbrani jezik.

4.5.3.2.5 Prenos podatkov s kartice

(282) Vozniška kartica je zmožna hraniti naslednje podatke o prenosih podatkov s kartice:

— datum in čas zadnjega prenosa podatkov s kartice (za druge namene kot nadzor).

(283) Vozniška kartica je zmožna hraniti en tak zapis.

4.5.3.2.6 Podatki o vozniškem dovoljenju

(284) Vozniška kartica je zmožna hraniti naslednje podatke o vozniškem dovoljenju:

— državo izdajateljico, ime organa izdajatelja,

— številko vozniškega dovoljenja (na dan izdaje kartice).

4.5.3.2.7 Podatki o dogodkih

Za namen tega pododstavka velja, da se čas shranjuje z ločljivostjo 1 sekunde.

▼B

(285) Vozniška kartica je zmožna hraniti podatke, povezane z naslednjimi dogodki, ki jih zazna zapisovalna naprava v času, ko je kartica vstavljena:

— časovno prekrivanje (kjer je vzrok dogodka ta kartica),

— vstavitev kartice med vožnjo (kjer pri dogodku nastopa ta kartica),

— zadnja seja s kartico nepravilno zaključena (kjer pri dogodku nastopa ta kartica),

— izpad napajanja,

— napaka pri komuniciranju z opremo za komunikacijo na daljavo,

— ni informacij o položaju s strani GNSS sprejemnika,

— napaka pri komuniciranju z zunanjo GNSS opremo,

— napaka v podatkih o gibanju,

— navzkrižje v gibanju vozila,

— poskusi kršenja varnosti,

— časovno navzkrižje.

(286) Vozniška kartica je zmožna hraniti naslednje podatke o teh dogodkih:

— kodo dogodka,

— datum in čas začetka dogodka (ali vstavitve kartice, če je dogodek ob tem času že v teku),

— datum in čas konca dogodka (ali izvleka kartice, če je dogodek ob tem času že v teku),

— registrsko številko vozila, v katerem je dogodek nastopil, in državo, v kateri je vozilo registrirano.

Opomba: Pri dogodku „časovno prekrivanje“:

— datum in čas začetka dogodka pomeni datum in čas izvleka kartice iz prejšnjega vozila,

— datum in čas konca dogodka pomeni datum in čas vstavitve kartice v trenutno vozilo,

— podatki o vozilu se nanašajo na trenutno vozilo, v katerem je dogodek nastopil.

Opomba: Pri dogodku „zadnja seja s kartico nepravilno zaključena“:

— datum in čas začetka dogodka sta datum in čas vstavitve kartice pri seji, ki ni bila pravilno zaključena,

— datum in čas konca dogodka sta datum in čas vstavitve kartice pri seji, v kateri je bil dogodek zaznan (tj. trenutni seji),

▼B

— podatki o vozilu se nanašajo na vozilo, v katerem seja ni bila pravilno zaključena.

(287) Vozniška kartica je zmožna hraniti podatke o šestih najnovejših dogodkih vsake vrste (tj. skupaj 66 dogodkih).

4.5.3.2.8 Podatki o napakah

Za namen tega pododstavka velja, da se čas zapisuje z ločljivostjo 1 sekunde.

(288) Vozniška kartica je zmožna hraniti podatke, povezane z naslednjimi napakami, ki jih zazna zapisovalna naprava v času, ko je kartica vstavljena:

— napaka kartice (kjer pri dogodku nastopa ta kartica),

— napaka na zapisovalni napravi.

(289) Vozniška kartica je zmožna hraniti naslednje podatke o teh napakah:

— kodo napake,

— datum in čas začetka napake (ali vstavitve kartice, če je napaka ob tem času že v teku),

— datum in čas konca napake (ali izvleka kartice, če je napaka ob tem času že v teku),

— registrsko številko vozila, v katerem se je napaka zgodila, in državo, v kateri je vozilo registrirano.

(290) Vozniška kartica je zmožna hraniti podatke o dvanajstih najnovejših napakah vsake vrste (tj. skupaj 24 napakah).

4.5.3.2.9 Podatki o voznikovih dejavnostih

(291) Vozniška kartica je za vsak koledarski dan, na katerega je bila kartica uporabljena ali za katerega je voznik dejavnosti vnesel ročno, zmožna hraniti naslednje podatke:

— datum,

— števec dni prisotnosti (ki se poveča za eno ob vsakem takem novem koledarskem dnevu),

— celotno dolžino poti, ki jo je voznik prevozil na ta dan,

— stanje voznika ob 00.00,

— ob vsaki voznikovi spremembi dejavnosti in/ali spremembi stanja vožnje in/ali ob vsaki vstavitvi/izvleku kartice:

— stanje vožnje (POSADKA, POSAMEZNIK),

— režo (VOZNIK, SOVOZNIK),

— stanje kartice (VSTAVLJENA, NI VSTAVLJENA),

— dejavnost (VOŽNJA, RAZPOLOŽLJIVOST, DELO, ODMOR/POČITEK),

▼B

— čas spremembe.

(292) Pomnilnik podatkov na vozniški kartici je zmožen hraniti podatke o voznikovih dejavnostih najmanj 28 dni (povprečna voznikova dejavnost je opredeljena kot 93 sprememb dejavnosti na dan).

(293) Podatki iz zahtev 286, 289 in 291 so shranjeni tako, da je mogoče poizvedovanje po dejavnostih iz pomnilnika v zaporedju njihovih nastopov, tudi v primerih časovnih prekrivanj.

4.5.3.2.10 Podatki o uporabljenih vozilih

(294) Vozniška kartica je za vsak koledarski dan, na katerega je bila uporabljena, in za vsako obdobje uporabe določenega vozila na ta dan (obdobje uporabe vključuje vse cikle vstavitve/izvleka kartice v vozilu z vidika kartice), zmožna hraniti naslednje podatke:

— datum in čas prve uporabe vozila (tj. prve vstavitve kartice v tem obdobju uporabe vozila ali čas 00.00, če je ob tem času uporaba vozila še v teku),

— vrednost števca prevožene poti ob tem času prve uporabe,

— datum in čas zadnje uporabe vozila (tj. zadnjega izvleka kartice v tem obdobju uporabe vozila ali čas 23.59, če je ob tem času uporaba vozila že v teku),

— vrednost števca prevožene poti ob tem času zadnje uporabe,

— registrsko številko vozila in državo, v kateri je registrirano,

— identifikacijsko številko vozila (VIN).

(295) Vozniška kartica je zmožna hraniti najmanj 84 takih zapisov.

4.5.3.2.11 Kraji in položaji, v katerih se dnevne delovne izmene začnejo in/ali končajo

(296) Vozniška kartica je zmožna hraniti naslednje podatke v zvezi s kraji začetka in/ali konca dnevnih delovnih izmen, ki jih vnese voznik:

— datum in čas vnosa (ali datum/čas, povezan z vnosom, kadar je vnos opravljen s postopkom ročnega vnosa),

— vrsto vnosa (začetek ali konec, stanje vnosa),

— vneseno državo in regijo,

— vrednost števca prevožene poti,

— položaj vozila,

— točnost GNSS, datum in čas v trenutku, ko je bil določen položaj.

(297) Pomnilnik podatkov na vozniški kartici je zmožen hraniti najmanj 84 parov takih zapisov.

▼B

4.5.3.2.12 Podatki o seji s kartico

(298) Vozniška kartica je zmožna hraniti naslednje podatke o vozilu, v katerem je bila odprta trenutna seja s to kartico:

— datum in čas odprtja seje (tj. vstavitve kartice) z ločljivostjo ene sekunde,

— registrsko številko vozila in državo, v kateri je registrirano.

4.5.3.2.13 Podatki o nadzornih dejavnostih

(299) Vozniška kartica je zmožna hraniti naslednje podatke, povezane z nadzornimi dejavnostmi:

— datum in čas nadzora,

— številko in državo izdajateljico nadzorne kartice,

— vrsto nadzora (prikazovanje in/ali tiskanje in/ali prenos podatkov iz VU in/ali prenos podatkov s kartice (gl. opombo)),

— v primeru prenosa podatkov obdobje, za katerega so podatki preneseni,

— registrsko številko vozila, v zvezi s katerim je bil izveden nadzor, in državo, v kateri je vozilo registrirano.

Opomba: Varnostne zahteve narekujejo, naj se prenos podatkov zabeleži le, če poteka preko zapisovalne naprave.

(300) Vozniška kartica je zmožna hraniti en tak zapis.

4.5.3.2.14 Podatki o posebnih stanjih

(301) Vozniška kartica je zmožna hraniti naslednje podatke, povezane s posebnimi stanji, vnesenimi v času, ko je bila kartica vstavljena (v katerikoli reži):

— datum in čas vnosa,

— vrsto posebnega stanja.

(302) Vozniška kartica je zmožna hraniti najmanj 56 takih zapisov.

4.5.3.2.15 Podatki o uporabljenih enotah v vozilu

(303) Vozniška kartica je zmožna hraniti naslednje podatke, povezane z različnimi enotami v vozilu, v katerih je bila kartica uporabljena:

— datum in čas začetka obdobja uporabe enote v vozilu (tj. prve vstavitve kartice v enoto v vozilu v danem obdobju),

— proizvajalca enote v vozilu,

— vrsto enote v vozilu,

— številko različice programske opreme enote v vozilu.

(304) Vozniška kartica je zmožna hraniti najmanj 84 takih zapisov.

▼B

4.5.3.2.16 Kraji, kjer čas neprekinjene vožnje doseže tri ure

(305) Vozniška kartica je zmožna hraniti naslednje podatke, povezane s krajem, kjer čas neprekinjene vožnje voznika doseže večkratnik treh ur:

— datum in čas v trenutku, ko čas neprekinjene vožnje imetnika kartice doseže večkratnik treh ur,

— položaj vozila,

— točnost GNSS, datum in čas v trenutku, ko je bil določen položaj.

(306) Vozniška kartica je zmožna hraniti najmanj 252 takih zapisov.

4.5.4 *Kartica servisne delavnice*

4.5.4.1 Tahografska aplikacija (dostopna enotam v vozilu prve in druge generacije)

4.5.4.1.1 Identifikacija aplikacije

(307) Kartica servisne delavnice je zmožna hraniti naslednje identifikacijske podatke aplikacije:

— identifikacijo tahografske aplikacije,

— vrsto identifikacije tahografske kartice.

4.5.4.1.2 Ključi in certifikati

(308) Kartica servisne delavnice je zmožna hraniti več različnih kriptografskih ključev in certifikatov, kot je določeno v delu A Dodatka 11.

(309) Kartica servisne delavnice je zmožna hraniti osebno identifikacijsko številko (PIN).

4.5.4.1.3 Identifikacija kartice

(310) Kartica servisne delavnice je zmožna hraniti naslednje identifikacijske podatke kartice:

— številko kartice,

— državo izdajateljico, ime organa izdajatelja, datum izdaje,

— datum začetka veljavnosti kartice, datum poteka veljavnosti kartice.

4.5.4.1.4 Identifikacija imetnika kartice

(311) Kartica servisne delavnice je zmožna hraniti naslednje identifikacijske podatke imetnika kartice:

— ime servisne delavnice,

— naslov servisne delavnice,

— priimek imetnika kartice,

— ime(-na) imetnika kartice,

— izbrani jezik.

4.5.4.1.5 Prenos podatkov s kartice

(312) Kartica servisne delavnice je zmožna hraniti podatkovni zapis o prenosih podatkov s kartice na enak način kot vozniška kartica.

▼B

4.5.4.1.6 Podatki o kalibraciji in nastavljanju časa

(313) Kartica servisne delavnice je zmožna hraniti zapise o kalibracijah in/ali nastavljanju časa, opravljenih na kartici, vstavljeni v zapisovalno napravo.

(314) Vsak zapis o kalibraciji obsega naslednje podatke:

— namen kalibracije (aktivacija, prva namestitev, namestitev, redni kontrolni pregled),

— identifikacijo vozila,

— posodobljene ali potrjene parametre (w, k, l, velikost pnevmatik, nastavitev naprave za omejevanje hitrosti, števec prevožene poti (stare in nove vrednosti), datum in čas (stare in nove vrednosti)),

— identifikacijo zapisovalne naprave (kataloška številka VU, serijska številka VU, serijska številka tipala gibanja).

(315) Kartica servisne delavnice je zmožna hraniti najmanj 88 takih zapisov.

(316) Kartica servisne delavnice ima vgrajen števec, ki kaže, koliko kalibracij je že bilo opravljenih s to kartico.

(317) Kartica servisne delavnice ima vgrajen števec, ki kaže, koliko kalibracij je že bilo opravljenih s to kartico od zadnjega prenosa podatkov z nje.

4.5.4.1.7 Podatki o dogodkih in napakah

(318) Kartica servisne delavnice je zmožna hraniti podatkovni zapis o dogodkih in napakah na enak način kot vozniška kartica.

(319) Kartica servisne delavnice je zmožna hraniti podatke o treh najnovejših dogodkih vsake vrste (tj. 18 dogodkov) in šestih najnovejših napakah vsake vrste (tj. 12 napak).

4.5.4.1.8 Podatki o voznikovih dejavnostih

(320) Kartica servisne delavnice je zmožna hraniti podatke o voznikovih dejavnostih na enak način kot vozniška kartica.

(321) Kartica servisne delavnice je zmožna hraniti podatke o voznikovih dejavnostih za najmanj en dan povprečnih voznikovih dejavnosti.

4.5.4.1.9 Podatki o uporabljenih vozilih

(322) Kartica servisne delavnice je zmožna hraniti podatkovni zapis o uporabljenih vozilih na enak način kot vozniška kartica.

(323) Kartica servisne delavnice je zmožna hraniti najmanj 4 take zapise.

4.5.4.1.10 Podatki o začetku in/ali koncu dnevnih delovnih izmen

(324) Kartica servisne delavnice je zmožna hraniti podatkovni zapis o začetku in/ali koncu dnevnih delovnih izmen na enak način kot vozniška kartica.

(325) Kartica servisne delavnice je zmožna hraniti najmanj tri pare takih zapisov.

▼B

4.5.4.1.11 Podatki o seji s kartico

(326) Kartica servisne delavnice je zmožna hraniti podatkovni zapis o sejah s kartico na enak način kot vozniška kartica.

4.5.4.1.12 Podatki o nadzornih dejavnostih

(327) Kartica servisne delavnice je zmožna hraniti podatkovni zapis o nadzornih dejavnostih na enak način kot vozniška kartica.

4.5.4.1.13 Podatki o posebnih stanjih

(328) Kartica servisne delavnice je zmožna hraniti podatke, povezane s posebnimi stanji, na enak način kot vozniška kartica.

(329) Kartica servisne delavnice je zmožna hraniti najmanj 2 taka zapisa.

4.5.4.2 Tahografske aplikacije druge generacije (niso dostopne enotam v vozilu prve generacije)

4.5.4.2.1 Identifikacija aplikacije

(330) Kartica servisne delavnice je zmožna hraniti naslednje identifikacijske podatke aplikacije:

— identifikacijo tahografske aplikacije,

— vrsto identifikacije tahografske kartice.

4.5.4.2.2 Ključi in certifikati

(331) Kartica servisne delavnice je zmožna hraniti več različnih kriptografskih ključev in certifikatov, kot je določeno v delu B Dodatka 11.

(332) Kartica servisne delavnice je zmožna hraniti osebno identifikacijsko številko (PIN).

4.5.4.2.3 Identifikacija kartice

(333) Kartica servisne delavnice je zmožna hraniti naslednje identifikacijske podatke kartice:

— številko kartice,

— državo izdajateljico, ime organa izdajatelja, datum izdaje,

— datum začetka veljavnosti kartice, datum poteka veljavnosti kartice.

4.5.4.2.4 Identifikacija imetnika kartice

(334) Kartica servisne delavnice je zmožna hraniti naslednje identifikacijske podatke imetnika kartice:

— ime servisne delavnice,

— naslov servisne delavnice,

— priimek imetnika kartice,

— ime(-na) imetnika kartice,

— izbrani jezik.

4.5.4.2.5 Prenos podatkov s kartice

(335) Kartica servisne delavnice je zmožna hraniti podatkovni zapis o prenosih podatkov s kartice na enak način kot vozniška kartica.

▼B

4.5.4.2.6 Podatki o kalibraciji in nastavljanju časa

(336) Kartica servisne delavnice je zmožna hraniti zapise o kalibracijah in/ali nastavljanju časa, opravljenih na kartici, vstavljeni v zapisovalno napravo.

(337) Vsak zapis o kalibraciji obsega naslednje podatke:

— namen kalibracije (aktivacija, prva namestitev, namestitev, redni kontrolni pregled),

— identifikacijo vozila,

— posodobljene ali potrjene parametre (w, k, l, velikost pnevmatik, nastavitev naprave za omejevanje hitrosti, števec prevožene poti (stare in nove vrednosti), datum in čas (stare in nove vrednosti)),

— identifikacijo zapisovalne naprave (kataloška številka VU, serijska številka VU, serijska številka tipala gibanja, serijska številka opreme za komunikacijo na daljavo in serijska številka zunanje GNSS opreme, če je ustrezno),

— vrsto in identifikatorje vseh nameščenih pečatov,

— zmožnost enote v vozilu za uporabo tahografskih kartic prve generacije (omogočena ali ne).

(338) Kartica servisne delavnice je zmožna hraniti najmanj 88 takih zapisov.

(339) Kartica servisne delavnice ima vgrajen števec, ki kaže, koliko kalibracij je že bilo opravljenih s to kartico.

(340) Kartica servisne delavnice ima vgrajen števec, ki kaže, koliko kalibracij je že bilo opravljenih s to kartico od zadnjega prenosa podatkov z nje.

4.5.4.2.7 Podatki o dogodkih in napakah

(341) Kartica servisne delavnice je zmožna hraniti podatkovni zapis o dogodkih in napakah na enak način kot vozniška kartica.

(342) Kartica servisne delavnice je zmožna hraniti podatke o treh najnovejših dogodkih vsake vrste (tj. 33 dogodkov) in šestih najnovejših napakah vsake vrste (tj. 12 napak).

4.5.4.2.8 Podatki o voznikovih dejavnostih

(343) Kartica servisne delavnice je zmožna hraniti podatke o voznikovih dejavnostih na enak način kot vozniška kartica.

(344) Kartica servisne delavnice je zmožna hraniti podatke o voznikovih dejavnostih za najmanj en dan povprečnih voznikovih dejavnosti.

4.5.4.2.9 Podatki o uporabljenih vozilih

(345) Kartica servisne delavnice je zmožna hraniti podatkovni zapis o uporabljenih vozilih na enak način kot vozniška kartica.

(346) Kartica servisne delavnice je zmožna hraniti najmanj 4 take zapise.

▼B

4.5.4.2.10 Podatki o začetku in/ali koncu dnevnih delovnih izmen

(347) Kartica servisne delavnice je zmožna hraniti podatkovni zapis o začetku in/ali koncu dnevnih delovnih izmen na enak način kot vozniška kartica.

(348) Kartica servisne delavnice je zmožna hraniti najmanj tri pare takih zapisov.

4.5.4.2.11 Podatki o seji s kartico

(349) Kartica servisne delavnice je zmožna hraniti podatkovni zapis o sejah s kartico na enak način kot vozniška kartica.

4.5.4.2.12 Podatki o nadzornih dejavnostih

(350) Kartica servisne delavnice je zmožna hraniti podatkovni zapis o nadzornih dejavnostih na enak način kot vozniška kartica.

4.5.4.2.13 Podatki o uporabljenih enotah v vozilu

(351) Kartica servisne delavnice je zmožna hraniti naslednje podatke, povezane z različnimi enotami v vozilu, v katerih je bila kartica uporabljena:

— datum in čas začetka obdobja uporabe enote v vozilu (tj. prve vstavitve kartice v enoto v vozilu v danem obdobju),

— proizvajalca enote v vozilu,

— vrsto enote v vozilu,

— številko različice programske opreme enote v vozilu.

(352) Kartica servisne delavnice je zmožna hraniti najmanj 4 take zapise.

4.5.4.2.14 Kraji, kjer čas neprekinjene vožnje doseže tri ure

(353) Kartica servisne delavnice je zmožna hraniti naslednje podatke, povezane s krajem, kjer čas neprekinjene vožnje voznika doseže večkratnik treh ur:

— datum in čas v trenutku, ko čas neprekinjene vožnje imetnika kartice doseže večkratnik treh ur,

— položaj vozila,

— točnost GNSS, datum in čas v trenutku, ko je bil določen položaj.

(354) Kartica servisne delavnice je zmožna hraniti najmanj 18 takih zapisov.

4.5.4.2.15 Podatki o posebnih stanjih

(355) Kartica servisne delavnice je zmožna hraniti podatke, povezane s posebnimi stanji, na enak način kot vozniška kartica.

(356) Kartica servisne delavnice je zmožna hraniti najmanj 2 taka zapisa.

▼B

4.5.5 *Nadzorna kartica*

4.5.5.1 Tahografska aplikacija (dostopna enotam v vozilu prve in druge generacije)

4.5.5.1.1 Identifikacija aplikacije

(357) Nadzorna kartica je zmožna hraniti naslednje identifikacijske podatke aplikacije:

— identifikacijo tahografske aplikacije,

— vrsto identifikacije tahografske kartice.

4.5.5.1.2 Ključi in certifikati

(358) Nadzorna kartica je zmožna hraniti več različnih kriptografskih ključev in certifikatov, kot je določeno v delu A Dodatka 11.

4.5.5.1.3 Identifikacija kartice

(359) Nadzorna kartica je zmožna hraniti naslednje identifikacijske podatke kartice:

— številko kartice,

— državo izdajateljico, ime organa izdajatelja, datum izdaje,

— datum začetka veljavnosti kartice, datum poteka veljavnosti kartice (če je določen).

4.5.5.1.4 Identifikacija imetnika kartice

(360) Nadzorna kartica je zmožna hraniti naslednje identifikacijske podatke imetnika kartice:

— ime nadzornega organa,

— naslov nadzornega organa,

— priimek imetnika kartice,

— ime(-na) imetnika kartice,

— izbrani jezik.

4.5.5.1.5 Podatki o nadzornih dejavnostih

(361) Nadzorna kartica je zmožna hraniti naslednje podatke o nadzornih dejavnostih:

— datum in čas nadzora,

— vrsto nadzora (prikazovanje in/ali tiskanje in/ali prenos podatkov iz VU in/ali prenos podatkov s kartice in/ali cestno preverjanje kalibracije),

— obdobje, v zvezi s katerim so podatki preneseni (če je bil prenos opravljen),

— registrsko številko vozila in organ države članice, pristojen za registracijo vozila,

— številko in državo izdajateljico nadzorovane vozniške kartice.

(362) Nadzorna kartica je zmožna hraniti najmanj 230 takih zapisov.

▼B

4.5.5.2 Tahografske aplikacije druge generacije (G2) (niso dostopne enotam v vozilu prve generacije)

4.5.5.2.1 Identifikacija aplikacije

(363) Nadzorna kartica je zmožna hraniti naslednje identifikacijske podatke aplikacije:

— identifikacijo tahografske aplikacije,

— vrsto identifikacije tahografske kartice.

4.5.5.2.2 Ključi in certifikati

(364) Nadzorna kartica je zmožna hraniti več različnih kriptografskih ključev in certifikatov, kot je določeno v delu B Dodatka 11.

4.5.5.2.3 Identifikacija kartice

(365) Nadzorna kartica je zmožna hraniti naslednje identifikacijske podatke kartice:

— številko kartice,

— državo izdajateljico, ime organa izdajatelja, datum izdaje,

— datum začetka veljavnosti kartice, datum poteka veljavnosti kartice (če je določen).

4.5.5.2.4 Identifikacija imetnika kartice

(366) Nadzorna kartica je zmožna hraniti naslednje identifikacijske podatke imetnika kartice:

— ime nadzornega organa,

— naslov nadzornega organa,

— priimek imetnika kartice,

— ime(-na) imetnika kartice,

— izbrani jezik.

4.5.5.2.5 Podatki o nadzornih dejavnostih

(367) Nadzorna kartica je zmožna hraniti naslednje podatke o nadzornih dejavnostih:

— datum in čas nadzora,

— vrsto nadzora (prikazovanje in/ali tiskanje in/ali prenos podatkov iz VU in/ali prenos podatkov s kartice in/ali cestno preverjanje kalibracije),

— obdobje, v zvezi s katerim so podatki preneseni (če je bil prenos opravljen),

— registrsko številko vozila in organ države članice, pristojen za registracijo vozila,

— številko in državo izdajateljico nadzorovane vozniške kartice.

(368) Nadzorna kartica je zmožna hraniti najmanj 230 takih zapisov.

▼B

4.5.6 *Kartica podjetja*

4.5.6.1 Tahografska aplikacija (dostopna enotam v vozilu prve in druge generacije)

4.5.6.1.1 Identifikacija aplikacije

(369) Kartica podjetja je zmožna hraniti naslednje identifikacijske podatke aplikacije:

— identifikacijo tahografske aplikacije,

— vrsto identifikacije tahografske kartice.

4.5.6.1.2 Ključi in certifikati

(370) Kartica podjetja je zmožna hraniti več različnih kriptografskih ključev in certifikatov, kot je določeno v delu A Dodatka 11.

4.5.6.1.3 Identifikacija kartice

(371) Kartica podjetja je zmožna hraniti naslednje identifikacijske podatke kartice:

— številko kartice,

— državo izdajateljico, ime organa izdajatelja, datum izdaje,

— datum začetka veljavnosti kartice, datum poteka veljavnosti kartice (če je določen).

4.5.6.1.4 Identifikacija imetnika kartice

(372) Kartica podjetja je zmožna hraniti naslednje identifikacijske podatke imetnika kartice:

— ime podjetja,

— naslov podjetja.

4.5.6.1.5 Podatki o dejavnostih podjetja

(373) Kartica podjetja je zmožna hraniti naslednje podatke o dejavnostih podjetja:

— datum in čas dejavnosti,

— vrsto dejavnosti (vklop in/ali izklop blokade VU in/ali prenos podatkov z VU in/ali kartice),

— obdobje, v zvezi s katerim so podatki preneseni (če je bil prenos opravljen),

— registrsko številko vozila in organ države članice, pristojen za registracijo vozila,

— številko in državo izdajateljico kartice (če je bil opravljen prenos podatkov s kartice).

(374) Kartica podjetja je zmožna hraniti najmanj 230 takih zapisov.

▼B

4.5.6.2 Tahografske aplikacije druge generacije (G2) (niso dostopne enotam v vozilu prve generacije)

4.5.6.2.1 Identifikacija aplikacije

(375) Kartica podjetja je zmožna hraniti naslednje identifikacijske podatke aplikacije:

— identifikacijo tahografske aplikacije,

— vrsto identifikacije tahografske kartice.

4.5.6.2.2 Ključi in certifikati

(376) Kartica podjetja je zmožna hraniti več različnih kriptografskih ključev in certifikatov, kot je določeno v delu B Dodatka 11.

4.5.6.2.3 Identifikacija kartice

(377) Kartica podjetja je zmožna hraniti naslednje identifikacijske podatke kartice:

— številko kartice,

— državo izdajateljico, ime organa izdajatelja, datum izdaje,

— datum začetka veljavnosti kartice, datum poteka veljavnosti kartice (če je določen).

4.5.6.2.4 Identifikacija imetnika kartice

(378) Kartica podjetja je zmožna hraniti naslednje identifikacijske podatke imetnika kartice:

— ime podjetja,

— naslov podjetja.

4.5.6.2.5 Podatki o dejavnostih podjetja

(379) Kartica podjetja je zmožna hraniti naslednje podatke o dejavnostih podjetja:

— datum in čas dejavnosti,

— vrsto dejavnosti (vklop in/ali izklop blokade VU in/ali prenos podatkov z VU in/ali kartice),

— obdobje, v zvezi s katerim so podatki preneseni (če je bil prenos opravljen),

— registrsko številko vozila in organ države članice, pristojen za registracijo vozila,

— številko in državo izdajateljico kartice (če je bil opravljen prenos podatkov s kartice).

(380) Kartica podjetja je zmožna hraniti najmanj 230 takih zapisov.

5 NAMESTITEV ZAPISOVALNE NAPRAVE

5.1 **Namestitev**

(381) Nova zapisovalna naprava se izvajalcem namestitve ali proizvajalcem vozil dobavi neaktivirana, z vsemi kalibracijskimi parametri iz poglavja 3.21, nastavljenimi na ustrezne in veljavne privzete vrednosti. Kjer ni ustrezna nobena privzeta vrednost, naj bodo črkovni parametri nastavljeni kot nizi znakov „?“, številski parametri pa na vrednosti „0“. Dobava delov zapisovalne naprave, pomembnih za varnost, se lahko omeji, če se tako zahteva med varnostnim certificiranjem.

▼B

(382) Dokler ni aktivirana, zapisovalna naprava omogoča dostop do funkcije kalibracije tudi, kadar ni v kalibracijskem načinu.

(383) Dokler ni aktivirana, zapisovalna naprava ne zapisuje in ne hrani podatkov, omenjenih v poglavjih 3.12.3, 3.12.9 ter od 3.12.12 do vključno 3.12.15.

(384) Pri nameščanju proizvajalci vozil prednastavijo vse znane parametre.

(385) Proizvajalci vozil ali izvajalci namestitve nameščeno zapisovalno napravo aktivirajo najpozneje, preden se vozilo uporabi v področju uporabe Uredbe (ES) št. 561/2006.

(386) Aktivacijo zapisovalne naprave samodejno sproži prva vstavitev veljavne kartice servisne delavnice v katero koli vmesniško napravo za kartice.

(387) Pred ali med aktivacijo se samodejno opravijo tudi vse potrebne operacije povezave med tipalom gibanja in enoto v vozilu.

(388) Podobno se pred ali med aktivacijo samodejno opravijo tudi vse potrebne operacije povezave med zunanjo GNSS opremo in enoto v vozilu.

(389) Po aktivaciji zapisovalna naprava v celoti opravlja predpisane funkcije in ustrezno omejuje dostop do podatkov.

(390) Po aktivaciji zapisovalna naprava opremi za komunikacijo na daljavo sporoča zaščitene podatke za namen usmerjenega cestnega nadzora.

(391) Po aktivaciji zapisovalna naprava v celoti opravlja funkcije zapisovanja in hranjenja podatkov.

(392) Namestitvi sledi kalibracija. Prva kalibracija ne vključuje nujno vnosa registrske številke vozila (VRN), če je pooblaščena servisna delavnica, ki mora opraviti to kalibracijo, ne pozna. V teh okoliščinah in samo v tem trenutku se lastniku vozila dovoli, da vnese VRN z uporabo svoje kartice podjetja, preden se vozilo uporabi v področju uporabe Uredbe (ES) št. 561/2006 (npr. s pomočjo ukazov v sestavu menijev uporabniškega vmesnika enote v vozilu) ([1]). Kakršne koli posodobitve ali potrditve tega vnosa so možne le z uporabo kartice servisne delavnice.

(393) Namestitev zunanje GNSS opreme zahteva povezavo z enoto v vozilu in preveritev GNSS informacij o položaju.

(394) Zapisovalna naprava je v vozilu nameščena tako, da voznik potrebne funkcije lahko doseže s svojega sedeža.

([1]) UL L 102, 11.4.2006, str. 1.

▼B

5.2 **Namestitvena ploščica**

(395) Po preveritvi zapisovalne naprave ob namestitvi se nanjo pritrdi jasno vidna in enostavno dostopna namestitvena ploščica z gravuro ali trajnim potiskom. Če to ni možno, se ploščica pritrdi na B-stebriček vozila tako, da je jasno vidna. Na vozilih, ki nimajo B-stebrička, se namestitvena ploščica pritrdi na okvir vrat na voznikovi strani vozila in je v vseh primerih jasno vidna.

Po vsakem pregledu pri pooblaščenem izvajalcu namestitve ali servisni delavnici se namesto prejšnje ploščice pritrdi nova ploščica.

(396) Na ploščici so navedeni vsaj naslednji podatki:

— ime, naslov ali trgovsko ime pooblaščenega izvajalca namestitve ali servisne delavnice,

— značilni koeficient vozila, izražen kot „w = … imp/km“,

— konstanta zapisovalne naprave, izražena kot „k = … imp/km“,

— dejanski obseg pnevmatik, izražen kot „l = … mm“,

— velikost pnevmatik,

— datum merjenja značilnega koeficienta vozila in dejanskega obsega pnevmatik,

— identifikacijska številka vozila,

— prisotnost (ali odsotnost) zunanje GNSS opreme,

— serijska številka zunanje GNSS opreme,

— serijska številka naprave za komunikacijo na daljavo,

— serijska številka vseh nameščenih pečatov,

— del vozila, v katerega je nameščen pretvornik, če ta obstaja,

— del vozila, v katerega je nameščeno tipalo gibanja, če ni povezano z menjalnikom vozila ali če se ne uporablja pretvornik,

— barva kabla med pretvornikom in tistim delom vozila, ki zagotavlja vhodne impulze,

— serijska številka vgrajenega tipala gibanja na pretvorniku.

(397) Samo za vozila kategorij M1 in N1, ki so opremljena s pretvornikom v skladu z Uredbo Komisije (ES) št. 68/2009 ([1]), kot je bila nazadnje spremenjena, in kadar ni mogoče vključiti vseh potrebnih informacij, kot so opredeljene v zahtevi 396, se lahko uporabi druga, dodatna ploščica. V teh primerih ta dodatna ploščica vsebuje vsaj zadnje štiri alinee iz zahteve 396.

([1]) Uredba Komisije (ES) št. 68/2009 z dne 23. januarja 2009 o deveti prilagoditvi Uredbe Sveta (EGS) št. 3821/85 o tahografu (nadzorni napravi) v cestnem prometu tehničnemu napredku (UL L 21, 24.1.2009, str. 3).

▼B

Druga, dodatna ploščica je, če se uporabi, pritrjena ob ali v bližini prve ploščice, opisane v zahtevi 396, in zanjo velja enaka raven zaščite. Tudi na drugi ploščici je navedeno ime, naslov ali trgovsko ime pooblaščenega izvajalca namestitve ali servisne delavnice, ki je opravila namestitev, in datum namestitve.

5.3 **Zapečatenje**

(398) Zapečateni so naslednji deli:

— vsi priključki, ki bi, če ne bi bili priključeni, lahko omogočili nezaznavne spremembe ali povzročili nezaznavno izgubo podatkov (to lahko med drugim velja za pritrdilni element tipala gibanja na menjalniku, pretvornik za vozila kategorij M1/N1, priključek zunanje GNSS opreme ali enoto v vozilu);

— namestitvena ploščica, razen če je pritrjena tako, da je ni mogoče odstraniti, ne da bi se pri tem uničile oznake na njej.

(399) Zgoraj omenjeni pečati se smejo odstraniti:

— v nujnih primerih,

— za namestitev, nastavitev ali popravilo naprave za omejevanje hitrosti vozila ali katere koli druge naprave, ki prispeva k varnosti v cestnem prometu, pod pogojem, da zapisovalna naprava še naprej deluje zanesljivo in pravilno ter jo pooblaščeni izvajalec namestitve ali servisna delavnica (v skladu s poglavjem 6) ponovno zapečati takoj po namestitvi naprave za omejevanje hitrosti ali katere koli druge naprave, ki prispeva k varnosti v cestnem prometu, ali v sedmih dneh v drugih primerih.

(400) Vsak prelom teh pečatov se pisno utemelji z navedbo razlogov; ta utemeljitev se da na voljo pristojnemu organu.

(401) Vsak pečat ima serijsko številko, ki mu jo dodeli njegov proizvajalec. Ta številka je edinstvena in se razlikuje od vseh drugih številk pečatov, ki jih dodeljujejo drugi proizvajalci pečatov.

Ta edinstvena identifikacijska številka je opredeljena kot: neodstranljiva oznaka MM NNNNNN, pri čemer je MM edinstvena identifikacija proizvajalca (vpisovanje v podatkovno zbirko izvaja Evropska komisija), NNNNNN pa je edinstvena alfanumerična številka pečata, kot jo določi proizvajalec.

(402) Na pečatih je prazen prostor, kamor lahko pooblaščeni izvajalci namestitve, servisne delavnice ali proizvajalci vozil dodajo posebno oznako v skladu s členom 22(3) Uredbe (EU) št. 165/2014.

Ta oznaka ne prekriva identifikacijske številke pečata.

(403) Proizvajalci pečatov so vpisani v namenski podatkovni zbirki in identifikacijske številke svojih pečatov javno objavijo v okviru postopka, ki ga določi Evropska komisija.

(404) Pooblaščene servisne delavnice in proizvajalci vozil v okviru Uredbe (EU) št. 165/2014 uporabljajo samo pečate tistih proizvajalcev pečatov, ki so vneseni v zgoraj omenjeni podatkovni zbirki.

▼B

(405) Proizvajalci pečatov in njihovi distributerji vodijo popolne evidence o sledljivosti pečatov, prodanih za uporabo v okviru Uredbe (EU) št. 165/2014, in jih na zahtevo predložijo pristojnim nacionalnim organom.

(406) Edinstvena identifikacijska številka pečata je vidna na namestitveni ploščici.

6 PREVERJANJA, KONTROLNI PREGLEDI IN POPRAVILA

Zahteve glede okoliščin iz člena 22(5) Uredbe (EU) št. 165/2014, ki upravičujejo prelom pečatov, so opredeljene v poglavju 5.3 te priloge.

6.1 **Pooblastitev izvajalcev namestitve, servisnih delavnic in proizvajalcev vozil**

Države članice odobravajo, redno nadzorujejo in certificirajo organe, ki izvajajo:

— nameščanje,

— preverjanja,

— kontrolne preglede,

— popravila.

Kartice servisne delavnice se izdajo le izvajalcem namestitve in/ali servisnim delavnicam, ki so odobreni za aktivacijo in/ali kalibracijo zapisovalne naprave v skladu s to prilogo ter, če ni ustrezno utemeljeno drugače:

— ki niso upravičeni do kartice podjetja in

— katerih druge poslovne dejavnosti ne predstavljajo potencialnega tveganja za varnost sistema, kot je določeno v Dodatku 10.

6.2 **Preverjanje novih ali popravljenih instrumentov**

(407) Vsako posamezno napravo, novo ali popravljeno, se preveri glede pravilnosti delovanja in točnosti odčitavanja in zapisovanja v okviru mej, predpisanih v poglavjih 3.2.1, 3.2.2, 3.2.3 in 3.3, z zapečatenjem v skladu s poglavjem 5.3 in kalibracijo.

6.3 **Pregled namestitve**

(408) Ob namestitvi v vozilo celotna instalacija (vključno z zapisovalno napravo) izpolnjuje določbe glede največjih dovoljenih odstopanj iz poglavij 3.2.1, 3.2.2, 3.2.3 in 3.3.

6.4 **Redni kontrolni pregledi**

(409) Redni kontrolni pregledi v vozilu nameščene opreme se opravijo po vsakem popravilu opreme ali po vsaki spremembi značilnega koeficienta vozila ali dejanskega obsega pnevmatik ali po tem, ko napaka časa UTC opreme preseže 20 minut, ali po spremembi registrske številke vozila ali najpozneje dve leti (24 mesecev) po zadnjem kontrolnem pregledu.

(410) Ti kontrolni pregledi vključujejo naslednja preverjanja:

— ali zapisovalna naprava deluje pravilno, vključno s funkcijo shranjevanja podatkov na tahografske kartice in komuniciranjem z bralniki komunikacij na daljavo,

▼B

— ali je zagotovljena skladnost z določbami poglavij 3.2.1 in 3.2.2 o največjih dovoljenih odstopanjih celotne instalacije,

— ali je zagotovljena skladnost z določbami poglavij 3.2.3 in 3.3,

— ali je zapisovalna naprava opremljena s homologacijsko oznako,

— ali sta pritrjeni namestitvena ploščica, kot je opredeljena v zahtevi 396, in označevalna ploščica, kot je opredeljena v zahtevi 225,

— preverjanje velikosti pnevmatik in njihovega dejanskega obsega,

— preverjanje, da na opremo ni pritrjena nobena naprava za prirejanje,

— preverjanje, da so pečati pravilno nameščeni in v dobrem stanju, da so njihove identifikacijske številke veljavne (da je proizvajalec pečata vnesen v podatkovno zbirko Evropske komisije) ter da njihove identifikacijske številke ustrezajo oznakam na namestitvenih ploščicah (glej zahtevo 401).

(411) Če se ugotovi, da se je po zadnjem kontrolnem pregledu zgodil eden od dogodkov, navedenih v poglavju 3.9 „Zaznavanje dogodkov in/ali napak“, ter proizvajalci tahografov in/ali nacionalni organi menijo, da ta dogodek lahko ogroža varnost naprave, servisna delavnica:

a. primerja identifikacijske podatke tipala gibanja, ki je priključeno na menjalnik, ter podatke povezanega tipala gibanja, registriranega v enoti v vozilu;

b. preveri, ali se informacije, zapisane na namestitveni ploščici, ujemajo z informacijami, ki jih vsebuje zapis enote v vozilu;

c. preveri, ali se serijska in homologacijska številka tipala gibanja, če sta natisnjeni na ohišju tipala gibanja, ujemata z informacijami, shranjenimi v pomnilniku podatkov enote v vozilu;

d. primerja identifikacijske podatke, označene na označevalni ploščici zunanje GNSS opreme, če obstaja, s podatki, shranjenimi v pomnilniku podatkov enote v vozilu.

(412) Servisne delavnice v svojih poročilih o kontrolnem pregledu zapišejo vse ugotovitve o prelomljenih pečatih ali napravah za prirejanje. Servisne delavnice ta poročila hranijo najmanj dve leti in jih na zahtevo pristojnih organov dajo na voljo.

(413) Ti kontrolni pregledi vključujejo kalibracijo in preventivno nadomestitev pečatov, za namestitev katerih so odgovorne servisne delavnice.

6.5 **Ugotavljanje napak**

(414) Napake pri namestitvi in med uporabo se ugotavljajo pod naslednjimi pogoji, ki se štejejo za standardne preskusne pogoje:

— prazno vozilo v normalnem delovanju;

— pritisk v pnevmatikah v skladu z navodili proizvajalca;

▼B

— obraba pnevmatik v dovoljenih mejah, določenih v nacionalni zakonodaji;

— gibanje vozila:

— vozilo se premika z lastnim motornim pogonom v ravni črti na ravni podlagi s hitrostjo 50 ± 5 km/h. Merilna razdalja je vsaj 1 000 m;

— za ta preskus se lahko uporabi tudi kaka druga metoda primerljive točnosti, npr. ustrezna preskusna proga.

6.6 **Popravila**

(415) Servisna delavnica ima zmogljivosti za prenos podatkov z zapisovalne naprave, tako da lahko te podatke posreduje nazaj prevoznemu podjetju.

(416) Če okvara zapisovalna naprave tudi po popravilu v servisni delavnici onemogoča prenos zapisanih podatkov, pooblaščena servisna delavnica prevoznemu podjetju izda potrdilo, da podatkov ni mogoče prenesti z zapisovalne naprave. Servisna delavnica hrani kopijo vsakega izdanega potrdila najmanj dve leti.

7 IZDAJANJE KARTIC

Procesi izdajanja kartic, ki jih vzpostavijo posamezne države članice, so v skladu z naslednjimi določbami:

(417) Ob prvi izdaji tahografske kartice prosilcu so indeks zaporedja (če obstaja), indeks nadomestitve in indeks podaljšanja kartice nastavljeni na „0“.

(418) Številke kartic pri neosebnih tahografskih karticah, ki se jih izda enemu nadzornemu organu ali eni servisni delavnici ali enemu prevoznemu podjetju, imajo prvih 13 števk enakih, indeksi zaporedja pa so različni.

(419) Tahografska kartica, ki se jo izda kot nadomestitev za obstoječo tahografsko kartico, ima enako številko kartice kot nadomeščena kartica, le indeks nadomestitve se poveča za „1“ (v vrstnem redu 0 … 9, A … Z).

(420) Tahografska kartica, ki se jo izda kot nadomestitev za obstoječo tahografsko kartico, ima isti datum poteka veljavnosti kot nadomeščena kartica.

(421) Tahografska kartica, ki se jo izda kot podaljšanje obstoječe tahografske kartice, ima enako številko kartice kot kartica, ki se obnavlja, le indeks nadomestitve se vrne na vrednost „0“, indeks podaljšanja pa se poveča za „1“ (v vrstnem redu 0 … 9, A … Z).

(422) Zamenjava obstoječe tahografske kartice, potrebna za spremembo upravnih podatkov, poteka po pravilih za podaljšanje kartice, če se izvede v isti državi članici, ali po pravilih za prvo izdajo kartice, če se izvede v drugi državi članici.

(423) V polje „priimek imetnika kartice“ se pri neosebnih karticah servisnih delavnic ali nadzornih karticah zapiše ime servisne delavnice ali nadzornega organa ali ime izvajalca namestitve ali inšpektorja, če tako določijo države članice.

▼B

(424) V skladu s členom 31 Uredbe (EU) št. 165/2014 morajo države članice med seboj po elektronski poti izmenjevati podatke, da bi zagotovile edinstvenost izdanih vozniških kartic.

8 HOMOLOGACIJA ZAPISOVALNE NAPRAVE IN TAHOGRAFSKIH KARTIC

8.1 **Splošne točke**

Za namen tega poglavja izraz „zapisovalna naprava“ pomeni „zapisovalno napravo ali njene sestavne dele“. Za kable, ki povezujejo tipalo gibanja z VU, zunanjo GNSS opremo z VU ali opremo za komunikacijo na daljavo z VU, homologacija ni potrebna. Papir, ki ga uporablja zapisovalna naprava, se šteje za sestavni del zapisovalne naprave.

Vsak proizvajalec lahko zaprosi za homologacijo svojega sestavnega dela v kombinaciji s katero koli vrsto tipala gibanja, zunanje GNSS opreme in obratno, pod pogojem, da je vsak od sestavnih delov skladen z zahtevami iz te priloge. Sicer lahko proizvajalci zaprosijo tudi za homologacijo zapisovalne naprave.

(425) Zapisovalna naprava se predloži v odobritev skupaj z vsemi vgrajenimi dodatnimi napravami.

(426) Homologacija zapisovalne naprave in tahografskih kartic vključuje varnostne preskuse, preskuse delovanja in preskuse interoperabilnosti. Pozitivne rezultate vsakega od teh preskusov se navede v ustreznem certifikatu.

(427) Pristojni homologacijski organi držav članic ne izdajo certifikata o homologaciji, če nimajo:

— potrdila o varnosti,

— potrdila o funkcionalnosti in

— potrdila o interoperabilnosti

za zapisovalno napravo ali tahografsko kartico, ki je predmet zahtevka za homologacijo.

(428) O vsaki spremembi programske ali strojne opreme naprave ali vrste materialov, uporabljenih pri njeni izdelavi, je treba pred uporabo obvestiti organ, ki je napravo homologiral. Ta organ lahko proizvajalcu odobri razširitev homologacije, lahko pa zahteva posodobitev ali potrditev ustreznih potrdil o funkcionalnosti, varnosti in/ali interoperabilnosti.

(429) Postopke za nadgradnjo nameščene zapisovalne naprave odobri organ, ki je zapisovalno napravo homologiral. Nadgradnja programske opreme ne sme spremeniti ali izbrisati nobenih podatkov o voznikovih dejavnostih, shranjenih v zapisovalni napravi. Nadgradnja programske opreme se sme izvesti le na odgovornost proizvajalca opreme.

(430) Homologacija sprememb programske opreme, namenjenih za nadgradnjo predhodno homologirane zapisovalne naprave, se ne sme zavrniti, če se takšne spremembe nanašajo samo na funkcije, ki niso opredeljene v tej prilogi. Iz nadgradnje programske opreme zapisovalne naprave se lahko izvzame uvedba novih naborov znakov, če ta tehnično ni izvedljiva.

▼B

8.2 **Potrdilo o varnosti**

(431) Potrdilo o varnosti se izda v skladu z določbami Dodatka 10 k tej prilogi. Certificirati je treba naslednje sestavne dele zapisovalne naprave: enoto v vozilu, tipalo gibanja, zunanjo GNSS opremo in tahografske kartice.

(432) V izjemnih okoliščinah, ko organi za varnostno certificiranje zavrnejo certificiranje nove opreme zaradi zastarelosti varnostnih mehanizmov, se homologacija še naprej podeli samo v teh posebnih in izjemnih okoliščinah in ko ni nobene druge rešitve, skladne z Uredbo.

(433) V takih okoliščinah zadevna država članica nemudoma obvesti Evropsko komisijo, ki v dvanajstih koledarskih mesecih od podelitve homologacije sproži postopek, s katerim zagotovi, da se ponovno vzpostavi prvotna raven varnosti.

8.3 **Potrdilo o funkcionalnosti**

(434) Vložnik zahtevka za homologacijo homologacijskemu organu države članice predloži vsa gradiva in dokumentacijo, za katere ta organ meni, da so potrebna.

(435) Proizvajalci v enem mesecu od datuma zahtevka zagotovijo ustrezne vzorce izdelkov, prijavljenih za homologacijo, in s tem povezano dokumentacijo, ki jo zahtevajo laboratoriji, imenovani za opravljanje preskusov delovanja. Stroške, ki nastanejo zaradi tega zahtevka, krije prosilec. Laboratoriji zaupno obravnavajo vse poslovno občutljive informacije.

(436) Potrdilo o funkcionalnosti se izda proizvajalcu šele po tem, ko so uspešno opravljeni vsaj vsi preskusi delovanja, predpisani v Dodatku 9.

(437) Potrdilo o funkcionalnosti izda homologacijski organ. To potrdilo poleg imena prejemnika in identifikacije modela navaja tudi podroben seznam opravljenih preskusov in doseženih rezultatov.

(438) V potrdilu o funkcionalnosti katerega koli sestavnega dela zapisovalne naprave so navedene tudi homologacijske številke vseh drugih homologiranih združljivih sestavnih delov zapisovalne naprave.

(439) V potrdilu o funkcionalnosti katerega koli sestavnega dela zapisovalne naprave so navedeni standardi ISO in CEN, v skladu s katerimi je bil potrjen funkcionalni vmesnik.

8.4 **Potrdilo o interoperabilnosti**

(440) Preskuse interoperabilnosti se opravijo v enem samem laboratoriju, za katerega je pristojna in odgovorna Evropska komisija.

(441) Laboratorij registrira zahtevke proizvajalcev za preskuse interoperabilnosti v vrstnem redu njihove predložitve.

(442) Zahtevek se uradno registrira šele takrat, ko laboratorij razpolaga z:

— vsemi gradivi in dokumentacijo, potrebnimi za te preskuse interoperabilnosti,

▼B

— ustreznim potrdilom o varnosti,

— ustreznim potrdilom o funkcionalnosti.

O datumu registracije zahtevka se obvesti proizvajalca.

(443) Laboratorij ne opravi nobenih preskusov interoperabilnosti zapisovalne naprave ali tahografske kartice, za katero še nista izdana potrdilo o varnosti in potrdilo o funkcionalnosti, razen v izjemnih okoliščinah, opisanih v zahtevi 432.

(444) Proizvajalec, ki vloži zahtevek za preskuse interoperabilnosti, laboratoriju, odgovornemu za te preskuse, prepusti na razpolago vsa gradiva in dokumentacijo, ki jih je predložil za izvedbo preskusov.

(445) Preskusi interoperabilnosti se v skladu z določbami Dodatka 9 k tej prilogi opravijo za vsako posamezno vrsto zapisovalne naprave ali tahografske kartice:

— za katero homologacija še velja, ali

— za katero se homologacija opravlja in ki ima veljavno potrdilo o interoperabilnosti.

(446) Preskusi interoperabilnosti zajemajo vse generacije zapisovalnih naprav ali tahografskih kartic, ki se še uporabljajo.

(447) Laboratorij potrdilo o interoperabilnosti proizvajalcu izda šele po uspešno opravljenih vseh zahtevanih preskusih interoperabilnosti.

(448) Če pri eni ali več zapisovalnih napravah ali tahografskih karticah preskusi skupne uporabnosti niso uspešni, laboratorij proizvajalcu ne izda potrdila o interoperabilnosti, dokler ta ne izvede potrebnih sprememb in njihovi izdelki preskuse interoperabilnosti uspešno prestanejo. Laboratorij ob pomoči proizvajalca, ki ga napaka glede interoperabilnosti zadeva, ugotovi vzrok težave in poskuša pomagati proizvajalcu pri iskanju tehnične rešitve. V primerih, ko proizvajalec spremeni svoj izdelek, mora na svojo odgovornost pri ustreznih organih ugotoviti, ali potrdilo o varnosti in funkcionalnosti za ta izdelek še veljata.

(449) Potrdilo o interoperabilnosti velja šest mesecev. Če proizvajalec v tem času ne pridobi ustreznega certifikata o homologaciji, se potrdilo prekliče. Ta certifikat proizvajalec posreduje homologacijskemu organu države članice, ki je izdal potrdilo o funkcionalnosti.

(450) Nobenega elementa, ki bi bil lahko vzrok napake glede interoperabilnosti, ni dopustno uporabiti za doseganje dobička ali prevladujočega položaja.

8.5 **Certifikat o homologaciji**

(451) Homologacijski organ države članice izda certifikat o homologaciji takoj, ko ima vsa tri zahtevana potrdila.

▼B

(452) V certifikatu o homologaciji katerega koli sestavnega dela zapisovalne naprave so navedene tudi homologacijske številke vseh drugih homologiranih vrst interoperabilnih zapisovalnih naprav.

(453) Ko izda certifikat o homologaciji proizvajalcu, homologacijski organ pošlje kopijo certifikata tudi laboratoriju, pristojnemu za preskuse interoperabilnosti.

(454) Laboratorij, pristojen za preskuse interoperabilnosti, vzdržuje javno spletno stran, na kateri objavlja posodobljeni seznam modelov zapisovalnih naprav ali tahografskih kartic:

— za katere so registrirani zahtevki za preskuse interoperabilnosti,

— za katere je bilo izdano potrdilo o interoperabilnosti (tudi začasno),

— za katere so bili izdani certifikati o homologaciji.

8.6 **Izredni postopek: prva potrdila o interoperabilnosti za zapisovalne naprave in tahografske kartice druge generacije**

(455) Dokler ne pretečejo štirje meseci od izdaje potrdil o interoperabilnosti za prvih nekaj modelov zapisovalnih naprav in tahografskih kartic (vozniških in nadzornih kartic ter kartic servisne delavnice in kartic podjetja) druge generacije, bo vsako izdano potrdilo o interoperabilnosti (vključno s prvimi, ki bodo izdani) pri zahtevkih, registriranih v tem obdobju, štelo za začasno.

(456) Če bodo po izteku tega obdobja vsi obravnavani izdelki vzajemno interoperabilni, bodo vsa ustrezna potrdila o interoperabilnosti postala dokončna.

(457) Če bodo v tem obdobju ugotovljene napake glede interoperabilnosti, laboratorij, pristojen za preskuse interoperabilnosti, ob pomoči vseh zadevnih proizvajalcev ugotovi vzroke težav in te proizvajalce pozove k izvedbi potrebnih sprememb.

(458) Če bodo tudi po koncu tega obdobja kakšne težave v zvezi z interoperabilnostjo ostale nerešene, laboratorij, pristojen za preskuse interoperabilnosti, v sodelovanju z zadevnimi proizvajalci in homologacijskimi organi, ki so izdali ustrezna potrdila o funkcionalnosti, ugotovi vzroke napak glede interoperabilnosti in navede, katere spremembe bi moral izvesti vsak od zadevnih proizvajalcev. Iskanje tehničnih rešitev lahko traja največ dva meseca; če v tem času ni najdena skupna rešitev, Komisija po posvetovanju z laboratorijem, pristojnim za preskuse interoperabilnosti, odloči, katerim napravam in tahografskim karticam se izdajo dokončna potrdila o interoperabilnosti, in svojo odločitev obrazloži.

(459) Vsi zahtevki za preskuse interoperabilnosti, ki jih laboratorij registrira v času od konca štirimesečnega obdobja po izdaji prvega začasnega potrdila o interoperabilnosti do dne odločitve Komisije, omenjene v zahtevi 455, se odložijo do rešitve začetnih težav glede interoperabilnosti. Ti zahtevki se nato obravnavajo v vrstnem redu njihove registracije.

▼B

Dodatek 1

SLOVAR PODATKOV

KAZALO

1. UVOD

1.1. Pristop pri opredelitvi podatkovnih tipov

1.2. Sklici

2. OPREDELITVE PODATKOVNIH TIPOV

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. Certifikat

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. Hitrost

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. OPREDELITVE OBMOČIJ VREDNOSTI IN VELIKOSTI

4. NABORI ZNAKOV

5. KODIRANJE

6. IDENTIFIKATORJI OBJEKTA IN IDENTIFIKATORJI APLIKACIJE

6.1. Identifikatorji objekta

6.2. Identifikatorji aplikacije

1. UVOD

Ta dodatek določa podatkovne formate, podatkovne elemente in podatkovne strukture, ki se uporabljajo na zapisovalni napravi in tahografskih karticah.

1.1. **Pristop pri opredelitvi podatkovnih tipov**

V tem dodatku se za opredelitev podatkovnih tipov uporablja abstraktni sintaktični zapis ASN.1. Ta zapis omogoča enostavno in strukturirano opredeljevanje podatkov, hkrati pa ne predpisuje pravil kodiranja, ki so odvisna od aplikacije in okolja.

Dogovori za poimenovanja vrst ASN.1 so v skladu s standardom ISO/IEC 8824-1. To pomeni, da:

— kadar je mogoče, je podatkovni tip nakazan že z izbranim imenom,

— kadar je podatkovni tip sestavljen iz drugih podatkovnih tipov, je ime podatkovnega tipa enovit niz abecednih znakov, ki se začne z veliko začetnico, velike začetnice v okviru tega niza pa posredujejo ustrezni pomen,

— v splošnem so imena podatkovnih tipov povezana z imeni podatkovnih tipov, iz katerih so sestavljena, napravo, v katerih so ti podatki shranjeni, in funkcijami, povezanimi s temi podatki.

Če je določen podatkovni tip po ASN.1 že opredeljen v okviru kakega drugega standarda in če je relevanten za uporabo pri zapisovalni napravi, je tak tip po ASN.1 opredeljen v tem dodatku.

Da se omogoči uporaba več pravil kodiranja, so določeni tipi po ASN.1 v tem dodatku omejeni z identifikatorji območij vrednosti. Identifikatorji območij vrednosti so opredeljeni v odstavku 3 in Dodatku 2.

1.2. **Sklici**

V tem dodatku so uporabljeni naslednji viri:

ISO 639	Koda za predstavljanje imen jezikov. Prva izdaja: 1988.

▼B

ISO 3166	Kode za predstavljanje imen držav in njihovih podrejenih enot – 1. del: Kode držav, 2013.
ISO 3779	Cestna vozila – Identifikacijska številka vozila (VIN) – Vsebina in struktura. 2009
ISO/IEC 7816-5	Identifikacijski dokumenti – Kartice z integriranim vezjem – 5. del: Registracija ponudnikov aplikacije. Druga izdaja: 2004.
ISO/IEC 7816-6	Identification cards – Integrated circuit(s) cards with contacts – Part 6: Interindustry data elements, 2004 + tehnični popravek 1: 2006
ISO/IEC 8824-1	Information technology – Abstract Syntax Notation One (ASN.1): Specification of basic notation. 2008 + Technical Corrigendum 1: 2012 and Technical Corrigendum 2: 2014.
ISO/IEC 8825-2	Information technology – ASN.1 encoding rules: Specification of Packed Encoding Rules (PER). 2008.
ISO/IEC 8859-1	Informacijska tehnologija – Nabori grafičnih znakov, kodiranih z enim 8-bitnim zlogom – 1. del: Latinična abeceda št. 1. Prva izdaja: 1998.
ISO/IEC 8859-7	Information technology – 8 bit single-byte coded graphic character sets – Part 7: Latin/Greek alphabet. 2003.
ISO 16844-3	Road vehicles – Tachograph systems – Motion Sensor Interface. 2004 + Technical Corrigendum 1: 2006..
TR-03110-3	BSI / ANSSI Tehnične smernice TR-03110-3, Napredni varnostni mehanizmi za strojno berljive potne listine in varnostni ključ eIDAS – 3. del, Skupne specifikacije, različica 2.20, 3. februar 2015

2. OPREDELITVE PODATKOVNIH TIPOV

Pri vsakem od podatkovnih tipov v nadaljevanju je privzeta vrednost za podatkovni element „neznano“ ali „se ne uporablja“, zapolnjen z bajti ‘FF’.

Vsi podatkovni tipi se uporabljajo za aplikacije prve in druge generacije, razen če je drugače navedeno.

2.1. **ActivityChangeInfo**

Ta podatkovni tip omogoča kodiranje v okviru dvobajtne besede, stanja reže ob času 00:00 in/ali stanja voznika v času 00:00 in/ali spremembe dejavnosti in/ali spremembe stanja vožnje in/ali spremembe stanja kartice za voznika ali sovoznika. Ta podatkovni tip je povezan z zahtevami 105, 266, 291, 320, 321, 343 in 344 iz Priloge 1C.

```
ActivityChangeInfo ::= OCTET STRING (SIZE(2))
```

Dodeljena vrednost – oktetno poravnano: ‘scpaatttttttttt’ B (16 bitov)

Za zapise v podatkovnem spominu (ali status reže)

‘s’B	Reža:
	‘0’B: DRIVER (VOZNIK),
	‘1’B: CO-DRIVER (SOVOZNIK),

▼B

‘c’B	Stanje vožnje: ‘0’B: SINGLE (POSAMEZNIK), ‘1’B: CREW (POSADKA),
‘p’B	Stanje vozniške kartice (ali kartice servisne delavnice) v ustrezni reži: ‘0’B: INSERTED (VSTAVLJENA), kartica je vstavljena, ‘1’B: NOT INSERTED (NI VSTAVLJENA), ni vstavljena nobena kartica (ali pa je kartica izvlečena),
‘aa’B	Dejavnost ‘00’B: BREAK/REST (ODMOR/POČITEK), ‘01’B: AVAILABILITY (RAZPOLOŽLJIVOST), ‘10’B: WORK (DELO), ‘11’B: DRIVING (VOŽNJA),
‘ttttttttttt’B	Čas spremembe: število minut od 00.00 v danem dnevu.

Za zapise na vozniško kartico (ali kartico servisne delavnice) (in stanje voznika):

‘s’B	Reža (ni relevantno, kadar je ‘p’ = 1, razen, kakor je navedeno v spodnji opombi): ‘0’B: DRIVER (VOZNIK), ‘1’B: CO-DRIVER (SOVOZNIK),
‘c’B	Stanje vožnje (primer ‘p’ = 0) ali Naslednje stanje dejavnosti (primer ‘p’ = 1): ‘0’B: SINGLE (POSAMEZNIK), ‘0’B: UNKNOWN (NEZNANO) ‘1’B: CREW (POSADKA), ‘1’B: KNOWN (ZNANO) (= vneseno ročno)
‘p’B	Stanje kartice: ‘0’B: INSERTED (VSTAVLJENA), kartica je vstavljena v zapisovalno napravo, ‘1’B: NOT INSERTED (NI VSTAVLJENA), kartica ni vstavljena (ali pa je izvlečena),
‘aa’B	Dejavnost (ni relevantno, kadar je ‘p’ = 1 in ‘c’ = 0, razen, kakor je navedeno v spodnji opombi): ‘00’B: BREAK/REST (ODMOR/POČITEK), ‘01’B: AVAILABILITY (RAZPOLOŽLJIVOST), ‘10’B: WORK (DELO), ‘11’B: DRIVING (VOŽNJA),
‘ttttttttttt’B	Čas spremembe: število minut od 00.00 v danem dnevu.

▼B

Opomba v primeru ‘izvleka kartice’:

Kadar se kartica odstrani:

— ‘s’ je relevantna in kaže režo, iz katere je kartica odstranjena,

— ‘c’ mora biti nastavljen na 0,

— ‘p’ mora biti nastavljen na 1,

— ‘aa’ mora kodirati trenutno dejavnost, izbrano ob navedenem času.

Zaradi ročnega vnosa se lahko bita ‘c’ in ‘aa’ besede (shranjene na kartici) pozneje prepišeta, da odražata vnos.

2.2. **Address**

Naslov.

```
Address ::= SEQUENCE {
   codePage                          INTEGER (0..255),
   address                           OCTET STRING (SIZE(35))
}
```

codePage določa nabor znakov, opredeljenih v poglavju 4,

address je naslov, kodiran z navedenim naborom znakov.

2.3. **AESKey**

Druga generacija:

AES ključ z dolžino 128, 192 ali 256 bitov.

```
AESKey ::= CHOICE {
   aes128Key                         AES128Key,
   aes192Key                         AES192Key,
   aes256Key                         AES256Key
}
```

Dodeljena vrednost: ni podrobneje določena.

2.4. **AES128Key**

Druga generacija:

ključ AES128.

```
AES128Key ::= SEQUENCE {
   length                              INTEGER(0..255),
   aes128Key                           OCTET STRING (SIZE(16))
}
```

dolžina označuje dolžino ključa AES128 v oktetih.

aes128Key je ključ AES z dolžino 128 bitov.

Dodeljena vrednost:

dolžina ima vrednost 16.

▼B

2.5. **AES192Key**

Druga generacija:

ključ AES192.

```
AES192Key ::= SEQUENCE {
   length                              INTEGER(0..255),
   aes192Key                           OCTET STRING (SIZE(24))
}
```

dolžina označuje dolžino ključa AES192 v oktetih.

aes192Key je ključ AES z dolžino 192 bitov.

Dodeljena vrednost:

dolžina ima vrednost 24.

2.6. **AES256Key**

Druga generacija:

ključ AES256.

```
AES256Key ::= SEQUENCE {
   length                              INTEGER(0..255),
   aes256Key                           OCTET STRING (SIZE(32))
}
```

dolžina označuje dolžino ključa AES256 v oktetih.

aes256Key je ključ AES z dolžino 256 bitov.

Dodeljena vrednost:

dolžina ima vrednost 32.

2.7. **BCDString**

BCDString se uporablja za binarno kodirano predstavitev desetiških števil (predstavitev BCD). Ta podatkovni tip se uporablja za predstavitev ene desetiške številke v enem pol-oktetu (4 bitih). BCDString temelji na ISO/IEC 8824-1 „CharacterStringType“.

```
BCDString ::= CHARACTER STRING (WITH COMPONENTS {
   identification ( WITH COMPONENTS {
   fixed PRESENT }) })
```

BCD String uporablja zapis „hstring“. Skrajna leva šestnajstiška številka je najpomembnejši pol-oktet prvega okteta. Mnogokratnik okteta se tvori tako, da se vstavi pol-oktete z zaključnimi ničlami za mestom levega pol-okteta v prvem oktetu.

Dovoljene številke so: 0, 1, .. 9.

2.8. **CalibrationPurpose**

Koda, ki razloži, zakaj je bil nabor kalibracijskih parametrov zapisan. Ta podatkovni tip je povezan z zahtevama 097 in 098 iz Priloge 1B in zahtevo 119 iz Priloge 1C.

```
CalibrationPurpose ::= OCTET STRING (SIZE(1))
```

▼B

Dodeljena vrednost:

prva generacija:

‘00’H	rezervirana vrednost,
‘01’H	aktiviranje: zapis kalibracijskih parametrov, znanih ob času aktiviranja VU,
‘02’H	prva namestitev: prva kalibracija VU po njenem aktiviranju,
‘03’H	namestitev: prva kalibracija VU v vozilu, v katerem je trenutno nameščena,
‘04’H	redni kontrolni pregled.

Druga generacija:

poleg vrednosti za prvo generacijo se uporabljajo še naslednje vrednosti:

‘05’H	vnos registrske številke vozila s strani podjetja,
‘06’H	nastavljanje časa brez kalibracije,
‘07’H do ‘7F’H	RFU,
‘80’H do ‘FF’H	določi proizvajalec.

2.9. **CardActivityDailyRecord**

Na kartici shranjena informacija, povezana z voznikovimi dejavnostmi na določen koledarski dan. Ta podatkovni tip je povezan z zahtevami iz Priloge 1C 266, 291, 320 in 343.

```
CardActivityDailyRecord ::= SEQUENCE {
   activityPreviousRecordLength         INTEGER(0..CardActivityLengthRange),
   activityRecordLength                 INTEGER(0..CardActivityLengthRange),
   activityRecordDate                   TimeReal,
   activityDailyPresenceCounter         DailyPresenceCounter,
   activityDayDistance                  Distance,
   activityChangeInfo                   SET SIZE(1..1440) OF ActivityChangeInfo
}
```

activityPreviousRecordLength je celotna dolžina prejšnjega dnevnega zapisa v bajtih. Največja vrednost je dana z dolžino OCTET STRING, ki vsebuje te zapise (glej CardActivityLengthRange v odstavku 4 Dodatka 2). Kadar je ta zapis najstarejši dnevni zapis, mora biti vrednost activityPreviousRecordLength nastavljena na 0.

activityRecordLength je celotna dolžina tega zapisa v bajtih. Največja vrednost je podana z dolžino OCTET STRING, ki vsebuje te zapise.

activityRecordDate je datum zapisa.

▼B

activityDailyPresenceCounter je dnevni števec prisotnosti kartice za ta dan.

activityDayDistance je celotna prevožena pot na ta dan.

activityChangeInfo je množica podatkov ActivityChangeInfo za voznika za ta dan. Vsebuje lahko do največ 1 440 vrednosti (ena sprememba dejavnosti na minuto). Ta množica obvezno vsebuje tudi kodo activityChangeInfo voznikovega stanja ob 00.00.

2.10. **CardActivityLengthRange**

Število bajtov na vozniški kartici ali kartici servisne delavnice, ki so na voljo za hranjenje zapisov voznikovih dejavnosti.

```
CardActivityLengthRange ::= INTEGER(0..2^16-1)
```

Dodeljena vrednost: glej Dodatek 2.

2.11. **CardApprovalNumber**

Homologacijska številka kartice.

```
CardApprovalNumber ::= IA5String(SIZE(8))
```

Dodeljena vrednost:

homologacijska številka se navede, kakor je objavljena na ustreznem spletišču Komisije, tj. vključno z vezaji, če obstajajo. Homologacijska številka se poravna levo.

2.12. **CardCertificate**

Prva generacija:

certifikat javnega ključa kartice.

```
CardCertificate ::= Certificate
```

2.13. **CardChipIdentification**

Informacija, shranjena na kartici, povezana z identifikacijo integriranega vezja (IC) kartice (zahteva 249 v Prilogi 1C). icSerialNumber skupaj z icManufacturingReferences nedvoumno identificira čip kartice. icSerialNumber sama po sebi čipa kartice ne identificira nedvoumno.

```
CardChipIdentification ::= SEQUENCE {
   icSerialNumber                    OCTET STRING (SIZE(4)),
   icManufacturingReferences         OCTET STRING (SIZE(4))
}
```

icSerialNumber je serijska številka IC.

icManufacturingReferences je identifikator IC, ki ga določi proizvajalec.

2.14. **CardConsecutiveIndex**

Zaporedna tekoča številka kartice (opredelitev h).

```
CardConsecutiveIndex ::= IA5String(SIZE(1))
```

Dodeljena vrednost: (glej poglavje 7 Priloge 1C).

Vrstni red pri povečevanju: ‘0, …, 9, A, …, Z, a, …, z’

▼B

2.15. **CardControlActivityDataRecord**

Informacija, shranjena na vozniški kartici ali kartici servisne delavnice, povezana z zadnjim nadzorom voznika (zahteve 274, 299, 327 in 350 iz Priloge 1C).

```
CardControlActivityDataRecord ::= SEQUENCE {
   controlType                          ControlType,
   controlTime                          TimeReal,
   controlCardNumber                    FullCardNumber,
   controlVehicleRegistration           VehicleRegistrationIdentification,
   controlDownloadPeriodBegin           TimeReal,
   controlDownloadPeriodEnd             TimeReal
}
```

controlType je vrsta nadzora.

controlTime je datum in čas nadzora.

controlCardNumber je FullCardNumber inšpektorja, ki je opravil nadzor.

controlVehicleRegistration je registrska številka vozila, v zvezi s katerim je bil izveden nadzor, in država članica, v kateri je vozilo registrirano.

controlDownloadPeriodBegin in **controlDownloadPeriodEnd** je obdobje, za katerega so bili preneseni podatki, če je bil prenos opravljen.

2.16. **CardCurrentUse**

Informacija o dejanski uporabi kartice (zahteve 273, 298, 326 in 349 iz Priloge 1C).

```
CardCurrentUse ::= SEQUENCE {
   sessionOpenTime                      TimeReal,
   sessionOpenVehicle                   VehicleRegistrationIdentification
}
```

sessionOpenTime je čas, v katerem je bila kartica vstavljena za trenutno uporabo. Ob izvleku kartice se ta podatek nastavi na nič.

sessionOpenVehicle je identifikacija vozila, ki se trenutno uporablja, in se nastavi ob vstavitvi kartice. Ob izvleku kartice se ta podatek nastavi na nič.

2.17. **CardDriverActivity**

Informacija, shranjena na vozniški kartici ali kartici servisne delavnice, povezana z dejavnostmi voznika (zahteve 267, 268, 292, 293, 321 in 344 iz Priloge 1C).

```
CardDriverActivity ::= SEQUENCE {
   activityPointerOldestDayRecord       INTEGER(0.. CardActivityLengthRange-1),
   activityPointerNewestRecord          INTEGER(0.. CardActivityLengthRange-1),
   activityDailyRecords                 OCTET STRING
                                        (SIZE(CardActivityLengthRange))
}
```

activityPointerOldestDayRecord je specifikacija začetka pomnilniškega prostora (število bajtov od začetka niza) najstarejšega popolnega dnevnega zapisa v nizu activityDailyRecords. Največja vrednost je dana z dolžino niza.

▼B

activityPointerNewestRecord je specifikacija začetka pomnilniškega prostora (število bajtov od začetka niza) najnovejšega dnevnega zapisa v nizu activityDailyRecords. Največja vrednost je dana z dolžino niza.

activityDailyRecords je razpoložljivi prostor za hranjenje podatkov o voznikovih dejavnostih (podatkovna struktura: CardActivityDailyRecord) za vsak koledarski dan, na katerega je kartica uporabljena.

Dodeljena vrednost: ta oktetni niz se ciklično polni z zapisi CardActivityDailyRecord. Ob prvi uporabi se začne shranjevanje v prvi bajt niza. Vsi novi zapisi se pripnejo za koncem prejšnjega. Ko je niz poln, se shranjevanje nadaljuje v prvi bajt niza ne glede na prekinitev, ki zaradi tega nastane v podatkovnem elementu. Pred vstavitvijo novih podatkov o dejavnostih v niz (podaljšanjem tekočega activityDailyRecord ali vstavitvijo novega activityDailyRecord), ki bodo prepisali starejše podatke o dejavnostih, je treba posodobiti activityPointerOldestDayRecord, tako da ustreza novemu položaju najstarejšega popolnega dnevnega zapisa, activityPreviousRecordLength tega (novega) najstarejšega popolnega dnevnega zapisa pa nastaviti na 0.

2.18. **CardDrivingLicenceInformation**

Informacija, shranjena na vozniški kartici, povezana s podatki o imetnikovem vozniškem dovoljenju (zahtevi 259 in 284 iz Priloge 1C).

```
CardDrivingLicenceInformation ::= SEQUENCE {
   drivingLicenceIssuingAuthority       Name,
   drivingLicenceIssuingNation          NationNumeric,
   drivingLicenceNumber                 IA5String(SIZE(16))
}
```

drivingLicenceIssuingAuthority je organ, pristojen za izdajanje vozniških dovoljenj.

drivingLicenceIssuingNation je državna pripadnost organa, ki je izdal vozniško dovoljenje.

drivingLicenceNumber je številka vozniškega dovoljenja.

2.19. **CardEventData**

Informacija, shranjena na vozniški kartici ali kartici servisne delavnice, povezana z dogodki v zvezi z imetnikom kartice (zahteve 260, 285, 318 in 341 iz Priloge 1C).

```
CardEventData ::= SEQUENCE SIZE(6) OF {
   cardEventRecords                     SET SIZE(NoOfEventsPerType) OF
                                        CardEventRecord
}
```

CardEventData je niz, urejen po naraščajoči vrednosti EventFaultType, zapisov cardEventRecords (razen zapisov poskusov kršenja varnosti, ki so zbrani v zadnji množici niza).

cardEventRecords je množica zapisov dogodkov določene vrste (ali kategorije pri dogodkih poskusov kršenja varnosti).

▼B

2.20. **CardEventRecord**

Informacija, shranjena na vozniški kartici ali kartici servisne delavnice, povezana z dogodkom v zvezi z imetnikom kartice (zahteve 261, 286, 318 in 341 iz Priloge 1C).

```
CardEventRecord ::= SEQUENCE {
   eventType                          EventFaultType,
   eventBeginTime                     TimeReal,
   eventEndTime                       TimeReal,
   eventVehicleRegistration           VehicleRegistrationIdentification
}
```

eventType je vrsta dogodka.

eventBeginTime je datum in čas začetka dogodka.

eventEndTime je datum in čas konca dogodka.

eventVehicleRegistration je registrska številka vozila, v katerem je dogodek nastopil, in država članica, v kateri je vozilo registrirano.

2.21. **CardFaultData**

Informacija, shranjena na vozniški kartici ali kartici servisne delavnice, povezana z napakami v zvezi z imetnikom kartice (zahteve 263, 288, 318 in 341 iz Priloge 1C).

```
CardFaultData ::= SEQUENCE SIZE(2) OF {
   cardFaultRecords                   SET SIZE(NoOfFaultsPerType) OF
                                      CardFaultRecord
}
```

CardFaultData je niz množice zapisov napak v zapisovalni napravi, za njimi pa še množice zapisov napak na kartici.

cardFaultRecords je množica zapisov napak določene kategorije napak (zapisovalna naprava ali kartica).

2.22. **CardFaultRecord**

Informacija, shranjena na vozniški kartici ali kartici servisne delavnice, povezana z napako v zvezi z imetnikom kartice (zahteve 264, 289, 318 in 341 iz Priloge 1C).

```
CardFaultRecord ::= SEQUENCE {
   faultType                          EventFaultType,
   faultBeginTime                     TimeReal,
   faultEndTime                       TimeReal,
   faultVehicleRegistration           VehicleRegistrationIdentification
}
```

faultType je vrsta napake.

faultBeginTime je datum in čas začetka napake.

faultEndTime je datum in čas konca napake.

faultVehicleRegistration je registrska številka vozila, v katerem se je napaka zgodila, in država članica, v kateri je vozilo registrirano.

▼B

2.23. **CardIccIdentification**

Informacija, shranjena na kartici, povezana z identifikacijo integriranega vezja (IC) kartice (zahteva 248 iz Priloge 1C).

```
CardIccIdentification ::= SEQUENCE {
   clockStop                          OCTET STRING (SIZE(1)),
   cardExtendedSerialNumber           ExtendedSerialNumber,
   cardApprovalNumber                 CardApprovalNumber,
   cardPersonaliserID                 ManufacturerCode,
   embedderIcAssemblerId              EmbedderIcAssemblerId,
   icIdentifier                       OCTET STRING (SIZE(2))
}
```

clockStop je način Clockstop, opredeljen v Dodatku 2.

cardExtendedSerialNumber je edinstvena serijska številka kartice integriranega vezja, kot jo podrobno določa podatkovni tip ExtendedSerialNumber.

cardApprovalNumber je homologacijska številka kartice.

cardPersonaliserID je ID personalizatorja kartice, kodiran kot ManufacturerCode.

embedderIcAssemblerId kaže podatek o vgrajevalcu/sestavljalcu integriranega vezja.

icIdentifier je identifikator integriranega vezja na kartici in njegov izdelovalec, kot je opredeljen v ISO/IEC 7816-6.

2.24. **CardIdentification**

Informacija, shranjena na kartici, povezana z identifikacijo kartice (zahteve 255, 280, 310, 333, 359, 365, 371 in 377 iz Priloge 1C).

```
CardIdentification ::= SEQUENCE {
   cardIssuingMemberState             NationNumeric,
   cardNumber                         CardNumber,
   cardIssuingAuthorityName           Name,
   cardIssueDate                      TimeReal,
   cardValidityBegin                  TimeReal,
   cardExpiryDate                     TimeReal
}
```

cardIssuingMemberState je koda države članice, ki je izdala kartico.

cardNumber je številka kartice.

cardIssuingAuthorityName je ime organa, ki je izdal kartico.

cardIssueDate je datum izdaje kartice zdajšnjemu imetniku.

cardValidityBegin je datum začetka veljavnosti kartice.

cardExpiryDate je datum izteka veljavnosti kartice.

▼B

2.25. **CardMACertificate**

Druga generacija:

certifikat javnega ključa kartice za medsebojno avtentikacijo z enoto v vozilu. Struktura tega certifikata je določena v Dodatku 11.

```
CardMACertificate ::= Certificate
```

2.26. **CardNumber**

Številka kartice, kakor jo opredeljuje opredelitev g).

```
CardNumber ::= CHOICE {
   SEQUENCE {
      driverIdentification              IA5String(SIZE(14)),
      cardReplacementIndex              CardReplacementIndex,
      cardRenewalIndex                  CardRenewalIndex
   },
   SEQUENCE {
      ownerIdentification               IA5String(SIZE(13)),
      cardConsecutiveIndex              CardConsecutiveIndex,
      cardReplacementIndex              CardReplacementIndex,
      cardRenewalIndex                  CardRenewalIndex
   }
}
```

driverIdentification je edinstvena identifikacija voznika v državi članici.

ownerIdentification je edinstvena identifikacija podjetja, servisne delavnice ali nadzornega organa v državi članici.

cardConsecutiveIndex je indeks zaporedja kartice.

cardReplacementIndex je indeks nadomestitve kartice.

cardRenewalIndex je indeks podaljšanja kartice.

Prvi niz izbire je primeren za kodiranje številke vozniške kartice, drugi niz izbire pa za kodiranje številk kartic servisne delavnice, nadzornih kartic in kartic podjetja.

2.27. **CardPlaceDailyWorkPeriod**

Informacija, shranjena na vozniški kartici ali kartici servisne delavnice, povezana s kraji začetkov in/ali koncev dnevnih delovnih izmen (zahteve 272, 297, 325 in 348 iz Priloge 1C).

```
CardPlaceDailyWorkPeriod ::= SEQUENCE {
   placePointerNewestRecord    INTEGER(0 .. NoOfCardPlaceRecords-1),
   placeRecords                SET SIZE(NoOfCardPlaceRecords) OF PlaceRecord
}
```

placePointerNewestRecord je indeks zadnjega posodobljenega zapisa krajev.

Dodeljena vrednost: število, ki ustreza številu zapisa kraja; začne se z vrednostjo ‘0’ za prvi zapis kraja v strukturi.

placeRecords je množica zapisov z informacijami o vnesenih krajih.

▼B

2.28. **CardPrivateKey**

Prva generacija:

zasebni ključ kartice.

```
CardPrivateKey ::= RSAKeyPrivateExponent
```

2.29. **CardPublicKey**

Javni ključ kartice.

```
CardPublicKey ::= PublicKey
```

2.30. **CardRenewalIndex**

Indeks podaljšanja kartice (opredelitev i).

```
CardRenewalIndex ::= IA5String(SIZE(1))
```

Dodeljena vrednost: (glej poglavje VII te priloge).

‘0’ Prva izdaja.

Vrstni red pri povečevanju: ‘0, …, 9, A, …, Z’

2.31. **CardReplacementIndex**

Indeks nadomestitve kartice (opredelitev j).

```
CardReplacementIndex ::= IA5String(SIZE(1))
```

Dodeljena vrednost: (glej poglavje VII te priloge).

‘0’ Prvotna kartica.

Vrstni red pri povečevanju: ‘0, …, 9, A, …, Z’

2.32. **CardSignCertificate**

Druga generacija:

certifikat javnega ključa kartice za podpis. Struktura tega certifikata je določena v Dodatku 11.

```
CardSignCertificate ::= Certificate
```

2.33. **CardSlotNumber**

Koda za razločevanje med režama enote v vozilu.

```
CardSlotNumber ::= INTEGER {
   driverSlot                          (0),
   co-driverSlot                       (1)
}
```

Dodeljena vrednost: ni podrobneje določena.

2.34. **CardSlotsStatus**

Koda vrste kartic, vstavljenih v režo enote v vozilu.

```
CardSlotsStatus ::= OCTET STRING (SIZE(1))
```

▼B

Dodeljena vrednost – oktetno poravnano: ‘ccccdddd’B

‘cccc’B Identifikacija vrste kartice, vstavljene v sovoznikovi reži,

‘dddd’B Identifikacija vrste kartice, vstavljene v voznikovi reži,

z naslednjimi identifikacijskimi kodami:

‘0000’B ni vstavljena nobena kartica,

‘0001’B vstavljena je vozniška kartica,

‘0010’B vstavljena je kartica servisne delavnice,

‘0011’B vstavljena je nadzorna kartica,

‘0100’B vstavljena je kartica podjetja.

2.35. **CardSlotsStatusRecordArray**

Druga generacija:

CardSlotsStatus in metapodatki, kot se uporabljajo v protokolu za prenos.

```
CardSlotsStatusRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF CardSlotsStatus
}
```

recordType označuje vrsto zapisa (CardSlotsStatus). **Dodeljena vrednost**: glej RecordType.

recordSize je v bajtih izražena velikost CardSlotsStatus.

noOfRecords je število zapisov, ki jih vsebuje množica zapisov.

records je množica zapisov CardSlotsStatus.

2.36. **CardStructureVersion**

Koda, ki označuje različico uvedene strukture na tahografski kartici.

```
CardStructureVersion ::= OCTET STRING (SIZE(2))
```

Dodeljena vrednost: ‘aabb’H:

‘aa’H Indeks sprememb strukture.

‘00’H za aplikacije prve generacije

‘01’H za aplikacije druge generacije

‘bb’H Indeks sprememb pri uporabi podatkovnih elementov, opredeljenih za strukturo podano z višjim bajtom.

‘00’H za to različico aplikacij prve generacije

‘00’H za to različico aplikacij druge generacije

▼B

2.37. **CardVehicleRecord**

Informacija, shranjena na vozniški kartici ali kartici servisne delavnice, povezana z obdobjem uporabe vozila na določen koledarski dan (zahteve 269, 294, 322 in 345 iz Priloge 1C).

Prva generacija:

```
CardVehicleRecord ::= SEQUENCE {
   vehicleOdometerBegin                    OdometerShort,
   vehicleOdometerEnd                      OdometerShort,
   vehicleFirstUse                         TimeReal,
   vehicleLastUse                          TimeReal,
   vehicleRegistration                     VehicleRegistrationIdentification,
   vuDataBlockCounter                      VuDataBlockCounter
}
```

vehicleOdometerBegin je vrednost števca prevožene poti na začetku obdobja uporabe vozila.

vehicleOdometerEnd je vrednost števca prevožene poti ob koncu obdobja uporabe vozila.

vehicleFirstUse je datum in čas začetka obdobja uporabe vozila.

vehicleLastUse je datum in čas konca obdobja uporabe vozila.

vehicleRegistration je registrska številka vozila in država, v kateri je registrirano.

vuDataBlockCounter je vrednost VuDataBlockCounter ob zadnjem izpisu obdobja uporabe vozila.

Druga generacija:

```
CardVehicleRecord ::= SEQUENCE {
   vehicleOdometerBegin                    OdometerShort,
   vehicleOdometerEnd                      OdometerShort,
   vehicleFirstUse                         TimeReal,
   vehicleLastUse                          TimeReal,
   vehicleRegistration                     VehicleRegistrationIdentification,
   vuDataBlockCounter                      VuDataBlockCounter,
   vehicleIdentificationNumber             VehicleIdentificationNumber
}
```

Poleg elementov za prvo generacijo se uporablja še naslednji podatkovni element:

VehicleIdentificationNumber je identifikacijska številka vozila, ki se nanaša na vozilo kot celoto.

2.38. **CardVehiclesUsed**

Informacija, shranjena na vozniški kartici ali kartici servisne delavnice, povezana z vozili, ki jih uporablja imetnik kartice (zahteve 270, 295, 323 in 346 iz Priloge 1C).

```
CardVehiclesUsed := SEQUENCE {
   vehiclePointerNewestRecord          INTEGER(0..NoOfCardVehicleRecords-1),
   cardVehicleRecords                  SET SIZE(NoOfCardVehicleRecords) OF
                                       CardVehicleRecord
}
```

placePointerNewestRecord je indeks zadnjega posodobljenega zapisa vozila.

▼B

Dodeljena vrednost: število, ki ustreza številu zapisa vozila; začne se z vrednostjo ‘0’ za prvi zapis vozila v strukturi.

cardVehicleRecords je množica zapisov podatkov o uporabljenih vozilih.

2.39. **CardVehicleUnitRecord**

Druga generacija:

informacija, shranjena na vozniški kartici ali kartici servisne delavnice, povezana z uporabljeno enoto v vozilu (zahtevi 303 in 351 iz Priloge 1C).

```
CardVehicleUnitRecord ::= SEQUENCE {
   timeStamp                              TimeReal,
   manufacturerCode                       ManufacturerCode,
   deviceID                               INTEGER(0..255),
   vuSoftwareVersion                      VuSoftwareVersion
}
```

timeStamp je datum in čas začetka obdobja uporabe enote v vozilu (tj. prve vstavitve kartice v enoto v vozilu v danem obdobju).

manufacturerCode identificira proizvajalca enote v vozilu.

deviceID identificira vrsto enote v vozilu proizvajalca. Vrednost določi proizvajalec.

vuSoftwareVersion je različica programske opreme enote v vozilu.

2.40. **CardVehicleUnitsUsed**

Druga generacija:

informacija, shranjena na vozniški kartici ali kartici servisne delavnice, povezana z enotami v vozilu, ki jih je uporabljal imetnik kartice (zahtevi 306 in 352 iz Priloge 1C).

```
CardVehicleUnitsUsed := SEQUENCE {
   vehicleUnitPointerNewestRecord       INTEGER(0..NoOfCardVehicleUnitRecords-1),
   cardVehicleUnitRecords               SET SIZE(NoOfCardVehicleUnitRecords) OF
                                        CardVehicleUnitRecord
}
```

vehicleUnitPointerNewestRecord je indeks zadnjega posodobljenega zapisa enote v vozilu.

Dodeljena vrednost: število, ki ustreza številu zapisa enot v vozilu; začne se z vrednostjo ‘0’ za prvi zapis enote v vozilu v strukturi.

cardVehicleUnitRecords je množica zapisov podatkov o uporabljenih enotah v vozilu.

2.41. **Certifikat**

Certifikat javnega ključa, ki ga je izdal certifikacijski organ.

Prva generacija:

```
Certificate ::= OCTET STRING (SIZE(194))
```

▼B

Dodeljena vrednost: digitalni podpis z delno obnovljeno vsebino CertificateContent v skladu z Dodatkom 11 „Skupni varnostni mehanizmi“: podpis (128 bajtov) || ostanek javnega ključa (58 bajtov) || oznaka certifikacijskega organa (8 bajtov).

Druga generacija:

```
Certificate ::= OCTET STRING (SIZE(204..341))
```

Dodeljena vrednost: glej Dodatek 11.

2.42. **CertificateContent**

Prva generacija:

(berljiva) vsebina certifikata javnega ključa v skladu z Dodatkom 11 „Skupni varnostni mehanizmi“.

```
CertificateContent ::= SEQUENCE {
   certificateProfileIdentifier          INTEGER(0..255),
   certificationAuthorityReference       KeyIdentifier,
   certificateHolderAuthorisation        CertificateHolderAuthorisation,
   certificateEndOfValidity              TimeReal,
   certificateHolderReference            KeyIdentifier,
   publicKey                             PublicKey
}
```

certificateProfileIdentifier je različica ustreznega certifikata.

Dodeljena vrednost: ‘01h’ za to različico.

certificationAuthorityReference identificira certifikacijski organ, ki je izdal certifikat. Sklicuje se tudi na javni ključ tega certifikacijskega organa.

certificateHolderAuthorisation identificira pravice imetnika certifikata.

certificateEndOfValidity je datum administrativnega izteka veljavnosti certifikata.

certificateHolderReference identificira imetnika certifikata. Vsebuje tudi sklic na njegov javni ključ.

publicKey je javni ključ, certificiran s tem certifikatom.

2.43. **CertificateHolderAuthorisation**

Identifikacija pravic imetnika certifikata.

```
CertificateHolderAuthorisation ::= SEQUENCE {
   tachographApplicationID               OCTET STRING(SIZE(6))
   equipmentType                         EquipmentType
}
```

Prva generacija:

tachographApplicationID je identifikator tahografske aplikacije.

Dodeljena vrednost: ‘FFh’ ‘54h’ ‘41h’ ‘43h’ ‘48h’ ‘4Fh’. Ta AID je lastniški neregistrirani identifikator aplikacije v skladu z ISO/IEC 7816-5.

equipmentType je identifikacija vrste naprave, za katero je namenjen certifikat.

Dodeljena vrednost: v skladu s podatkovnim tipom EquipmentType. **0**, če je imetnik certifikata država članica.

▼B

Druga generacija:

tachographApplicationID označuje 6 najpomembnejših bajtov identifikatorja aplikacije tahografske kartice druge generacije (AID). AID za aplikacijo tahografske kartice je določen v poglavju 6.2.

Dodeljena vrednost: ‘FF 53 4D 52 44 54’.

equipmentType je identifikacija vrste naprave, kot je določena za drugo generacijo, za katero je namenjen certifikat.

Dodeljena vrednost: v skladu s podatkovnim tipom EquipmentType.

2.44. **CertificateRequestID**

Edinstvena identifikacija zahtevka za certifikat. Če v času tvorbe certifikata ni znana serijska številka enote v vozilu, za katero je ključ namenjen, se lahko uporabi tudi kot identifikator javnega ključa enote v vozilu.

```
CertificateRequestID ::= SEQUENCE{
   requestSerialNumber                  INTEGER(0..2^32-1),
   requestMonthYear                     BCDString(SIZE(2)),
   crIdentifier                         OCTET STRING(SIZE(1)),
   manufacturerCode                     ManufacturerCode
}
```

requestSerialNumber je serijska številka zahtevka za certifikat, edinstvena za proizvajalca in mesec spodaj.

requestMonthYear je identifikacija meseca in leta zahtevka za certifikat.

Dodeljena vrednost: BCD-kodirana mesec (dve števki) in leto (zadnji dve števki).

crIdentifier: je identifikator, s katerim se zahtevek za certifikat loči od podaljšane serijske številke.

Dodeljena vrednost: ‘FFh’.

manufacturerCode: je številska koda proizvajalca, ki zahteva certifikat.

2.45. **CertificationAuthorityKID**

Identifikator javnega ključa certifikacijskega organa (države članice ali EU).

```
CertificationAuthorityKID ::= SEQUENCE{
   nationNumeric                        NationNumeric,
   nationAlpha                          NationAlpha,
   keySerialNumber                      INTEGER(0..255),
   additionalInfo                       OCTET STRING(SIZE(2)),
   caIdentifier                         OCTET STRING(SIZE(1))
}
```

nationNumeric je številska koda države certifikacijskega organa.

nationAlpha je alfanumerična koda države certifikacijskega organa.

▼B

keySerialNumber je serijska številka, po kateri se v primeru sprememb ključev med seboj ločijo različni ključi certifikacijskega organa.

additionalInfo je dvobajtno polje za dodatne kode (značilne za certifikacijski organ).

caIdentifier je identifikator, po katerem se identifikator ključa certifikacijskega organa loči od drugih identifikatorjev ključev.

Dodeljena vrednost: ‘01h’.

2.46. **CompanyActivityData**

Informacija, shranjena na kartici podjetja, povezana z dejavnostmi, opravljenimi s kartico (zahtevi 373 in 379 iz Priloge 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 je indeks zadnjega posodobljenega zapisa companyActivityRecord.

Dodeljena vrednost: število, ki ustreza številu zapisa dejavnosti podjetja; začne se z vrednostjo ‘0’ za prvi zapis dejavnosti podjetja v strukturi.

companyActivityRecords je množica vseh zapisov dejavnosti podjetja.

companyActivityRecord je niz informacij, povezanih z eno dejavnostjo podjetja.

companyActivityType je vrsta dejavnosti podjetja.

companyActivityTime je datum in čas dejavnosti podjetja.

cardNumberInformation je številka kartice in država izdajateljica kartice, s katere so bili preneseni podatki, če je relevantno.

vehicleRegistrationInformation je registrska številka vozila in država, v kateri je registrirano, za katero so bili preneseni podatki, oziroma je bila blokada vklopljena ali izklopljena.

downloadPeriodBegin in **downloadPeriodEnd** je obdobje, preneseno iz enote v vozilu, če je relevantno.

2.47. **CompanyActivityType**

koda dejavnosti, ki jo je opravilo podjetje s svojo kartico podjetja.

```
CompanyActivityType ::= INTEGER {
   card downloading                  (1),
   VU downloading                    (2),
   VU lock-in                        (3),
   VU lock-out                       (4)
}
```

▼B

2.48. **CompanyCardApplicationIdentification**

Informacija, shranjena na kartici podjetja, povezana z identifikacijo uporabe kartice (zahtevi 369 in 375 iz Priloge 1C).

```
CompanyCardApplicationIdentification ::= SEQUENCE {
   typeOfTachographCardId              EquipmentType,
   cardStructureVersion                CardStructureVersion,
   noOfCompanyActivityRecords          NoOfCompanyActivityRecords
}
```

typeOfTachographCardId določa uporabljeno vrsto kartice.

cardStructureVersion določa različico uporabljene strukture na kartici.

noOfCompanyActivityRecords je število zapisov dejavnosti podjetja, ki jih lahko hrani kartica.

2.49. **CompanyCardHolderIdentification**

Informacija, shranjena na kartici podjetja, povezana z identifikacijo imetnika kartice (zahtevi 372 in 378 iz Priloge 1C).

```
CompanyCardHolderIdentification ::= SEQUENCE {
   companyName                         Name,
   companyAddress                      Address,
   cardHolderPreferredLanguage         Language
}
```

companyName je ime podjetja, ki je imetnik kartice.

companyAddress je naslov podjetja, ki je imetnik kartice.

cardHolderPreferredLanguage je izbrani jezik imetnika kartice.

2.50. **ControlCardApplicationIdentification**

Informacija, shranjena na nadzorni kartici, povezana z identifikacijo aplikacije kartice (zahtevi 357 in 363 iz Priloge 1C).

```
ControlCardApplicationIdentification ::= SEQUENCE {
   typeOfTachographCardId              EquipmentType,
   cardStructureVersion                CardStructureVersion,
   noOfControlActivityRecords          NoOfControlActivityRecords
}
```

typeOfTachographCardId določa uporabljeno vrsto kartice.

cardStructureVersion določa različico uporabljene strukture na kartici.

noOfControlActivityRecords je število zapisov nadzornih dejavnosti, ki jih lahko hrani kartica.

▼B

2.51. **ControlCardControlActivityData**

Informacija, shranjena na nadzorni kartici, povezana z nadzornimi dejavnostmi, opravljenimi s kartico (zahtevi 361 in 367 iz Priloge 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 je indeks zadnjega posodobljenega zapisa nadzornih dejavnosti.

Dodeljena vrednost: število, ki ustreza številu zapisa nadzornih dejavnosti; začne se z vrednostjo ‘0’ za prvi zapis nadzornih dejavnosti v strukturi.

controlActivityRecords je množica vseh zapisov nadzornih dejavnosti.

controlActivityRecord je niz informacij, povezanih z enim nadzorom.

controlType je vrsta nadzora.

controlTime je datum in čas nadzora.

controlledCardNumber je številka kartice in država izdajateljica kartice, ki se nadzoruje.

controlledVehicleRegistration je registrska številka vozila, v zvezi s katerim je bil izveden nadzor, in država, v kateri je registrirano.

controlDownloadPeriodBegin in **controlDownloadPeriodEnd** je obdobje, za katero se lahko prenesejo podatki.

2.52. **ControlCardHolderIdentification**

Informacija, shranjena na nadzorni kartici, povezana z identifikacijo imetnika kartice (zahtevi 360 in 366 iz Priloge 1C).

```
ControlCardHolderIdentification ::= SEQUENCE {
   controlBodyName                    Name,
   controlBodyAddress                 Address,
   cardHolderName                     HolderName,
   cardHolderPreferredLanguage        Language
}
```

controlBodyName je ime nadzornega organa imetnika kartice.

controlBodyAddress je naslov nadzornega organa imetnika kartice.

cardHolderName je priimek in ime(na) imetnika nadzorne kartice.

▼B

cardHolderPreferredLanguage je izbrani jezik imetnika kartice.

2.53. **ControlType**

Koda, ki označuje dejavnosti, opravljene med nadzorom. Ta podatkovni tip je povezan z zahtevami 126, 274, 299, 327 in 350 iz Priloge 1C.

```
ControlType ::= OCTET STRING (SIZE(1))
```

Prva generacija:

dodeljena vrednost – oktetno poravnano: ‘cvpdxxxx’B (8 bitov)

‘c’B prenos podatkov s kartice:

‘0’B: med to nadzorno dejavnostjo podatki s kartice niso bili preneseni,

‘1’B: med to nadzorno dejavnostjo so bili podatki s kartice preneseni,

‘v’B prenos podatkov z VU:

‘0’B: med to nadzorno dejavnostjo podatki iz VU niso bili preneseni,

‘1’B: med to nadzorno dejavnostjo so bili podatki iz VU preneseni,

‘p’B tiskanje:

‘0’B: med to nadzorno dejavnostjo ni bilo opravljeno tiskanje,

‘1’B: med to nadzorno dejavnostjo je bilo opravljeno tiskanje,

‘d’B prikazovalnik:

‘0’B: med to nadzorno dejavnostjo ni bil uporabljen prikazovalnik,

‘1’B: med to nadzorno dejavnostjo je bil uporabljen prikazovalnik,

‘xxxx’B se ne uporablja.

Druga generacija:

dodeljena vrednost – oktetno poravnano: ‘cvpdexxx’B (8 bitov)

‘c’B prenos podatkov s kartice:

‘0’B: med to nadzorno dejavnostjo podatki s kartice niso bili preneseni,

‘1’B: med to nadzorno dejavnostjo so bili podatki s kartice preneseni,

‘v’B prenos podatkov z VU:

‘0’B: med to nadzorno dejavnostjo podatki iz VU niso bili preneseni,

‘1’B: med to nadzorno dejavnostjo so bili podatki iz VU preneseni,

‘p’B tiskanje:

‘0’B: med to nadzorno dejavnostjo ni bilo opravljeno tiskanje,

‘1’B: med to nadzorno dejavnostjo je bilo opravljeno tiskanje,

▼B

‘d’B	prikazovalnik:
	‘0’B: med to nadzorno dejavnostjo ni bil uporabljen prikazovalnik,
	‘1’B: med to nadzorno dejavnostjo je bil uporabljen prikazovalnik,
‘e’B	cestno preverjanje kalibracije:
	‘0’B: kalibracijski parametri niso bili preverjeni med to nadzorno dejavnostjo,
	‘1’B: kalibracijski parametri so bili preverjeni med to nadzorno dejavnostjo,
‘xxx’B	RFU.

2.54. **CurrentDateTime**

Trenutni datum in čas zapisovalne naprave.

```
CurrentDateTime ::= TimeReal
```

Dodeljena vrednost: ni podrobneje določena.

2.55. **CurrentDateTimeRecordArray**

Druga generacija:

trenutni datum in čas ter metapodatki, kot se uporabljajo v protokolu za prenos.

```
CurrentDateTimeRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF CurrentDateTime
}
```

recordType označuje vrsto zapisa (CurrentDateTime). **Dodeljena vrednost**: glej RecordType.

recordSize je v bajtih izražena velikost CurrentDateTime.

noOfRecords je število zapisov, ki jih vsebuje množica zapisov.

records je množica zapisov trenutnega datuma in časa.

2.56. **DailyPresenceCounter**

Števec, shranjen na vozniški kartici ali kartici servisne delavnice, ki se poveča za ena za vsak koledarski dan, v katerem je kartica vstavljena v VU. Ta podatkovni tip je povezan z zahtevami 266, 299, 320 in 343 iz Priloge 1C.

```
DailyPresenceCounter ::= BCDString(SIZE(2))
```

Dodeljena vrednost: zaporedno število z največjo vrednostjo = 9 999; po tem se začne spet od 0. Ob prvi izdaji kartice je število nastavljeno na 0.

▼B

2.57. **Datef**

Datum, zapisan v številskem formatu, primernem za tiskanje.

```
Datef ::= SEQUENCE {
   year        BCDString(SIZE(2)),
   month       BCDString(SIZE(1)),
   day         BCDString(SIZE(1))
}
```

Dodeljena vrednost:

llll	Leto
mm	Mesec
dd	Dan
‘00000000’H	izrecno ne označuje nobenega datuma.

2.58. **DateOfDayDownloaded**

Druga generacija:

datum in čas prenosa.

```
DateOfDayDownloaded ::= TimeReal
```

Dodeljena vrednost: ni podrobneje določena.

2.59. **DateOfDayDownloadedRecordArray**

Druga generacija:

datum in čas prenosa ter metapodatki, kot se uporabljajo v protokolu za prenos.

```
DateofDayDownloadedRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF
                                       DateOfDayDownloaded
}
```

recordType označuje vrsto zapisa (DateOfDayDownloaded). **Dodeljena vrednost**: glej RecordType.

recordSize je v bajtih izražena velikost CurrentDateTime.

noOfRecords je število zapisov, ki jih vsebuje množica zapisov.

records je množica zapisov datuma in časa prenosa podatkov.

2.60. **Distance**

Prevožena pot (rezultat izračuna razlike med dvema vrednostma števca prevožene poti v kilometrih).

```
Distance ::= INTEGER(0..2^16-1)
```

Dodeljena vrednost: binarno število brez predznaka. Vrednost v km v območju delovanja od 0 do 9 999 km.

2.61. **DriverCardApplicationIdentification**

Informacija, shranjena na vozniški kartici, povezana z identifikacijo aplikacije kartice (zahtevi 253 in 278 iz Priloge 1C).

▼B

Prva generacija:

```
DriverCardApplicationIdentification ::= SEQUENCE {
   typeOfTachographCardId              EquipmentType,
   cardStructureVersion                CardStructureVersion,
   noOfEventsPerType                   NoOfEventsPerType,
   noOfFaultsPerType                   NoOfFaultsPerType,
   activityStructureLength             CardActivityLengthRange,
   noOfCardVehicleRecords              NoOfCardVehicleRecords,
   noOfCardPlaceRecords                NoOfCardPlaceRecords
}
```

typeOfTachographCardId določa uporabljeno vrsto kartice.

cardStructureVersion določa različico uporabljene strukture na kartici.

noOfEventsPerType je število dogodkov posamezne vrste, ki jih lahko zapiše kartica.

noOfFaultsPerType je število napak posamezne vrste, ki jih lahko zapiše kartica.

activityStructureLength označuje število razpoložljivih bajtov za hranjenje zapisov dejavnosti.

noOfCardVehicleRecords je število zapisov vozila, ki jih lahko vsebuje kartica.

noOfCardPlaceRecords je število krajev, ki jih lahko zapiše kartica.

Druga generacija:

```
DriverCardApplicationIdentification ::= SEQUENCE {
   typeOfTachographCardId              EquipmentType,
   cardStructureVersion                CardStructureVersion,
   noOfEventsPerType                   NoOfEventsPerType,
   noOfFaultsPerType                   NoOfFaultsPerType,
   activityStructureLength             CardActivityLengthRange,
   noOfCardVehicleRecords              NoOfCardVehicleRecords,
   noOfCardPlaceRecords                NoOfCardPlaceRecords,
   noOfGNSSCDRecords                   NoOfGNSSCDRecords,
   noOfSpecificConditionRecords        NoOfSpecificConditionRecords
}
```

Poleg elementov za prvo generacijo se uporabljajo še naslednji podatkovni elementi:

noOfGNSSCDRecords je število zapisov neprekinjene vožnje GNSS, ki jih lahko hrani kartica.

noOfSpecificConditionRecords je število zapisov posebnih pogojev, ki jih lahko hrani kartica.

2.62. **DriverCardHolderIdentification**

Informacija, shranjena na vozniški kartici, povezana z identifikacijo imetnika kartice (zahtevi 256 in 281 iz Priloge 1C).

```
DriverCardHolderIdentification ::= SEQUENCE {
   cardHolderName                      HolderName,
   cardHolderBirthDate                 Datef,
   cardHolderPreferredLanguage         Language
}
```

▼B

cardHolderName je priimek in ime(na) imetnika vozniške kartice.

cardHolderBirthDate je datum rojstva imetnika vozniške kartice.

cardHolderPreferredLanguage je izbrani jezik imetnika kartice.

2.63. **DSRCSecurityData**

Druga generacija:

informacija v golem besedilu in MAC, ki se pošlje prek DSRC iz tahografa v daljinski čitalnik, za podrobnosti glej poglavje 13 Dela B iz Dodatka 11.

```
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
}
```

tag je del kodiranja DER-TLV in se nastavi na ‘81 10’ (glej poglavje 13 Dela B iz Dodatka 11).

currentDateTime je trenutni datum in čas enote v vozilu.

counter šteje sporočila RTM.

vuSerialNumber je serijska številka enote v vozilu.

dSRCMKVersionNumber je številka različice glavnega ključa DSRC, iz katerega so bili ustvarjeni ključi DSRC, specifični za VU.

tagLengthMac je oznaka in dolžina podatkovnega objekta MAC kot del kodiranja DER-TLV. Oznaka se nastavi na ‘8E’, dolžina kodira dolžino MAC v oktetih (glej poglavje 13 Dela B iz Dodatka 11).

mac je MAC, izračunan na podlagi sporočila RTM (glej poglavje 13 Dela B iz Dodatka 11).

2.64. **EGFCertificate**

Druga generacija:

certifikat javnega ključa zunanje GNSS opreme za vzajemno avtentikacijo z enoto v vozilu. Struktura tega certifikata je določena v Dodatku 11.

```
EGFCertificate ::= Certificate
```

▼B

2.65. **EmbedderIcAssemblerId**

Kaže podatek o vgrajevalcu IC.

```
EmbedderIcAssemblerId ::= SEQUENCE{
   countryCode                          IA5String(SIZE(2)),
   moduleEmbedder                       BCDString(SIZE(2)),
   manufacturerInformation              OCTET STRING(SIZE(1))
}
```

countryCode je dvočrkovna koda države vgrajevalca modula v skladu z ISO 3166.

moduleEmbedder identificira vgrajevalca modula.

manufacturerInformation za interno uporabo proizvajalca.

2.66. **EntryTypeDailyWorkPeriod**

Koda, po kateri se razlikujejo vnosi kraja in načini vnosa ob začetku in ob koncu dnevne delovne izmene.

Prva generacija

```
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)
}
```

Dodeljena vrednost: v skladu z ISO/IEC8824-1.

Druga generacija:

```
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)
}
```

Dodeljena vrednost: v skladu z ISO/IEC8824-1.

2.67. **EquipmentType**

Koda, po kateri se ločijo vrste naprave za tahografsko aplikacijo.

```
EquipmentType ::= INTEGER(0..255)
```

▼B

Prva generacija:

```
--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)
```

Dodeljena vrednost: v skladu z ISO/IEC8824-1.

Vrednost 0 je rezervirana za namen imenovanja države članice ali Evrope v polje certifikatov CHA.

Druga generacija:

enake vrednosti kot pri prvi generaciji se uporabljajo z naslednjimi dodatki:

```
--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)
```

Opomba: vrednosti za drugo generacijo za ploščico, pretvornik in zunanjo GNSS povezavo ter vrednosti za prvo generacijo za enoto v vozilu in tipalo gibanja se lahko uporabljajo v SealRecord, tj. če se uporablja.

2.68. **EuropeanPublicKey**

Prva generacija:

evropski javni ključ.

```
EuropeanPublicKey ::= PublicKey
```

2.69. **EventFaultRecordPurpose**

Koda z razlago, zakaj je bil dogodek ali napaka zapisan.

```
EventFaultRecordPurpose ::= OCTET STRING (SIZE(1))
```

Dodeljena vrednost:

'00'H	eden od 10 najnovejših (ali zadnjih) dogodkov ali napak
'01'H	najdaljši dogodek za enega od 10 zadnjih dni nastopov dogodkov
'02'H	eden od 5 najdaljših dogodkov v zadnjih 365 dneh
'03'H	zadnji dogodek za enega od 10 zadnjih dni nastopov dogodkov
'04'H	najresnejši dogodek za enega od 10 zadnjih dni nastopov dogodkov
'05'H	eden od 5 najresnejših dogodkov v zadnjih 365 dneh
'06'H	prvi dogodek ali napaka, ki je nastopila po zadnji kalibraciji
'07'H	aktivni/tekoči dogodek ali napaka
'08'H to '7F'H	RFU
'80'H to 'FF'H	določi proizvajalec

▼B

2.70. **EventFaultType**

Koda, ki označuje dogodek ali napako.

```
EventFaultType ::= OCTET STRING (SIZE(1))
```

Dodeljena vrednost:

Prva generacija:

'0x'H	Splošni dogodki
'00'H	Ni dodatnih podrobnosti
'01'H	Vstavitev neveljavne kartice
'02'H	Navzkrižje med karticami
'03'H	Časovno prekrivanje
'04'H	Vožnja brez ustrezne kartice
'05'H	Vstavitev kartice med vožnjo
'06'H	Zadnja seja s kartico nepravilno zaključena
'07'H	Prekoračitev hitrosti
'08'H	Izpad napajanja
'09'H	Napaka v podatkih o gibanju
'0A'H	Navzkrižje v gibanju vozila
'0B' to '0F'H	RFU
'1x'H	Dogodki poskusov kršenja varnosti, povezani z enoto v vozilu
'10'H	Ni dodatnih podrobnosti
'11'H	Neuspešna avtentikacija tipala gibanja
'12'H	Neuspešna avtentikacija tahografske kartice
'13'H	Nepooblaščena zamenjava tipala gibanja
'14'H	Napaka v celovitosti vhodnih podatkov s kartice
'15'H	Napaka v celovitosti shranjenih podatkov uporabnika
'16'H	Napaka pri notranjem prenosu podatkov
'17'H	Nepooblaščeno odprtje ohišja
'18'H	Sabotaža strojne opreme
'19'H to '1F'H	RFU
'2x'H	Dogodki poskusov kršenja varnosti, povezani s tipalom
'20'H	Ni dodatnih podrobnosti
'21'H	Neuspešna avtentikacija
'22'H	Napaka v celovitosti shranjenih podatkov
'23'H	Napaka pri notranjem prenosu podatkov
'24'H	Nepooblaščeno odprtje ohišja
'25'H	Sabotaža strojne opreme
'26'H to '2F'H	RFU
'3x'H	Napake zapisovalne naprave
'30'H	Ni dodatnih podrobnosti
'31'H	Notranja napaka VU
'32'H	Napaka na tiskalniku
'33'H	Napaka na prikazovalniku
'34'H	Napaka pri prenosu podatkov
'35'H	Napaka na tipalu
'36'H to '3F'H	RFU
'4x'H	Napake na kartici
'40'H	Ni dodatnih podrobnosti
'41'H to '4F'H	RFU
'50'H to '7F'H	RFU
'80'H to 'FF'H	Določi proizvajalec.

▼B

Druga generacija:

enake vrednosti kot pri prvi generaciji se uporabljajo z naslednjimi dodatki:

‘0B’H	Časovno navzkrižje (med GNSS in notranjo uro VU)
‘0C’ to ‘0F’H	RFU
‘5x’H	Napake, povezane z GNSS
‘50’H	Ni dodatnih podrobnosti
‘51’H	Notranja napaka GNSS sprejemnika
‘52’H	Zunanja napaka GNSS sprejemnika
‘53’H	Zunanja napaka GNSS komunikacije
‘54’H	Ni GNSS podatkov o položaju
‘55’H	Zaznavanje poskusov manipulacije GNSS
‘56’H	Certifikat zunanje GNSS opreme je potekel
‘57’H to ‘5F’H	RFU
‘6x’H	Napake, povezane z opremo za komunikacijo na daljavo
‘60’H	Ni dodatnih podrobnosti
‘61’H	Napaka na modulu za komunikacijo na daljavo
‘62’H	Napaka pri komunikaciji z modulom za komunikacijo na daljavo
‘63’H to ‘6F’H	RFU
‘7x’H	Napake vmesnika z ITS
‘70’H	Ni dodatnih podrobnosti
‘71’H to ‘7F’H	RFU

2.71. **ExtendedSealIdentifier**

Druga generacija:

podaljšani identifikator pečata edinstveno identificira pečat (zahteva 401 iz Priloge 1C).

```
ExtendedSealIdentifier ::= SEQUENCE{
   manufacturerCode                    OCTET STRING (SIZE(2)),
   sealIdentifier                      OCTET STRING (SIZE(6))
}
```

manufacturerCode je koda proizvajalca pečata.

sealIdentifier je identifikator za pečat, ki je glede na proizvajalca edinstven.

2.72. **ExtendedSerialNumber**

Edinstvena identifikacija opreme. Uporablja se lahko tudi kot identifikator opreme javnega ključa.

Prva generacija:

```
ExtendedSerialNumber ::= SEQUENCE{
   serialNumber                        INTEGER(0..2^32-1),
   monthYear                           BCDString(SIZE(2)),
   type                                OCTET STRING(SIZE(1)),
   manufacturerCode                    ManufacturerCode
}
```

serialNumber je serijska številka naprave, edinstvena za proizvajalca, vrsto naprave ter mesec in leto proizvodnje spodaj.

monthYear je identifikacija meseca in leta izdelave (ali dodelitve serijske številke).

▼B

Dodeljena vrednost: BCD-kodirana mesec (dve števki) in leto (zadnji dve števki).

type je identifikator vrste naprave.

Dodeljena vrednost: določi proizvajalec; vrednost ‘FFh’ je rezervirana.

manufacturerCode: je številska koda, ki identificira proizvajalca homologacijske opreme.

Druga generacija:

```
ExtendedSerialNumber ::= SEQUENCE{
   serialNumber                          INTEGER(0..2^32-1),
   monthYear                             BCDString(SIZE(2)),
   type                                  EquipmentType,
   manufacturerCode                      ManufacturerCode
}
```

serialNumber glej prvo generacijo.

monthYear glej prvo generacijo.

type označuje vrsto opreme.

manufacturerCode: glej prvo generacijo.

2.73. **FullCardNumber**

Koda, ki v celoti identificira tahografsko kartico.

```
FullCardNumber ::= SEQUENCE {
   cardType                              EquipmentType,
   cardIssuingMemberState                NationNumeric,
   cardNumber                            CardNumber
}
```

cardType je vrsta tahografske kartice.

cardIssuingMemberState je koda države članice, ki je izdala kartico.

cardNumber je številka kartice.

2.74. **FullCardNumberAndGeneration**

Druga generacija:

koda, ki v celoti identificira tahografsko kartico in njeno generacijo.

```
FullCardNumberAndGeneration ::= SEQUENCE {
   fullCardNumber                        FullCardNumber,
   generation                            Generation
}
```

fullcardNumber identificira tahografsko kartico.

generation označuje generacijo uporabljene tahografske kartice.

▼B

2.75. **Generation**

Druga generacija:

označuje generacijo uporabljenega tahografa.

```
Generation ::= INTEGER(0..255)
```

Dodeljena vrednost:

‘00’H	RFU
‘01’H	Prva generacija
‘02’H	Druga generacija
‘03’H .. ‘FF’H	RFU

2.76. **GeoCoordinates**

Druga generacija:

zemljepisne koordinate so kodirane kot cela števila. Ta cela števila so večkratniki kodiranja ±DDMM.M za zemljepisno širino in kodiranja ±DDDMM.M za zemljepisno dolžino. Tu ±DD oziroma ±DDD označuje stopinje in MM.M minute.

```
GeoCoordinates ::= SEQUENCE {
   latitude                                INTEGER(-90000..90001),
   longitude                               INTEGER(-180000..180001)
}
```

latitude je kodiran kot večkratnik (faktor 10) predstavitve ± DDMM.M.

longitude je kodiran kot večkratnik (faktor 10) predstavitve ± DDDMM.M.

2.77. **GNSSAccuracy**

Druga generacija:

točnost GNSS podatkov o položaju (opredelitev eee)). Ta točnost je kodirana kot celo število in je večkratnik (faktor 10) vrednosti X.Y, dobljene iz stavka GSA NMEA.

```
GNSSAccuracy ::= INTEGER(1..100)
```

2.78. **GNSSContinuousDriving**

Druga generacija:

informacija, shranjena na vozniški kartici ali kartici servisne delavnice, povezana z GNSS položajem vozila, če čas neprekinjene vožnje voznika doseže večkratnik treh ur (zahtevi 306 in 354 iz Priloge 1C).

```
GNSSContinuousDriving := SEQUENCE {
   gnssCDPointerNewestRecord               INTEGER(0..NoOfGNSSCDRecords -1),
   gnssContinuousDrivingRecords            SET SIZE(NoOfGNSSCDRecords) OF
                                           GNSSContinuousDrivingRecord
}
```

gnssCDPointerNewestRecord je indeks zadnjega posodobljenega GNSS zapisa neprekinjene vožnje.

▼B

Dodeljena vrednost: število, ki ustreza števcu GNSS zapisa neprekinjene vožnje; začne se z vrednostjo ‘0’ za prvi GNSS zapis neprekinjene vožnje v strukturi.

gnssContinuousDrivingRecords je množica podatkov, ki vsebujejo datum in čas, ko neprekinjena vožnja doseže večkratnik treh ur, in informacijo o položaju vozila.

2.79. **GNSSContinuousDrivingRecord**

Druga generacija:

informacija, shranjena na vozniški kartici ali kartici servisne delavnice, povezana z GNSS položajem vozila, če čas neprekinjene vožnje voznika doseže večkratnik treh ur (zahtevi 305 in 353 iz Priloge 1C).

```
GNSSContinuousDrivingRecord ::= SEQUENCE {
   timeStamp                                TimeReal,
   gnssPlaceRecord                          GNSSPlaceRecord
}
```

timeStamp je datum in čas, ko čas neprekinjene vožnje imetnika kartice doseže večkratnik treh ur.

gnssPlaceRecord vsebuje informacijo, povezano s položajem vozila.

2.80. **GNSSPlaceRecord**

Druga generacija:

informacija, povezana s položajem GNSS vozila (zahteve 108, 109, 110, 296, 305, 347 in 353 iz Priloge 1C).

```
GNSSPlaceRecord ::= SEQUENCE {
   timeStamp                                TimeReal,
   gnssAccuracy                             GNSSAccuracy,
   geoCoordinates                           GeoCoordinates
}
```

timeStamp je datum in čas, ko je bil določen GNSS položaj vozila.

gnssAccuracy je točnost podatka o GNSS položaju.

geoCoordinates je zapisana lokacija z uporabo GNSS.

2.81. **HighResOdometer**

Vrednost števca prevožene poti vozila: skupna prevožena pot vozila med premikanjem.

```
HighResOdometer ::= INTEGER(0..2^32-1)
```

▼B

Dodeljena vrednost: binarno število brez predznaka. Vrednost, v enotah 1/200 km, v območju od 0 do 21 055 406 km.

2.82. **HighResTripDistance**

Pot, prevožena na določeni vožnji ali etapi vožnje.

```
HighResTripDistance ::= INTEGER(0..2^32-1)
```

Dodeljena vrednost: binarno število brez predznaka. Vrednost, v enotah 1/200 km, v območju od 0 do 21 055 406 km.

2.83. **HolderName**

Priimek in ime(na) imetnika kartice.

```
HolderName ::= SEQUENCE {
   holderSurname                    Name,
   holderFirstNames                 Name
}
```

holderSurname je priimek imetnika. Priimek ne vključuje nazivov.

Dodeljena vrednost: če kartica ni osebna, vsebuje holderSurname isto informacijo kot companyName ali workshopName ali controlBodyName.

holderFirstNames so ime(na) in začetnice imetnika.

2.84. **InternalGNSSReceiver**

Druga generacija:

informacija o tem, ali je GNSS sprejemnik glede na enoto v vozilu notranji ali zunanji. ‘True’ pomeni, da je GNSS sprejemnik glede na enoto v vozilu notranji. ‘False’ pomeni, da je GNSS sprejemnik zunanji.

```
InternalGNSSReceiver ::= BOOLEAN
```

2.85. **K-ConstantOfRecordingEquipment**

Konstanta zapisovalne naprave (opredelitev m).

```
K-ConstantOfRecordingEquipment ::= INTEGER(0..2^16-1)
```

Dodeljena vrednost: število impulzov na kilometer v območju od 0 do 64 255 impulzov/km.

2.86. **KeyIdentifier**

Edinstveni identifikator javnega ključa, uporabljen za sklicevanje in izbiranje ključa. Identificira tudi imetnika ključa.

```
KeyIdentifier ::= CHOICE {
   extendedSerialNumber             ExtendedSerialNumber,
   certificateRequestID             CertificateRequestID,
   certificationAuthorityKID        CertificationAuthorityKID
}
```

▼B

Prva oblika je primerna za sklicevanje na javni ključ enote v vozilu ali na tahografski kartici.

Druga oblika je primerna za sklicevanje na javni ključ enote v vozilu (kadar v času tvorbe javnega ključa ni mogoče poznati serijske številke enote v vozilu).

Tretja oblika je primerna za sklicevanje na javni ključ države članice.

2.87. **KMWCKey**

Druga generacija:

ključ AES in njegova povezana različica ključa za povezovanje VU–tipalo gibanja. Za podrobnosti glej Dodatek 11.

```
KMWCKey ::= SEQUENCE {
   kMWCKey                                 AESKey,
   keyVersion                              INTEGER (SIZE(1))
}
```

kMWCKey je dolžina ključa AES, povezanega s ključem, ki se uporablja za povezovanje VU–tipalo gibanja.

keyVersion označuje različico ključa AES.

2.88. **Language**

Koda, ki identificira jezik.

```
Language ::= IA5String(SIZE(2))
```

Dodeljena vrednost: dvomestna koda z malimi črkami v skladu z ISO 639.

2.89. **LastCardDownload**

Datum in čas, shranjena na vozniški kartici, zadnjega prenosa podatkov (za namene, ki niso nadzorni), zahtevi 257 in 282 iz Priloge 1C. Ta datum lahko posodablja VU ali kak drug bralnik kartic.

```
LastCardDownload ::= TimeReal
```

Dodeljena vrednost: ni podrobneje določena.

2.90. **LinkCertificate**

Druga generacija:

certifikat,s katerim se povezujejo pari ključev evropskega certifikacijskega organa za korenske certifikate.

```
LinkCertificate ::= Certificate
```

2.91. **L-TyreCircumference**

Dejanski obseg pnevmatik (opredelitev u)).

```
L-TyreCircumference ::= INTEGER(0.. 2^16-1)
```

▼B

Dodeljena vrednost: binarno število brez predznaka, vrednost v enotah 1/8 mm v območju od 0 do 8 031 mm.

2.92. **MAC**

Druga generacija:

kriptografska kontrolna vsota dolžine 8, 12 ali 16 bajtov, ki ustreza nizom kod iz Dodatka 11.

```
MAC ::= CHOICE {
   mac8                                    OCTET STRING (SIZE(8)),
   mac12                                   OCTET STRING (SIZE(12)),
   mac16                                   OCTET STRING (SIZE(12))
}
```

2.93. **ManualInputFlag**

Koda, ki identificira, ali je imetnik kartice ob njeni vstavitvi ročno vnesel voznikove dejavnosti (zahteva 081 iz Priloge 1B in zahteva 102 iz Priloge 1C).

```
ManualInputFlag ::= INTEGER {
   noEntry                                 (0)
   manualEntries                           (1)
}
```

Dodeljena vrednost: ni podrobneje določena.

2.94. **ManufacturerCode**

Koda, ki identificira proizvajalca homologirane naprave.

```
ManufacturerCode ::= INTEGER(0..255)
```

Laboratorij, pristojen za preskuse interoperabilnosti, na svojem spletišču vodi in objavlja seznam kod proizvajalcev (zahteva 454 iz Priloge 1C).

ManufacturerCodes se na podlagi zahteve laboratoriju, pristojnemu za preskuse interoperabilnosti, začasno dodelijo razvijalcem tahografske opreme.

2.95. **ManufacturerSpecificEventFaultData**

Druga generacija:

kode o napaki, ki jih določi proizvajalec, olajšajo analizo napak in vzdrževanje enot v vozilu.

```
ManufacturerSpecificEventFaultData ::= SEQUENCE {
   manufacturerCode                        ManufacturerCode,
   manufacturerSpecificErrorCode           OCTET STRING(SIZE(3))
}
```

manufacturerCode identificira proizvajalca enote v vozilu.

manufacturerSpecificErrorCode je koda napake, ki jo določi proizvajalec.

▼B

2.96. **MemberStateCertificate**

Certifikat javnega ključa države članice, ki ga izda evropski certifikacijski organ.

```
MemberStateCertificate ::= Certificate
```

2.97. **MemberStateCertificateRecordArray**

Druga generacija:

certifikat države članice in metapodatki, kot se uporabljajo v protokolu za prenos.

```
MemberStateCertificateRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF
                                       MemberStateCertificate
}
```

recordType označuje vrsto zapisa (MemberStateCertificate). **Dodeljena vrednost**: glej RecordType.

recordSize je v bajtih izražena velikost MemberStateCertificate.

noOfRecords je število zapisov, ki jih vsebuje množica zapisov. Vrednost se nastavi na 1, saj so certifikati lahko različne dolžine.

records je množica certifikatov države članice.

2.98. **MemberStatePublicKey**

Prva generacija:

javni ključ države članice.

```
MemberStatePublicKey ::= PublicKey
```

2.99. **Name**

Naziv.

```
Name ::= SEQUENCE {
   codePage                            INTEGER (0..255),
   name                                OCTET STRING (SIZE(35))
}
```

codePage določa nabor znakov, opredeljenih v poglavju 4.

name je ime, kodirano z navedenim naborom znakov.

2.100. **NationAlpha**

Črkovna oznaka države je skladna z oznakami, ki se uporabljajo na vozilih v mednarodnem prometu (Dunajska konvencija Združenih narodov o cestnem prometu, 1968).

```
NationAlpha ::= IA5String(SIZE(3))
```

Kode Nation Alpha in številske kode so navedene na seznamu na spletišču laboratorija, imenovanega za opravljanje preskusov interoperabilnosti, kot je določeno v zahtevi 440 iz Priloge 1C.

▼B

2.101. **NationNumeric**

Številska oznaka države.

```
NationNumeric ::= INTEGER(0 .. 255)
```

Dodeljena vrednost: glej podatkovni tip 2.100 (NationAlpha)

Specifikacijo Nation Alpha ali Nation Numeric, opisano v zgornjem odstavku, se lahko spremeni ali posodobi šele potem, ko imenovani laboratorij pridobi stališča proizvajalcev homologiranih digitalnih in pametnih tahografskih enot v vozilu.

2.102. **NoOfCalibrationRecords**

Število zapisov o kalibraciji, ki jih lahko hrani kartica servisne delavnice.

Prva generacija:

```
NoOfCalibrationRecords ::= INTEGER(0..255)
```

Dodeljena vrednost: glej Dodatek 2.

Druga generacija:

```
NoOfCalibrationRecords ::= INTEGER(0..2^16-1)
```

Dodeljena vrednost: glej Dodatek 2.

2.103. **NoOfCalibrationsSinceDownload**

Števec, ki kaže število kalibracij, opravljenih s kartico servisne delavnice od zadnjega prenosa podatkov z nje (zahtevi 317 in 340 iz Priloge 1C).

```
NoOfCalibrationsSinceDownload ::= INTEGER(0..2^16-1)
```

Dodeljena vrednost: ni podrobneje določena.

2.104. **NoOfCardPlaceRecords**

Število zapisov krajev, ki jih lahko hrani vozniška kartica ali kartica servisne delavnice.

Prva generacija:

```
NoOfCardPlaceRecords ::= INTEGER(0..255)
```

Dodeljena vrednost: glej Dodatek 2.

Druga generacija:

```
NoOfCardPlaceRecords ::= INTEGER(0..2^16-1)
```

Dodeljena vrednost: glej Dodatek 2.

▼B

2.105. **NoOfCardVehicleRecords**

Število zapisov o uporabljenih vozilih, ki jih lahko shrani vozniška kartica ali kartica servisne delavnice.

```
NoOfCardVehicleRecords ::= INTEGER(0.. 2^16-1)
```

Dodeljena vrednost: glej Dodatek 2.

2.106. **NoOfCardVehicleUnitRecords**

Druga generacija:

število zapisov o uporabljenih enotah v vozilu, ki jih lahko shrani vozniška kartica ali kartica servisne delavnice.

```
NoOfCardVehicleUnitRecords ::= INTEGER(0.. 2^16-1)
```

Dodeljena vrednost: glej Dodatek 2.

2.107. **NoOfCompanyActivityRecords**

Število zapisov dejavnosti podjetja, ki jih lahko hrani kartica podjetja.

```
NoOfCompanyActivityRecords ::= INTEGER(0.. 2^16-1)
```

Dodeljena vrednost: glej Dodatek 2.

2.108. **NoOfControlActivityRecords**

Število zapisov nadzornih dejavnosti, ki jih lahko hrani nadzorna kartica.

```
NoOfControlActivityRecords ::= INTEGER(0.. 2^16-1)
```

Dodeljena vrednost: glej Dodatek 2.

2.109. **NoOfEventsPerType**

Število dogodkov posamezne vrste, ki jih lahko hrani kartica.

```
NoOfEventsPerType ::= INTEGER(0..255)
```

Dodeljena vrednost: glej Dodatek 2.

2.110. **NoOfFaultsPerType**

Število napak posamezne vrste, ki jih lahko hrani kartica.

```
NoOfFaultsPerType ::= INTEGER(0..255)
```

Dodeljena vrednost: glej Dodatek 2.

▼B

2.111. **NoOfGNSSCDRecords**

Druga generacija:

število GNSS zapisov neprekinjene vožnje, ki jih lahko hrani kartica.

```
NoOfGNSSCDRecords ::= INTEGER(0..2^16-1)
```

Dodeljena vrednost: glej Dodatek 2.

2.112. **NoOfSpecificConditionRecords**

Druga generacija:

število zapisov posebnih pogojev, ki jih lahko hrani kartica.

```
NoOfSpecificConditionRecords ::= INTEGER(0..2^16-1)
```

Dodeljena vrednost: glej Dodatek 2.

2.113. **OdometerShort**

Vrednost števca prevožene poti vozila v kratki obliki.

```
OdometerShort ::= INTEGER(0..2^24-1)
```

Dodeljena vrednost: binarno število brez predznaka. Vrednost v km v območju 0 do 9 999 999 km.

2.114. **OdometerValueMidnight**

Vrednost števca prevožene poti vozila na dani dan ob polnoči (zahteva 090 iz Priloge 1B in zahteva 113 iz Priloge 1C).

```
OdometerValueMidnight ::= OdometerShort
```

Dodeljena vrednost: ni podrobneje določena.

2.115. **OdometerValueMidnightRecordArray**

Druga generacija:

OdometerValueMidnight in metapodatki, uporabljeni v protokolu za prenos.

```
OdometerValueMidnightRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF
                                       OdometerValueMidnight
}
```

recordType označuje vrsto zapisa (OdometerValueMidnight). **Dodeljena vrednost**: glej RecordType.

recordSize je velikost OdometerValueMidnight v bajtih.

noOfRecords je število zapisov, ki jih vsebuje množica zapisov.

records je množica zapisov OdometerValueMidnight.

▼B

2.116. **OverspeedNumber**

Število dogodkov prekoračitve hitrosti od zadnjega nadzora prekoračitve hitrosti.

```
OverspeedNumber ::= INTEGER(0..255)
```

Dodeljena vrednost: 0 pomeni, da od zadnjega nadzora prekoračitev hitrosti ni bilo nobene prekoračitve hitrosti; 1 pomeni, da se je od zadnjega nadzora prekoračitve hitrosti zgodil en dogodek prekoračitve hitrosti, … 255 pomeni, da je bilo od zadnjega nadzora prekoračitve hitrosti že 255 ali več dogodkov prekoračitve hitrosti.

2.117. **PlaceRecord**

Informacija, povezana s krajem začetka ali konca dnevne delovne izmene (zahteve 108, 271, 296, 324 in 347 iz Priloge 1C).

Prva generacija:

```
PlaceRecord ::= SEQUENCE {
   entryTime                        TimeReal,
   entryTypeDailyWorkPeriod         EntryTypeDailyWorkPeriod,
   dailyWorkPeriodCountry           NationNumeric,
   dailyWorkPeriodRegion            RegionNumeric,
   vehicleOdometerValue             OdometerShort
}
```

entryTime je datum in čas vnosa.

entryTypeDailyWorkPeriod je vrsta vnosa.

dailyWorkPeriodCountry je vnesena država.

dailyWorkPeriodRegion je vnesena regija.

vehicleOdometerValue je vrednost števca prevožene poti ob času vnosa kraja.

Druga generacija:

```
PlaceRecord ::= SEQUENCE {
   entryTime                        TimeReal,
   entryTypeDailyWorkPeriod         EntryTypeDailyWorkPeriod,
   dailyWorkPeriodCountry           NationNumeric,
   dailyWorkPeriodRegion            RegionNumeric,
   vehicleOdometerValue             OdometerShort,
   entryGNSSPlaceRecord             GNSSPlaceRecord
}
```

Poleg elementov prve generacije se uporablja še naslednji element:

entryGNSSPlaceRecord je zapisana lokacija in čas.

▼B

2.118. **PreviousVehicleInfo**

Informacija, povezana z vozilom, ki ga je uporabljal voznik pred vstavitvijo svoje kartice v trenutno enoto v vozilu (zahteva 081 iz Priloge 1B in zahteva 102 iz Priloge 1C).

Prva generacija:

```
PreviousVehicleInfo ::= SEQUENCE {
   vehicleRegistrationIdentification      VehicleRegistrationIdentification,
   cardWithdrawalTime                     TimeReal
}
```

vehicleRegistrationIdentification je registrska številka vozila in država, v kateri je registrirano.

cardWithdrawalTime je datum in čas izvleka kartice.

Druga generacija:

```
PreviousVehicleInfo ::= SEQUENCE {
   vehicleRegistrationIdentification      VehicleRegistrationIdentification,
   cardWithdrawalTime                     TimeReal,
   vuGeneration                           Generation
}
```

Poleg elementov za prvo generacijo se uporablja še naslednji podatkovni element:

vuGeneration identificira generacijo enote v vozilu.

2.119. **PublicKey**

Prva generacija:

javni ključ RSA.

```
PublicKey ::= SEQUENCE {
   rsaKeyModulus                          RSAKeyModulus,
   rsaKeyPublicExponent                   RSAKeyPublicExponent
}
```

rsaKeyModulus je modul para ključev.

rsaKeyPublicExponent je javni eksponent para ključev.

2.120. **RecordType**

Druga generacija:

sklic na vrsto zapisa. Ta podatkovni tip se uporablja v RecordArrays.

```
RecordType ::= OCTET STRING(SIZE(1))
```

▼B

Dodeljena vrednost:

‘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	Določi proizvajalec.

2.121. **RegionAlpha**

Črkovna oznaka regije v določeni državi.

```
RegionAlpha ::= IA5STRING(SIZE(3))
```

Prva generacija:

Dodeljena vrednost:

‘ ’	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

Druga generacija:

kode RegionAlpha so navedene na seznamu na spletišču laboratorija, imenovanega za opravljanje preskusov interoperabilnosti.

2.122. **RegionNumeric**

Številska oznaka regije v določeni državi.

```
RegionNumeric ::= OCTET STRING (SIZE(1))
```

Prva generacija:

Dodeljena vrednost:

```
'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
```

Druga generacija:

kode RegionNumeric so navedene na seznamu na spletišču laboratorija, imenovanega za opravljanje preskusov interoperabilnosti.

2.123. **RemoteCommunicationModuleSerialNumber**

Druga generacija:

serijska številka modula za komunikacijo na daljavo.

```
RemoteCommunicationModuleSerialNumber ::= ExtendedSerialNumber
```

2.124. **RSAKeyModulus**

Prva generacija:

modul para ključev RSA.

```
RSAKeyModulus ::= OCTET STRING (SIZE(128))
```

Dodeljena vrednost: ni določena.

2.125. **RSAKeyPrivateExponent**

Prva generacija:

zasebni eksponent para ključev RSA.

```
RSAKeyPrivateExponent ::= OCTET STRING (SIZE(128))
```

Dodeljena vrednost: ni določena.

▼B

2.126. **RSAKeyPublicExponent**

Prva generacija:

javni eksponent para ključev RSA.

```
RSAKeyPublicExponent ::= OCTET STRING (SIZE(8))
```

Dodeljena vrednost: ni določena.

2.127. **RtmData**

Druga generacija:

za opredelitev tega podatkovnega tipa glej Dodatek 14.

2.128. **SealDataCard**

Druga generacija:

ta podatkovni tip shranjuje informacije o pečatih, ki so pritrjeni na različne sestavne dele vozila, in je namenjen za hrambo na kartici. Ta podatkovni tip je povezan z zahtevo 337 iz Priloge 1C.

```
SealDataCard ::= SEQUENCE {
   noOfSealRecords                    INTEGER(1..5),
   sealRecords                        SET SIZE(noOfSealRecords) OF SealRecord
}
```

noOfSealRecords je število zapisov v sealRecords.

sealRecords je množica zapisov o pečatih.

2.129. **SealDataVu**

Druga generacija:

ta podatkovni tip shranjuje informacije o pečatih, ki so pritrjeni na različne sestavne dele vozila, in je namenjen za hrambo v enoti v vozilu.

```
SealDataVu ::= SEQUENCE SIZE(5) OF {
   sealRecords                        SealRecord
}
```

sealRecords je množica zapisov o pečatih. Če je na voljo manj kot pet pečatov, se vrednost EquipmentType v vseh neuporabljenih sealRecords nastavi na 16, tj. neuporabljeno.

2.130. **SealRecord**

Druga generacija:

ta podatkovni tip hrani informacijo o pečatu, ki se pritrdi na sestavni del. Ta podatkovni tip je povezan z zahtevo 337 iz Priloge 1C.

```
SealRecord ::= SEQUENCE {
   equipmentType                      EquipmentType,
   extendedSealIdentifier             ExtendedSealIdentifier
}
```

equipmentType identificira vrsto opreme, na katero je pritrjen pečat.

extendedSealIdentifier je identifikator pečata, ki je pritrjen na opremo.

▼B

2.131. **SensorApprovalNumber**

Homologacijska številka tipala.

Prva generacija:

```
SensorApprovalNumber ::= IA5String(SIZE(8))
```

Dodeljena vrednost: ni določena.

Druga generacija:

```
SensorApprovalNumber ::= IA5String(SIZE(16))
```

Dodeljena vrednost:

homologacijska številka se navede, kakor je objavljena na ustreznem spletišču Komisije, tj. vključno z vezaji, če obstajajo. Homologacijska številka se poravna levo.

2.132. **SensorExternalGNSSApprovalNumber**

Druga generacija:

homologacijska številka zunanje GNSS opreme.

```
SensorExternalGNSSApprovalNumber ::= IA5String(SIZE(16))
```

Dodeljena vrednost:

homologacijska številka se navede, kakor je objavljena na ustreznem spletišču Komisije, tj. vključno z vezaji, če obstajajo. Homologacijska številka se poravna levo.

2.133. **SensorExternalGNSSCoupledRecord**

Druga generacija:

informacija, shranjena v enoti v vozilu, povezana z identifikacijo zunanje GNSS opreme, povezane z enoto v vozilu (zahteva 100 iz Priloge 1C).

```
SensorExternalGNSSCoupledRecord ::= SEQUENCE {
   sensorSerialNumber                  SensorGNSSSerialNumber,
   sensorApprovalNumber                SensorExternalGNSSApprovalNumber,
   sensorCouplingDate                  SensorGNSSCouplingDate
}
```

sensorSerialNumber je serijska številka zunanje GNSS opreme, povezane z enoto v vozilu.

sensorApprovalNumber je homologacijska številka te zunanje GNSS opreme.

sensorPairingDate je datum povezave te zunanje GNSS opreme z enoto v vozilu.

2.134. **SensorExternalGNSSIdentification**

Druga generacija:

informacija, shranjena na kartici, povezana z identifikacijo zunanje GNSS opreme (zahteva 98 iz Priloge 1C).

▼B

```
SensorExternalGNSSIdentification ::= SEQUENCE {
   sensorSerialNumber                    SensorGNSSSerialNumber,
   sensorApprovalNumber                  SensorExternalGNSSApprovalNumber,
   sensorSCIdentifier                    SensorExternalGNSSSCIdentifier,
   sensorOSIdentifier                    SensorExternalGNSSOSIdentifier
}
```

sensorSerialNumber je podaljšana serijska številka zunanje GNSS opreme.

sensorApprovalNumber je homologacijska številka zunanje GNSS opreme.

sensorSCIdentifier je identifikator varnostnega dela zunanje GNSS opreme.

sensorOSIdentifier je identifikator operacijskega sistema zunanje GNSS opreme.

2.135. **SensorExternalGNSSInstallation**

Druga generacija:

informacija, shranjena v zunanji GNSS opremi, povezana z namestitvijo zunanjega GNSS tipala (zahteva 123 iz Priloge 1C).

```
SensorExternalGNSSInstallation ::= SEQUENCE {
   sensorCouplingDateFirst               SensorGNSSCouplingDate,
   firstVuApprovalNumber                 VuApprovalNumber,
   firstVuSerialNumber                   VuSerialNumber,
   sensorCouplingDateCurrent             SensorGNSSCouplingDate,
   currentVuApprovalNumber               VuApprovalNumber,
   currentVUSerialNumber                 VuSerialNumber
}
```

sensorCouplingDateFirst je datum prve povezave zunanje GNSS opreme z enoto v vozilu.

firstVuApprovalNumber je homologacijska številka prve enote v vozilu, s katero je bila povezana zunanja GNSS oprema.

firstVuSerialNumber je serijska številka prve enote v vozilu, s katero je bila povezana zunanja GNSS oprema.

sensorCouplingDateCurrent je datum trenutne povezave zunanje GNSS opreme z enoto v vozilu.

currentVuApprovalNumber je homologacijska številka enote v vozilu, s katero je trenutno povezana zunanja GNSS oprema.

currentVUSerialNumber je serijska številka enote v vozilu, s katero je trenutno povezana zunanja GNSS oprema.

▼B

2.136. **SensorExternalGNSSOSIdentifier**

Druga generacija:

identifikator operacijskega sistema zunanje GNSS opreme.

```
SensorOSIdentifier ::= IA5String(SIZE(2))
```

Dodeljena vrednost: določi proizvajalec.

2.137. **SensorExternalGNSSSCIdentifier**

Druga generacija:

ta tip se na primer uporablja za identifikacijo kriptografskega modula zunanje GNSS opreme.

Identifikator varnostnega dela zunanje GNSS opreme.

```
SensorExternalGNSSSCIdentifier ::= IA5String(SIZE(8))
```

Dodeljena vrednost: določi proizvajalec sestavnega dela.

2.138. **SensorGNSSCouplingDate**

Druga generacija:

datum povezave zunanje GNSS opreme z enoto v vozilu.

```
SensorGNSSCouplingDate ::= TimeReal
```

Dodeljena vrednost: ni določena.

2.139. **SensorGNSSSerialNumber**

Druga generacija:

ta tip se uporablja za shranjevanje serijske številke GNSS sprejemnika, kadar je znotraj ali zunaj enote v vozilu.

Serijska številka GNSS sprejemnika.

```
SensorGNSSSerialNumber ::= ExtendedSerialNumber
```

2.140. **SensorIdentification**

Informacija, povezana z identifikacijo tipala gibanja, shranjena v tipalu gibanja (zahteva 077 iz Priloge 1B in zahteva 95 iz Priloge 1C).

```
SensorIdentification ::= SEQUENCE {
   sensorSerialNumber                  SensorSerialNumber,
   sensorApprovalNumber                SensorApprovalNumber,
   sensorSCIdentifier                  SensorSCIdentifier,
   sensorOSIdentifier                  SensorOSIdentifier
}
```

sensorSerialNumber je podaljšana serijska številka tipala gibanja (vključuje kataloško številko in kodo proizvajalca).

sensorApprovalNumber je homologacijska številka tipala gibanja.

sensorSCIdentifier je identifikator varnostnega dela tipala gibanja.

▼B

sensorOSIdentifier je identifikator operacijskega sistema tipala gibanja.

2.141. **SensorInstallation**

Informacija, shranjena v tipalu gibanja, povezana z namestitvijo tipala gibanja (zahteva 099 iz Priloge 1B in zahteva 122 iz Priloge 1C).

```
SensorInstallation ::= SEQUENCE {
   sensorPairingDateFirst                SensorPairingDate,
   firstVuApprovalNumber                 VuApprovalNumber,
   firstVuSerialNumber                   VuSerialNumber,
   sensorPairingDateCurrent              SensorPairingDate,
   currentVuApprovalNumber               VuApprovalNumber,
   currentVUSerialNumber                 VuSerialNumber
}
```

sensorPairingDateFirst je datum prve povezave tipala gibanja z enoto v vozilu.

firstVuApprovalNumber je homologacijska številka prve enote v vozilu, s katero je bilo povezano tipalo gibanja.

firstVuSerialNumber je serijska številka prve enote v vozilu, s katero je povezano tipalo gibanja.

sensorPairingDateCurrent je datum trenutne povezave tipala gibanja z enoto v vozilu.

currentVuApprovalNumber je homologacijska številka enote v vozilu, s katero je trenutno povezano tipalo gibanja.

currentVUSerialNumber je serijska številka enote v vozilu, s katero je trenutno povezano tipalo gibanja.

2.142. **SensorInstallationSecData**

Informacija, shranjena na kartici servisne delavnice, povezana z varnostnimi podatki, potrebnimi za povezavo tipal gibanja z enotami v vozilu (zahtevi 308 in 331 iz Priloge 1C).

Prva generacija:

```
SensorInstallationSecData ::= TdesSessionKey
```

Dodeljena vrednost: v skladu z ISO 16844-3.

Druga generacija:

kot je opisano v Dodatku 11, kartica servisne delavnice shrani največ tri ključe za povezavo VU–tipalo gibanja. Ti ključi imajo različne različice ključev.

```
SensorInstallationSecData ::= SEQUENCE {
   kMWCKey1                              KMWCKey,
   kMWCKey2                              KMWCKey OPTIONAL,
   kMWCKey3                              KMWCKey OPTIONAL
}
```

▼B

2.143. **SensorOSIdentifier**

Identifikator operacijskega sistema tipala gibanja.

```
SensorOSIdentifier ::= IA5String(SIZE(2))
```

Dodeljena vrednost: določi proizvajalec.

2.144. **SensorPaired**

Prva generacija:

informacija, shranjena v enoti v vozilu, povezana z identifikacijo tipala gibanja, povezanega z enoto v vozilu (zahteva 079 iz Priloge 1B).

```
SensorPaired ::= SEQUENCE {
   sensorSerialNumber                  SensorSerialNumber,
   sensorApprovalNumber                SensorApprovalNumber,
   sensorPairingDateFirst              SensorPairingDate
}
```

sensorSerialNumber je serijska številka tipala gibanja, s katerim je trenutno povezana enota v vozilu.

sensorApprovalNumber je homologacijska številka tipala gibanja, s katerim je trenutno povezana enota v vozilu.

sensorPairingDateFirst je datum prve povezave tipala gibanja z enoto v vozilu, s katero je trenutno povezano.

2.145. **SensorPairedRecord**

Druga generacija:

informacija, shranjena v enoti v vozilu, povezana z identifikacijo tipala gibanja, povezanega z enoto v vozilu (zahteva 97 iz Priloge 1C).

```
SensorPairedRecord ::= SEQUENCE {
   sensorSerialNumber                  SensorSerialNumber,
   sensorApprovalNumber                SensorApprovalNumber,
   sensorPairingDate                   SensorPairingDate
}
```

sensorSerialNumber je serijska številka tipala gibanja, s katerim je povezana enota v vozilu.

sensorApprovalNumber je homologacijska številka tega tipala gibanja.

sensorPairingDate je datum povezave tega tipala gibanja z enoto v vozilu.

2.146. **SensorPairingDate**

Datum povezave tipala gibanja z enoto v vozilu.

```
SensorPairingDate ::= TimeReal
```

Dodeljena vrednost: ni določena.

▼B

2.147. **SensorSCIdentifier**

Identifikator varnostnega dela tipala gibanja.

```
SensorSCIdentifier ::= IA5String(SIZE(8))
```

Dodeljena vrednost: določi proizvajalec sestavnega dela.

2.148. **SensorSerialNumber**

Serijska številka tipala gibanja.

```
SensorSerialNumber ::= ExtendedSerialNumber
```

2.149. **Signature**

Digitalni podpis.

Prva generacija:

```
Signature ::= OCTET STRING (SIZE(128))
```

Dodeljena vrednost: v skladu z Dodatkom 11 „Skupni varnostni mehanizmi“.

Druga generacija:

```
 Signature ::= OCTET STRING (SIZE(64..132))
```

Dodeljena vrednost: v skladu z Dodatkom 11 „Skupni varnostni mehanizmi“.

2.150. **SignatureRecordArray**

Druga generacija:

množica podpisov in metapodatki, uporabljeni v protokolu za prenos.

```
SignatureRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF Signature
}
```

recordType označuje vrsto zapisa (Signature). **Dodeljena vrednost**: glej RecordType.

recordSize je v bajtih izražena velikost Signature.

noOfRecords je število zapisov, ki jih vsebuje množica zapisov. Vrednost se nastavi na 1, saj so certifikati lahko različnih dolžin.

records je množica podpisov.

2.151. **SimilarEventsNumber**

Število podobnih dogodkov v enem danem dnevu (zahteva 094 iz Priloge 1B in zahteva 117 iz Priloge 1C).

```
SimilarEventsNumber ::= INTEGER(0..255)
```

Dodeljena vrednost: 0 se ne uporablja, 1 pomeni, da se je na navedeni dan zgodil le en dogodek te vrste, 2 pomeni, da sta se navedeni dan zgodila dva dogodka te vrste (shranjen pa je bil le eden), … 255 pomeni, da se je na navedeni dan zgodilo 255 ali več dogodkov te vrste.

▼B

2.152. **SpecificConditionRecord**

Informacija, shranjena na vozniški kartici, na kartici servisne delavnice ali v enoti v vozilu, povezana s posebnim stanjem (zahteve 130, 276, 301, 328 in 355 iz Priloge 1C).

```
SpecificConditionRecord ::= SEQUENCE {
   entryTime                              TimeReal,
   specificConditionType                  SpecificConditionType
}
```

entryTime je datum in čas vnosa.

specificConditionType je koda, ki identificira posebno stanje.

2.153. **SpecificConditions**

Informacija, shranjena na vozniški kartici, na kartici servisne delavnice ali v enoti v vozilu, povezana s posebnim stanjem (zahteve 131, 277, 302, 329 in 356 iz Priloge 1C).

Druga generacija:

```
SpecificConditions := SEQUENCE {
   conditionPointerNewestRecord         INTEGER(0..NoOfSpecificConditionRecords-1),
   specificConditionRecords             SET SIZE(NoOfSpecificConditionRecords) OF
                                        SpecificConditionRecord
}
```

placePointerNewestRecord je indeks zadnjega posodobljenega zapisa posebnih pogojev.

Dodeljena vrednost: število, ki ustreza številu zapisa posebnih pogojev; začne se z vrednostjo ‘0’ za prvi zapis posebnega pogoja v strukturi.

cardVehicleRecords je množica zapisov podatkov o zapisanih posebnih stanjih.

2.154. **SpecificConditionType**

Koda, ki identificira posebno stanje (zahteve 050b, 105a, 212a in 230a iz Priloge 1B ter zahteva 62 iz Priloge 1C).

```
SpecificConditionType ::= INTEGER(0..255)
```

Prva generacija:

Dodeljena vrednost:

‘00’H	RFU
‘01’H	Zunaj področja veljavnosti – začetek
‘02’H	Zunaj področja veljavnosti – konec
‘03’H	Prevoz s trajektom/vlakom
‘04’H .. ‘FF’H	RFU

Druga generacija:

Dodeljena vrednost:

‘00’H	RFU
‘01’H	Zunaj področja veljavnosti – začetek
‘02’H	Zunaj področja veljavnosti – konec
‘03’H	Prevoz s trajektom/vlakom – začetek
‘04’H	Prevoz s trajektom/vlakom – konec
‘05’H .. ‘FF’H	RFU

▼B

2.155. **Hitrost**

Hitrost vozila (km/h).

```
Speed ::= INTEGER(0..255)
```

Dodeljena vrednost: kilometri na uro v območju od 0 do 220 km/h.

2.156. **SpeedAuthorised**

Največja dovoljena hitrost vozila (opredelitev hh)).

```
SpeedAuthorised ::= Speed
```

2.157. **SpeedAverage**

Povprečna hitrost v prej določenem obdobju (km/h).

```
SpeedAverage ::= Speed
```

2.158. **SpeedMax**

Največja hitrost, izmerjena v prej določenem obdobju.

```
SpeedMax ::= Speed
```

2.159. **TachographPayload**

Druga generacija:

za opredelitev tega podatkovnega tipa glej Dodatek 14.

2.160. **TachographPayloadEncrypted**

Druga generacija:

šifrirani koristni podatki tahografa DER-TLV, tj. podatki, poslani šifrirano v sporočilu RTM. Za šifriranje glej poglavje 13 Dela B iz Dodatka 11.

```
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 je del kodiranja DER-TLV in se nastavi na ‘87’ (glej poglavje 13 Dela B iz Dodatka 11).

length je del kodiranja DER-TLV in kodira dolžino naslednjega paddingContentIndicatorByte in encryptedData.

paddingContentIndicatorByte se nastavi na ‘00’.

encryptedData je šifrirani tachographPayload, kot je določen v poglavju 13 Dela B iz Dodatka 11. Dolžina tega podatka v oktetih je vedno večkratnik števila 16.

2.161. **TDesSessionKey**

Prva generacija:

trojni DES ključ seje.

```
TDesSessionKey ::= SEQUENCE {
   tDesKeyA                             OCTET STRING (SIZE(8)),
   tDesKeyB                             OCTET STRING (SIZE(8))
}
```

Dodeljena vrednost: ni podrobneje določena.

▼B

2.162. **TimeReal**

Koda sestava datum/čas, v kateri sta datum in čas izražena kot število sekund od časa 00h.00m.00s. po GMT dne 1. januarja 1970.

```
TimeReal{INTEGER:TimeRealRange} ::= INTEGER(0..TimeRealRange)
```

Dodeljena vrednost – oktetno poravnano: Število sekund od polnoči 1. januarja 1970 po GMT.

Najpoznejši možni datum/čas je v letu 2106.

2.163. **TyreSize**

Oznaka mer pnevmatik.

```
TyreSize ::= IA5String(SIZE(15))
```

Dodeljena vrednost: V skladu z Direktivo 92/23 (EGS), 31.3.1992, UL L 129, str. 95.

2.164. **VehicleIdentificationNumber**

Identifikacijska številka vozila (VIN), ki se nanaša na vozilo kot celoto; navadno serijska številka šasije ali okvira podvozja.

```
VehicleIdentificationNumber ::= IA5String(SIZE(17))
```

Dodeljena vrednost: kakor določa ISO 3779.

2.165. **VehicleIdentificationNumberRecordArray**

Druga generacija:

identifikacijska številka vozila in metapodatki, kot se uporabljajo v protokolu za prenos.

```
VehicleIdentificationNumberRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF
                                       VehicleIdentificationNumber
}
```

recordType označuje vrsto zapisa (VehicleIdentificationNumber). **Dodeljena vrednost**: glej RecordType.

recordSize je v bajtih izražena velikost VehicleIdentificationNumber.

noOfRecords je število zapisov, ki jih vsebuje množica zapisov.

records je množica identifikacijskih številk vozila.

2.166. **VehicleRegistrationIdentification**

Identifikacija vozila, edinstvena za Evropo (registrska številka in država, v kateri je registrirano).

```
VehicleRegistrationIdentification ::= SEQUENCE {
   vehicleRegistrationNation           NationNumeric,
   vehicleRegistrationNumber           VehicleRegistrationNumber
}
```

vehicleRegistrationNation je država, v kateri je vozilo registrirano.

▼B

vehicleRegistrationNumber je registrska številka vozila (VRN).

2.167. **VehicleRegistrationNumber**

Registrska številka vozila (VRN). Registrsko številko dodeli organ, pristojen za registracijo.

```
VehicleRegistrationNumber ::= SEQUENCE {
   codePage                              INTEGER (0..255),
   vehicleRegNumber                      OCTET STRING (SIZE(13))
}
```

codePage določa nabor znakov, opredeljenih v poglavju 4,

vehicleRegNumber je registrska številka vozila, kodirana z navedenim naborom znakov.

Dodeljena vrednost: določena za posamezno državo.

2.168. **VehicleRegistrationNumberRecordArray**

Druga generacija:

registrska številka vozila in metapodatki, kot se uporabljajo v protokolu za prenos.

```
VehicleRegistrationNumberRecordArray ::= SEQUENCE {
   recordType                            RecordType,
   recordSize                            INTEGER(1..65535),
   noOfRecords                           INTEGER(0..65535),
   records                               SET SIZE(noOfRecords) OF
                                         VehicleRegistrationNumber
}
```

recordType označuje vrsto zapisa (VehicleRegistrationNumber). **Dodeljena vrednost**: glej RecordType.

recordSize je v bajtih izražena velikost VehicleRegistrationNumber.

noOfRecords je število zapisov, ki jih vsebuje množica zapisov.

records je množica registrskih številk vozila.

2.169. **VuAbility**

Druga generacija:

informacija, shranjena v enoti v vozilu, o tem, ali enota v vozilu lahko uporablja tahografske kartice prve generacije (zahteva 121 iz Priloge 1C).

```
VuAbility ::= OCTET STRING (SIZE(1))
```

Dodeljena vrednost – oktetno poravnano: ‘xxxxxxxa’B (8 bitov)

Če lahko podpira prvo generacijo:

‘a’B	Podpora tahografskih kartic prve generacije:
	‘0’ B prva generacija je podprta,
	‘1’B prva generacija ni podprta,
‘xxxxxxx’B	RFU

▼B

2.170. **VuActivityDailyData**

Prva generacija:

informacija, shranjena v enoti v vozilu, povezana s spremembami dejavnosti in/ali spremembami stanja vožnje in/ali spremembami stanja kartice na določen koledarski dan (zahteva 084 iz Priloge 1B ter zahteve 105, 106 in 107 iz Priloge 1C) ter s stanjem rež ob 00,00 na ta dan.

```
VuActivityDailyData ::= SEQUENCE {
   noOfActivityChanges                    INTEGER SIZE(0..1440),
   activityChangeInfos                    SET SIZE(noOfActivityChanges) OF
                                          ActivityChangeInfo
}
```

noOfActivityChanges je število besed ActivityChangeInfo v množici activityChangeInfos.

activityChangeInfos je množica besed ActivityChangeInfo, shranjena v enoti v vozilu za določen dan. Vedno vključuje dve besedi ActivityChangeInfo o stanju obeh rež ob 00.00 na ta dan.

2.171. **VuActivityDailyRecordArray**

Druga generacija:

informacija, shranjena v enoti v vozilu, povezana s spremembami dejavnosti in/ali spremembami stanja vožnje in/ali spremembami stanja kartice na določen koledarski dan (zahteve 105, 106 in 107 iz Priloge 1C) ter s stanjem rež ob 00.00 na ta dan.

```
VuActivityDailyRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF ActivityChangeInfo
}
```

recordType označuje vrsto zapisa (ActivityChangeInfo). **Dodeljena vrednost**: glej RecordType.

recordSize je v bajtih izražena velikost ActivityChangeInfo.

noOfRecords je število zapisov, ki jih vsebuje množica zapisov.

records je množica besed ActivityChangeInfo, shranjena v enoti v vozilu za določen dan. Vedno vključuje dve besedi ActivityChangeInfo o stanju obeh rež ob 00.00 na ta dan.

2.172. **VuApprovalNumber**

Homologacijska številka enote v vozilu.

Prva generacija:

```
VuApprovalNumber ::= IA5String(SIZE(8))
```

Dodeljena vrednost: ni določena.

Druga generacija:

```
VuApprovalNumber ::= IA5String(SIZE(16))
```

▼B

Dodeljena vrednost:

homologacijska številka se navede, kakor je objavljena na ustreznem spletišču Komisije, tj. vključno z vezaji, če obstajajo. Homologacijska številka se poravna levo.

2.173. **VuCalibrationData**

Prva generacija:

informacija, shranjena v enoti v vozilu, povezana s kalibracijami zapisovalne naprave (zahteva 098 iz Priloge 1B).

```
VuCalibrationData ::= SEQUENCE {
   noOfVuCalibrationRecords              INTEGER(0..255),
   vuCalibrationRecords                  SET SIZE(noOfVuCalibrationRecords) OF
                                         VuCalibrationRecord
}
```

noOfVuCalibrationRecords je število zapisov, ki jih vsebuje množica vuCalibrationRecords.

vuCalibrationRecords je množica zapisov o kalibraciji.

2.174. **VuCalibrationRecord**

Informacija, shranjena v enoti v vozilu, povezana s kalibracijo zapisovalne naprave (zahteva 098 iz Priloge 1B ter zahtevi 119 in 120 iz Priloge 1C).

Prva generacija:

```
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 je namen kalibracije.

workshopName, workshopAddress sta ime in naslov servisne delavnice.

workshopCardNumber identificira kartico servisne delavnice, uporabljeno pri kalibraciji.

workshopCardExpiryDate je datum izteka veljavnosti kartice.

vehicleIdentificationNumber je VIN.

▼B

vehicleRegistrationIdentification vsebuje registrsko številko vozila in državo, v kateri je registrirano.

wVehicleCharacteristicConstant je značilni koeficient vozila.

kConstantOfRecordingEquipment je konstanta zapisovalne naprave.

lTyreCircumference je dejanski obseg pnevmatik.

tyreSize je oznaka mer pnevmatik na vozilu.

authorisedSpeed je dovoljena hitrost vozila.

oldOdometerValue, newOdometerValue sta stara in nova vrednost števca prevožene poti.

oldTimeValue, newTimeValue sta stara in nova vrednost datuma in časa.

nextCalibrationDate je datum, na katerega naj se opravi naslednja kalibracija vrste, označene v CalibrationPurpose, pri pooblaščenem inšpekcijskem organu.

Druga generacija:

```
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
}
```

Poleg elementov za prvo generacijo se uporablja še naslednji podatkovni element:

sealDataVu daje informacije o pečatih, ki so pritrjeni na različne sestavne dele vozila.

2.175. **VuCalibrationRecordArray**

Druga generacija:

informacija, shranjena v enoti v vozilu, povezana s kalibracijami zapisovalne naprave (zahtevi 119 in 120 iz Priloge 1C)

▼B

```
VuCalibrationRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF
                                       VuCalibrationRecord
}
```

recordType označuje vrsto zapisa (VuCalibrationRecord). **Dodeljena vrednost**: glej RecordType.

recordSize je v bajtih izražena velikost VuCalibrationRecord.

noOfRecords je število zapisov, ki jih vsebuje množica zapisov.

records je množica zapisov o kalibraciji.

2.176. **VuCardIWData**

Prva generacija:

informacija, shranjena v enoti v vozilu, povezana s cikli vstavitve in izvleka vozniških kartic ali kartic servisne delavnice v enoto/iz enote v vozilu (zahteva 081 iz Priloge 1B in zahteva 103 iz Priloge 1C).

```
VuCardIWData ::= SEQUENCE {
   noOfIWRecords                       INTEGER(0..2^16-1),
   vuCardIWRecords                     SET SIZE(noOfIWRecords) OF VuCardIWRecord
}
```

noOfIWRecords je število zapisov v množici vuCardIWRecords.

vuCardIWRecords je množica zapisov v zvezi s cikli vstavitve in izvleka kartice.

2.177. **VuCardIWRecord**

Informacija, shranjena v enoti v vozilu, povezana s ciklom vstavitve in izvleka vozniške kartice ali kartice servisne delavnice v enoto/iz enote v vozilu (zahteva 081 iz Priloge 1B in zahteva 102 iz Priloge 1C).

Prva generacija:

```
VuCardIWRecord ::= SEQUENCE {
   cardHolderName                      HolderName,
   fullCardNumber                      FullCardNumber,
   cardExpiryDate                      TimeReal,
   cardInsertionTime                   TimeReal,
   vehicleOdometerValueAtInsertion     OdometerShort,
   cardSlotNumber                      CardSlotNumber,
   cardWithdrawalTime                  TimeReal,
   vehicleOdometerValueAtWithdrawal    OdometerShort,
   previousVehicleInfo                 PreviousVehicleInfo,
   manualInputFlag                     ManualInputFlag
}
```

cardHolderName je priimek in ime(na) imetnika vozniške kartice ali kartice servisne delavnice, kot so shranjeni na kartici.

fullCardNumber je vrsta kartice, njena država izdajateljica in številka kartice, kot so shranjene na kartici.

▼B

cardExpiryDate je datum izteka kartice, shranjen na kartici.

cardInsertionTime je datum in čas vstavitve.

vehicleOdometerValueAtInsertion je vrednost števca prevožene poti ob vstavitvi kartice.

cardSlotNumber je reža, v katero je kartica vstavljena.

cardWithdrawalTime je datum in čas izvleka.

vehicleOdometerValueAtWithdrawal je vrednost števca prevožene poti ob izvleku kartice.

previousVehicleInfo vsebuje podatke o prejšnjem vozilu, ki ga je uporabljal voznik, kot so shranjeni na kartici.

manualInputFlag je zastavica, ki kaže, ali je imetnik kartice ob vstavitvi kartice ročno vnesel voznikove dejavnosti.

Druga generacija:

```
VuCardIWRecord ::= SEQUENCE {
   cardHolderName                       HolderName,
   fullCardNumberAndGeneration          FullCardNumberAndGeneration,
   cardExpiryDate                       TimeReal,
   cardInsertionTime                    TimeReal,
   vehicleOdometerValueAtInsertion      OdometerShort,
   cardSlotNumber                       CardSlotNumber,
   cardWithdrawalTime                   TimeReal,
   vehicleOdometerValueAtWithdrawal     OdometerShort,
   previousVehicleInfo                  PreviousVehicleInfo,
   manualInputFlag                      ManualInputFlag
}
```

Namesto fullCardNumber struktura podatkov druge generacije uporablja naslednji podatkovni element.

fullCardNumberAndGeneration je vrsta kartice, njena država izdajateljica, številka kartice in njena generacija, kot so shranjene na kartici.

2.178. **VuCardIWRecordArray**

Druga generacija:

informacija, shranjena v enoti v vozilu, povezana s cikli vstavitve in izvleka vozniških kartic ali kartic servisne delavnice v enoti/iz enote v vozilu (zahteva 103 iz Priloge 1C).

```
VuCardIWRecordArray ::= SEQUENCE {
   recordType                           RecordType,
   recordSize                           INTEGER(1..65535),
   noOfRecords                          INTEGER(0..65535),
   records                              SET SIZE(noOfRecords) OF VuCardIWRecord
}
```

recordType označuje vrsto zapisa (VuCardIWRecord). **Dodeljena vrednost**: glej RecordType.

recordSize je v bajtih izražena velikost VuCardIWRecord.

▼B

noOfRecords je število zapisov, ki jih vsebuje množica zapisov.

records je množica zapisov v zvezi s cikli vstavitve in izvleka kartice.

2.179. **VuCardRecord**

Druga generacija:

informacija, shranjena v enoti v vozilu, povezana z uporabljeno tahografsko kartico (zahteva 132 iz Priloge 1C).

```
VuCardRecord ::= SEQUENCE {
   cardExtendedSerialNumber            ExtendedSerialNumber,
   cardPersonaliserID                  OCTET STRING(SIZE(1)),
   typeofTachographCardID              EquipmentType,
   cardStructureVersion                CardStructureVersion,
   cardNumber                          CardNumber
}
```

cardExtendedSerialNumber, kot se prebere s kartice iz datoteke EF_ICC v MF.

cardPersonaliserID, kot se prebere s kartice iz datoteke EF_ICC v MF.

typeOfTachographCardId, kot se prebere iz datoteke EF_Application_Identification v DF_Tachograph_G2.

cardStructureVersion, kot se prebere iz datoteke EF_Application_Identification v DF_Tachograph_G2.

cardNumber, kot se prebere iz datoteke EF_Application_Identification v DF_Tachograph_G2.

2.180. **VuCardRecordArray**

Druga generacija:

informacija, shranjena v enoti v vozilu, o tahografskih karticah, uporabljenih v tej enoti v vozilu. Ta informacija je namenjena za analizo enote v vozilu – težave s karticami (zahteva 132 iz Priloge 1C).

```
VuCardRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF VuCardRecord
}
```

recordType označuje vrsto zapisa (VuCardRecord). **Dodeljena vrednost**: glej RecordType.

recordSize je v bajtih izražena velikost VuCardRecord.

noOfRecords je število zapisov, ki jih vsebuje množica zapisov.

records je množica zapisov v zvezi s tahografskimi karticami, uporabljenimi v enoti v vozilu.

▼B

2.181. **VuCertificate**

Certifikat javnega ključa enote v vozilu.

```
VuCertificate ::= Certificate
```

2.182. **VuCertificateRecordArray**

Druga generacija:

certifikat enote v vozilu in metapodatki, kot se uporabljajo v protokolu za prenos.

```
VuCertificateRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF VuCertificate
}
```

recordType označuje vrsto zapisa (VuCertificate). **Dodeljena vrednost**: glej RecordType.

recordSize je v bajtih izražena velikost VuCertificate.

noOfRecords je število zapisov, ki jih vsebuje množica zapisov. Vrednost se nastavi na 1, saj so certifikati lahko različne dolžine.

records je množica certifikatov enote v vozilu.

2.183. **VuCompanyLocksData**

Prva generacija:

informacija, shranjena v enoti v vozilu, povezana z blokadami podjetja (zahteva 104 iz Priloge 1B).

```
VuCompanyLocksData ::= SEQUENCE {
   noOfLocks                           INTEGER(0..255),
   vuCompanyLocksRecords               SET SIZE(noOfLocks) OF VuCompanyLocksRecord
}
```

noOfLocks je število blokad, navedenih v vuCompanyLocksRecords.

vuCompanyLocksRecord je množica zapisov blokad podjetja.

2.184. **VuCompanyLocksRecord**

Informacija, shranjena v enoti v vozilu, povezana z blokado podjetja (zahteva 104 iz Priloge 1B in zahteva 128 iz Priloge 1C).

Prva generacija:

```
VuCompanyLocksRecord ::= SEQUENCE {
   lockInTime                          TimeReal,
   lockOutTime                         TimeReal,
   companyName                         Name,
   companyAddress                      Address,
   companyCardNumber                   FullCardNumber
}
```

▼B

lockInTime, lockOutTime sta datum in čas vklopa ali izklopa blokade.

companyName, companyAddress sta ime in naslov podjetja, povezanega z vklopom blokade.

companyCardNumber identificira kartico, uporabljeno ob vklopu blokade.

Druga generacija:

```
VuCompanyLocksRecord ::= SEQUENCE {
   lockInTime                          TimeReal,
   lockOutTime                         TimeReal,
   companyName                         Name,
   companyAddress                      Address,
   companyCardNumberAndGeneration      FullCardNumberAndGeneration
}
```

Namesto companyCardNumber struktura podatkov druge generacije uporablja naslednji podatkovni element.

companyCardNumberAndGeneration identificira kartico, vključno z njeno generacijo, uporabljeno ob vklopu blokade.

2.185. **VuCompanyLocksRecordArray**

Druga generacija:

informacija, shranjena v enoti v vozilu, povezana z blokadami podjetja (zahteva 128 iz Priloge 1C).

```
VuCompanyLocksRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF
                                       VuCompanyLocksRecord
}
```

recordType označuje vrsto zapisa (VuCompanyLocksRecord). **Dodeljena vrednost**: glej RecordType.

recordSize je v bajtih izražena velikost VuCompanyLocksRecord.

noOfRecords je število zapisov, ki jih vsebuje množica zapisov. Vrednost 0..255.

records je množica zapisov o blokadah podjetja.

2.186. **VuControlActivityData**

Prva generacija:

informacija, shranjena v enoti v vozilu, povezana z nadzori, pri katerih je bila uporabljena ta enota v vozilu (zahteva 102 iz Priloge 1B).

```
VuControlActivityData ::= SEQUENCE {
   noOfControls                        INTEGER(0..20),
   vuControlActivityRecords            SET SIZE(noOfControls) OF
                                       VuControlActivityRecord
}
```

▼B

noOfControls je število nadzorov, navedenih v vuControlActivityRecords.

vuControlActivityRecords je množica zapisov o nadzornih dejavnostih.

2.187. **VuControlActivityRecord**

Informacija, shranjena v enoti v vozilu, povezana z nadzorom, pri katerem je bila uporabljena ta enota v vozilu (zahteva 102 iz Priloge 1B in zahteva 126 iz Priloge 1C).

Prva generacija:

```
VuControlActivityRecord ::= SEQUENCE {
   controlType                          ControlType,
   controlTime                          TimeReal,
   controlCardNumber                    FullCardNumber,
   downloadPeriodBeginTime              TimeReal,
   downloadPeriodEndTime                TimeReal
}
```

controlType je vrsta nadzora.

controlTime je datum in čas nadzora.

controlCardNumber identificira nadzorno kartico, uporabljeno pri nadzoru.

downloadPeriodBeginTime je začetek obdobja, za katerega je bil opravljen prenos podatkov, če je bil tak prenos opravljen.

downloadPeriodEndTime je konec obdobja, za katerega je bil opravljen prenos podatkov, če je bil tak prenos opravljen.

Druga generacija:

```
VuControlActivityRecord ::= SEQUENCE {
   controlType                          ControlType,
   controlTime                          TimeReal,
   controlCardNumberAndGeneration       FullCardNumberAndGeneration,
   downloadPeriodBeginTime              TimeReal,
   downloadPeriodEndTime                TimeReal
}
```

Namesto controlCardNumber struktura podatkov druge generacije uporablja naslednji podatkovni element.

controlCardNumber identificira nadzorno kartico, uporabljeno pri nadzoru, vključno z njeno generacijo.

2.188. **VuControlActivityRecordArray**

Druga generacija:

informacija, shranjena v enoti v vozilu, povezana z nadzori, pri katerih je bila uporabljena ta enota v vozilu (zahteva 126 iz Priloge 1C).

▼B

```
VuControlActivityRecordArray ::= SEQUENCE {
   recordType                              RecordType,
   recordSize                              INTEGER(1..65535),
   noOfRecords                             INTEGER(0..65535),
   records                                 SET SIZE(noOfRecords) OF
                                           VuControlActivityRecord
}
```

recordType označuje vrsto zapisa (VuControlActivityRecord). **Dodeljena vrednost**: glej RecordType.

recordSize je v bajtih izražena velikost VuControlActivityRecord.

noOfRecords je število zapisov, ki jih vsebuje množica zapisov.

records je množica zapisov o dejavnostih nadzora VU.

2.189. **VuDataBlockCounter**

Števec, shranjen na kartici, ki identificira zaporedje ciklov vstavitve in izvleka kartice v različnih enotah v vozilu.

```
VuDataBlockCounter ::= BCDString(SIZE(2))
```

Dodeljena vrednost: zaporedna številka z največjo vrednostjo 9 999; nato se začne ponovno z 0.

2.190. **VuDetailedSpeedBlock**

Informacija, shranjena v enoti v vozilu, povezana s podrobnimi podatki o hitrosti za minuto, v kateri se je vozilo premikalo (zahteva 093 iz Priloge 1B in zahteva 116 iz Priloge 1C).

```
VuDetailedSpeedBlock ::= SEQUENCE {
   speedBlockBeginDate    TimeReal,
   speedsPerSecond        SEQUENCE SIZE(60) OF Speed
}
```

speedBlockBeginDate je datum in čas prve vrednosti hitrosti v bloku.

speedsPerSecond je časovno zaporedje vsako sekundo izmerjenih hitrosti od (vključno) minute, navedene v speedBlockBeginDate.

2.191. **VuDetailedSpeedBlockRecordArray**

Druga generacija:

informacija, shranjena v enoti v vozilu, povezana s podrobnimi podatki o hitrosti vozila.

```
VuDetailedSpeedBlockRecordArray ::= SEQUENCE {
   recordType                              RecordType,
   recordSize                              INTEGER(1..65535),
   noOfRecords                             INTEGER(0..65535),
   records                                 SET SIZE(noOfRecords) OF
                                           VuDetailedSpeedBlock
}
```

recordType označuje vrsto zapisa (VuDetailedSpeedBlock). **Dodeljena vrednost**: glej RecordType.

▼B

recordSize je v bajtih izražena velikost VuDetailedSpeedBlock.

noOfRecords je število zapisov, ki jih vsebuje množica zapisov.

records je množica blokov podrobnih podatkov o hitrosti.

2.192. **VuDetailedSpeedData**

Prva generacija:

informacija, shranjena v enoti v vozilu, povezana s podrobnimi podatki o hitrosti vozila.

```
VuDetailedSpeedData ::= SEQUENCE {
   noOfSpeedBlocks                    INTEGER(0..2^16-1),
   vuDetailedSpeedBlocks              SET SIZE(noOfSpeedBlocks) OF
                                      VuDetailedSpeedBlock
}
```

noOfSpeedBlocks je število blokov hitrosti v množici vuDetailedSpeedBlocks.

vuDetailedSpeedBlocks je množica blokov podrobnih podatkov o hitrosti.

2.193. **VuDownloadablePeriod**

Najstarejši in najnovejši datumi, za katere enota v vozilu hrani podatke o voznikovih dejavnostih (zahteve 081, 084 ali 087 iz Priloge 1B in zahteve 102, 105, 108 iz Priloge 1C).

```
VuDownloadablePeriod ::= SEQUENCE {
   minDownloadableTime                TimeReal
   maxDownloadableTime                TimeReal
}
```

minDownloadableTime je nastarejša vstavitev kartice ali sprememba dejavnosti ali datum in čas vnosa kraja, shranjen v enoti vozila.

maxDownloadableTime je najnovejši izvlek kartice ali sprememba dejavnosti ali datum in čas vnosa kraja, shranjena v enoti vozila.

2.194. **VuDownloadablePeriodRecordArray**

Druga generacija:

VUDownloadablePeriod in metapodatki, uporabljeni v protokolu za prenos.

```
VuDownloadablePeriodRecordArray ::= SEQUENCE {
   recordType                         RecordType,
   recordSize                         INTEGER(1..65535),
   noOfRecords                        INTEGER(0..65535),
   records                            SET SIZE(noOfRecords) OF
                                      VuDownloadablePeriod
}
```

recordType označuje vrsto zapisa (VuDownloadablePeriod). **Dodeljena vrednost**: glej RecordType.

▼B

recordSize je v bajtih izražena velikost VuDownloadablePeriod.

noOfRecords je število zapisov, ki jih vsebuje množica zapisov.

records je množica zapisov VuDownloadablePeriod.

2.195. **VuDownloadActivityData**

Informacija, shranjena v enoti v vozilu, povezana z njenim zadnjim prenosom (zahteva 105 iz Priloge 1B in zahteva 129 iz Priloge 1C).

Prva generacija:

```
VuDownloadActivityData ::= SEQUENCE {
   downloadingTime                        TimeReal,
   fullCardNumber                         FullCardNumber,
   companyOrWorkshopName                  Name
}
```

downloadingTime je datum in čas prenosa podatkov.

fullCardNumber identificira kartico, ki je bila uporabljena za odobritev prenosa podatkov.

companyOrWorkshopName je ime podjetja ali servisne delavnice.

Druga generacija:

```
VuDownloadActivityData ::= SEQUENCE {
   downloadingTime                        TimeReal,
   fullCardNumberAndGeneration            FullCardNumberAndGeneration,
   companyOrWorkshopName                  Name
}
```

Namesto fullCardNumber struktura podatkov druge generacije uporablja naslednji podatkovni element.

fullCardNumberAndGeneration identificira kartico, vključno z njeno generacijo, ki je bila uporabljena za odobritev prenosa.

2.196. **VuDownloadActivityDataRecordArray**

Druga generacija:

informacija, povezana z zadnjim prenosom podatkov iz enote v vozilu (zahteva 129 iz Priloge 1C).

```
VuDownloadActivityDataRecordArray ::= SEQUENCE {
   recordType                             RecordType,
   recordSize                             INTEGER(1..65535),
   noOfRecords                            INTEGER(0..65535),
   records                                SET SIZE(noOfRecords) OF VuDownloadActivityData
}
```

recordType označuje vrsto zapisa (VuDownloadActivityData). **Dodeljena vrednost**: glej RecordType.

recordSize je v bajtih izražena velikost VuDownloadActivityData.

noOfRecords je število zapisov, ki jih vsebuje množica zapisov.

▼B

records je množica zapisov podatkov o prenosih podatkov.

2.197. **VuEventData**

Prva generacija:

informacija, shranjena v enoti v vozilu, povezana z dogodki (zahteva 094 iz Priloge 1B, razen dogodkov prekoračitve hitrosti).

```
VuEventData ::= SEQUENCE {
   noOfVuEvents                          INTEGER(0..255),
   vuEventRecords                        SET SIZE(noOfVuEvents) OF VuEventRecord
}
```

noOfVuEvents je število dogodkov, navedenih v množici vuEventRecords.

vuEventRecords je množica zapisov dogodkov.

2.198. **VuEventRecord**

Informacija, shranjena v enoti v vozilu, povezana z dogodkom (zahteva 094 iz Priloge 1B in zahteva 117 iz Priloge 1C, razen dogodkov prekoračitve hitrosti).

Prva generacija:

```
VuEventRecord ::= SEQUENCE {
   eventType                             EventFaultType,
   eventRecordPurpose                    EventFaultRecordPurpose,
   eventBeginTime                        TimeReal,
   eventEndTime                          TimeReal,
   cardNumberDriverSlotBegin             FullCardNumber,
   cardNumberCodriverSlotBegin           FullCardNumber,
   cardNumberDriverSlotEnd               FullCardNumber,
   cardNumberCodriverSlotEnd             FullCardNumber,
   similarEventsNumber                   SimilarEventsNumber
}
```

eventType je vrsta dogodka.

eventRecordPurpose je namen, za katerega je bil ta dogodek zapisan.

eventBeginTime je datum in čas začetka dogodka.

eventEndTime je datum in čas konca dogodka.

cardNumberDriverSlotBegin identificira kartico, vstavljeno v voznikovo režo ob začetku dogodka.

cardNumberCodriverSlotBegin identificira kartico, vstavljeno v sovoznikovo režo ob začetku dogodka.

cardNumberDriverSlotEnd identificira kartico, vstavljeno v voznikovo režo ob koncu dogodka.

cardNumberCodriverSlotEnd identificira kartico, vstavljeno v sovoznikovo režo ob koncu dogodka.

similarEventsNumber je število podobnih dogodkov v danem dnevu.

Ta niz se lahko uporablja za vse dogodke razen dogodkov prekoračitve hitrosti.

▼B

Druga generacija:

```
VuEventRecord ::= SEQUENCE {
   eventType                              EventFaultType,
   eventRecordPurpose                     EventFaultRecordPurpose,
   eventBeginTime                         TimeReal,
   eventEndTime                           TimeReal,
   cardNumberAndGenDriverSlotBegin        FullCardNumberAndGeneration,
   cardNumberAndGenCodriverSlotBegin      FullCardNumberAndGeneration,
   cardNumberAndGenDriverSlotEnd          FullCardNumberAndGeneration,
   cardNumberAndGenCodriverSlotEnd        FullCardNumberAndGeneration,
   similarEventsNumber                    SimilarEventsNumber,
   manufacturerSpecificEventFaultData   ManufacturerSpecificEventFaultData
}
```

Poleg elementov za prvo generacijo se uporabljajo še naslednji podatkovni elementi:

manufacturerSpecificEventFaultData vsebuje dodatne informacije o dogodku, ki jih določi proizvajalec.

Namesto cardNumberDriverSlotBegin, cardNumberCodriverSlotBegin, cardNumberDriverSlotEnd in cardNumberCodriverSlotEnd struktura podatkov druge generacije uporablja naslednje podatkovne elemente:

cardNumberAndGenDriverSlotBegin identificira kartico, vključno z njeno generacijo, vstavljeno v voznikovo režo ob začetku dogodka.

cardNumberAndGenCodriverSlotBegin identificira kartico, vključno z njeno generacijo, vstavljeno v sovoznikovo režo ob začetku dogodka.

cardNumberAndGenDriverSlotEnd identificira kartico, vključno z njeno generacijo, vstavljeno v voznikovo režo ob koncu dogodka.

cardNumberAndGenCodriverSlotEnd identificira kartico, vključno z njeno generacijo, vstavljeno v sovoznikovo režo ob koncu dogodka.

Če je dogodek v časovnem navzkrižju, se eventBeginTime in eventEndTime razumeta kot:

eventBeginTime je datum in čas zapisovalne naprave.

eventEndTime je datum in čas GNSS.

2.199. **VuEventRecordArray**

Druga generacija:

informacija, shranjena v enoti v vozilu, povezana z dogodki (zahteva 117 iz Priloge 1C, razen dogodkov prekoračitve hitrosti).

```
VuEventRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF VuEventRecord
}
```

recordType označuje vrsto zapisa (VuEventRecord). **Dodeljena vrednost**: glej RecordType.

▼B

recordSize je v bajtih izražena velikost VuEventRecord.

noOfRecords je število zapisov, ki jih vsebuje množica zapisov.

records je množica zapisov dogodkov.

2.200. **VuFaultData**

Prva generacija:

informacija, shranjena v enoti v vozilu, povezana z napakami (zahteva 096 iz Priloge 1B).

```
VuFaultData ::= SEQUENCE {
   noOfVuFaults                          INTEGER(0..255),
   vuFaultRecords                        SET SIZE(noOfVuFaults) OF VuFaultRecord
}
```

noOfVuFaults je število napak iz množice vuFaultRecords.

vuFaultRecords je množica zapisov napak.

2.201. **VuFaultRecord**

Informacija, shranjena v enoti v vozilu, povezana z napako (zahteva 096 iz Priloge 1B in zahteva 118 iz Priloge 1C).

Prva generacija:

```
VuFaultRecord ::= SEQUENCE {
   faultType                             EventFaultType,
   faultRecordPurpose                    EventFaultRecordPurpose,
   faultBeginTime                        TimeReal,
   faultEndTime                          TimeReal,
   cardNumberDriverSlotBegin             FullCardNumber,
   cardNumberCodriverSlotBegin           FullCardNumber,
   cardNumberDriverSlotEnd               FullCardNumber,
   cardNumberCodriverSlotEnd             FullCardNumber
}
```

faultType je vrsta napake zapisovalne naprave.

faultRecordPurpose je namen, za katerega je bila ta napaka zapisana.

faultBeginTime je datum in čas začetka napake.

faultEndTime je datum in čas konca napake.

cardNumberDriverSlotBegin identificira kartico, vstavljeno v voznikovo režo ob začetku napake.

cardNumberCodriverSlotBegin identificira kartico, vstavljeno v sovoznikovo režo ob začetku napake.

cardNumberDriverSlotEnd identificira kartico, vstavljeno v voznikovo režo ob koncu napake.

cardNumberCodriverSlotEnd identificira kartico, vstavljeno v sovoznikovo režo ob koncu napake.

▼B

Druga generacija:

```
VuFaultRecord ::= SEQUENCE {
   faultType                              EventFaultType,
   faultRecordPurpose                     EventFaultRecordPurpose,
   faultBeginTime                         TimeReal,
   faultEndTime                           TimeReal,
   cardNumberAndGenDriverSlotBegin        FullCardNumberAndGeneration,
   cardNumberAndGenCodriverSlotBegin      FullCardNumberAndGeneration,
   cardNumberAndGenDriverSlotEnd          FullCardNumberAndGeneration,
   cardNumberAndGenCodriverSlotEnd        FullCardNumberAndGeneration,
   manufacturerSpecificEventFaultData   ManufacturerSpecificEventFaultData
}
```

Poleg elementov za prvo generacijo se uporablja še naslednji podatkovni element:

manufacturerSpecificEventFaultData vsebuje dodatne informacije o napaki, ki jih določi proizvajalec.

Namesto cardNumberDriverSlotBegin, cardNumberCodriverSlotBegin, cardNumberDriverSlotEnd in cardNumberCodriverSlotEnd struktura podatkov druge generacije uporablja naslednje podatkovne elemente:

cardNumberAndGenDriverSlotBegin identificira kartico, vključno z njeno generacijo, vstavljeno v voznikovo režo ob začetku napake.

cardNumberAndGenCodriverSlotBegin identificira kartico, vključno z njeno generacijo, vstavljeno v sovoznikovo režo ob začetku napake.

cardNumberAndGenDriverSlotEnd identificira kartico, vključno z njeno generacijo, vstavljeno v voznikovo režo ob koncu napake.

cardNumberAndGenCodriverSlotEnd identificira kartico, vključno z njeno generacijo, vstavljeno v sovoznikovo režo ob koncu napake.

2.202. **VuFaultRecordArray**

Druga generacija:

informacija, shranjena v enoti v vozilu, povezana z napakami (zahteva 118 iz Priloge 1C).

```
VuFaultRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF VuFaultRecord
}
```

recordType označuje vrsto zapisa (VuFaultRecord). **Dodeljena vrednost**: glej RecordType.

recordSize je v bajtih izražena velikost VuFaultRecord.

noOfRecords je število zapisov, ki jih vsebuje množica zapisov.

records je množica zapisov napak.

▼B

2.203. **VuGNSSCDRecord**

Druga generacija:

informacija, shranjena v enoti v vozilu, povezana z GNSS položajem vozila, če čas neprekinjene vožnje voznika doseže večkratnik treh ur (zahtevi 108 in 110 iz Priloge 1C).

```
VuGNSSCDRecord ::= SEQUENCE {
   timeStamp                          TimeReal,
   cardNumberAndGenDriverSlot         FullCardNumberAndGeneration,
   cardNumberAndGenCodriverSlot       FullCardNumberAndGeneration,
   gnssPlaceRecord                    GNSSPlaceRecord
}
```

timeStamp je datum in čas, ko čas neprekinjene vožnje imetnika kartice doseže večkratnik treh ur.

cardNumberAndGenDriverSlot identificira kartico, vstavljeno v voznikovo režo, vključno z njeno generacijo.

cardNumberAndGenCodriverSlot identificira kartico, vstavljeno v sovoznikovo režo, vključno z njeno generacijo.

gnssPlaceRecord vsebuje informacijo, povezano s položajem vozila.

2.204. **VuGNSSCDRecordArray**

Druga generacija:

informacija, shranjena v enoti v vozilu, povezana z GNSS položajem vozila, če čas neprekinjene vožnje voznika doseže večkratnik treh ur (zahtevi 108 in 110 iz Priloge 1C).

```
VuGNSSCDRecordArray  ::= SEQUENCE {
   recordType                         RecordType,
   recordSize                         INTEGER(1..65535),
   noOfRecords                        INTEGER(0..65535),
   records                            SET SIZE(noOfRecords) OF VuGNSSCDRecord
}
```

recordType označuje vrsto zapisa (VuGNSSCDRecord). **Dodeljena vrednost**: glej RecordType.

recordSize je v bajtih izražena velikost VuGNSSCDRecord.

noOfRecords je število zapisov, ki jih vsebuje množica zapisov.

records je množica zapisov neprekinjene vožnje GNSS.

2.205. **VuIdentification**

Informacija, shranjena v enoti v vozilu, povezana z identifikacijo enote v vozilu (zahteva 075 iz Priloge 1B ter zahtevi 93 in 121 iz Priloge 1C).

▼B

Prva generacija:

```
VuIdentification ::= SEQUENCE {
   vuManufacturerName                    VuManufacturerName,
   vuManufacturerAddress                 VuManufacturerAddress,
   vuPartNumber                          VuPartNumber,
   vuSerialNumber                        VuSerialNumber,
   vuSoftwareIdentification              VuSoftwareIdentification,
   vuManufacturingDate                   VuManufacturingDate,
   vuApprovalNumber                      VuApprovalNumber
}
```

vuManufacturerName je ime proizvajalca enote v vozilu.

vuManufacturerAddress je naslov proizvajalca enote v vozilu.

vuPartNumber je kataloška številka enote v vozilu.

vuSerialNumber je serijska številka enote v vozilu.

vuSoftwareIdentification identificira programsko opremo, ki se uporablja v enoti v vozilu.

vuManufacturingDate je datum izdelave enote v vozilu.

vuApprovalNumber je homologacijska številka enote v vozilu.

Druga generacija:

```
VuIdentification ::= SEQUENCE {
   vuManufacturerName                    VuManufacturerName,
   vuManufacturerAddress                 VuManufacturerAddress,
   vuPartNumber                          VuPartNumber,
   vuSerialNumber                        VuSerialNumber,
   vuSoftwareIdentification              VuSoftwareIdentification,
   vuManufacturingDate                   VuManufacturingDate,
   vuApprovalNumber                      VuApprovalNumber,
   vuGeneration                          Generation,
   vuAbility                             VuAbility
}
```

Poleg elementov za prvo generacijo se uporabljata še naslednja podatkovna elementa:

vuGeneration identificira generacijo enote v vozilu.

vuAbility daje informacijo, ali enota v vozilu podpira tahografske kartice prve generacije.

2.206. **VuIdentificationRecordArray**

Druga generacija:

VuIdentification in metapodatki, uporabljeni v protokolu za prenos.

▼B

```
VuIdentificationRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF VuIdentification
}
```

recordType označuje vrsto zapisa (VuIdentification). **Dodeljena vrednost**: glej RecordType.

recordSize je v bajtih izražena velikost VuIdentification.

noOfRecords je število zapisov, ki jih vsebuje množica zapisov.

records je množica zapisov VuIdentification.

2.207. **VuITSConsentRecord**

Druga generacija:

informacija, shranjena v enoti v vozilu, povezana s privolitvijo voznika v uporabo inteligentnih prevoznih sistemov.

```
VuITSConsentRecord ::= SEQUENCE {
   cardNumberAndGen                    FullCardNumberAndGeneration,
   consent                             BOOLEAN
}
```

cardNumberAndGen identificira kartico, vključno z njeno generacijo. Mora biti vozniška kartica ali kartica servisne delavnice.

consent je zastavica, ki pove, ali je voznik privolil v uporabo inteligentnih prevoznih sistemov s tem vozilom/enoto v vozilu.

Dodeljena vrednost:

TRUE	označuje voznikovo privolitev v uporabo inteligentnih prometnih sistemov
FALSE	označuje voznikovo zavrnitev uporabe inteligentnih prometnih sistemov.

2.208. **VuITSConsentRecordArray**

Druga generacija:

informacija, shranjena v enoti v vozilu, povezana s privolitvijo voznika v uporabo inteligentnih prevoznih sistemov (zahteva 200 iz Priloge 1C)

```
VuITSConsentRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF VuITSConsentRecord
}
```

recordType označuje vrsto zapisa (VuITSConsentRecord). **Dodeljena vrednost**: glej RecordType.

recordSize je v bajtih izražena velikost VuITSConsentRecord.

noOfRecords je število zapisov, ki jih vsebuje množica zapisov.

records je množica zapisov o privolitvi v uporabo ITS.

▼B

2.209. **VuManufacturerAddress**

Naslov proizvajalca enote v vozilu.

```
VuManufacturerAddress ::= Address
```

Dodeljena vrednost: ni določena.

2.210. **VuManufacturerName**

Ime proizvajalca enote v vozilu.

```
VuManufacturerName ::= Name
```

Dodeljena vrednost: ni določena.

2.211. **VuManufacturingDate**

Datum proizvodnje enote v vozilu.

```
VuManufacturingDate ::= TimeReal
```

Dodeljena vrednost: ni določena.

2.212. **VuOverSpeedingControlData**

Informacija, shranjena v enoti v vozilu, povezana z dogodki prekoračitev hitrosti od zadnjega nadzora prekoračitev hitrosti (zahteva 095 iz Priloge 1B in zahteva 117 iz Priloge 1C).

```
VuOverSpeedingControlData ::= SEQUENCE {
   lastOverspeedControlTime             TimeReal,
   firstOverspeedSince                  TimeReal,
   numberOfOverspeedSince               OverspeedNumber
}
```

lastOverspeedControlTime je datum in čas zadnjega nadzora prekoračitve hitrosti.

firstOverspeedSince je datum in čas prve prekoračitve hitrosti po tem nadzoru prekoračitve hitrosti.

numberOfOverspeedSince je število dogodkov prekoračitve hitrosti od zadnjega nadzora prekoračitve hitrosti.

2.213. **VuOverSpeedingControlDataRecordArray**

Druga generacija:

VuOverSpeedingControlData in metapodatki, uporabljeni v protokolu za prenos.

```
VuOverSpeedingControlDataRecordArray ::= SEQUENCE {
   recordType                           RecordType,
   recordSize                           INTEGER(1..65535),
   noOfRecords                          INTEGER(0..65535),
   records                              SET SIZE(noOfRecords) OF
                                        VuOverSpeedingControlData
}
```

▼B

recordType označuje vrsto zapisa (VuOverSpeedingControlData). **Dodeljena vrednost**: glej RecordType.

recordSize je v bajtih izražena velikost VuOverSpeedingControlData.

noOfRecords je število zapisov, ki jih vsebuje množica zapisov.

records je množica zapisov nadzornih podatkov o prekoračitvah hitrosti.

2.214. **VuOverSpeedingEventData**

Prva generacija:

informacija, shranjena v enoti v vozilu, povezana z dogodki prekoračitev hitrosti (zahteva 094 iz Priloge 1B).

```
VuOverSpeedingEventData ::= SEQUENCE {
   noOfVuOverSpeedingEvents              INTEGER(0..255),
   vuOverSpeedingEventRecords            SET SIZE(noOfVuOverSpeedingEvents) OF
                                         VuOverSpeedingEventRecord
}
```

noOfVuOverSpeedingEvents je število dogodkov, navedenih v množici vuOverSpeedingEventRecords.

vuOverSpeedingEventRecords je množica zapisov dogodkov prekoračitev hitrosti.

2.215. **VuOverSpeedingEventRecord**

Prva generacija:

informacija, shranjena v enoti v vozilu, povezana z dogodki prekoračitev hitrosti (zahteva 094 iz Priloge 1B in zahteva 117 iz Priloge 1C).

```
VuOverSpeedingEventRecord ::= SEQUENCE {
   eventType                             EventFaultType,
   eventRecordPurpose                    EventFaultRecordPurpose,
   eventBeginTime                        TimeReal,
   eventEndTime                          TimeReal,
   maxSpeedValue                         SpeedMax,
   averageSpeedValue                     SpeedAverage,
   cardNumberDriverSlotBegin             FullCardNumber,
   similarEventsNumber                   SimilarEventsNumber
}
```

eventType je vrsta dogodka.

eventRecordPurpose je namen, za katerega je bil ta dogodek zapisan.

eventBeginTime je datum in čas začetka dogodka.

eventEndTime je datum in čas konca dogodka.

maxSpeedValue je najvišja hitrost, izmerjena med dogodkom.

averageSpeedValue je aritmetična sredina hitrosti, izmerjenih med dogodkom.

▼B

cardNumberDriverSlotBegin identificira kartico, vstavljeno v voznikovo režo ob začetku dogodka.

similarEventsNumber je število podobnih dogodkov v danem dnevu.

Druga generacija:

informacija, shranjena v enoti v vozilu, povezana z dogodki prekoračitev hitrosti (zahteva 094 iz Priloge 1B in zahteva 117 iz Priloge 1C).

```
VuOverSpeedingEventRecord ::= SEQUENCE {
   eventType                              EventFaultType,
   eventRecordPurpose                     EventFaultRecordPurpose,
   eventBeginTime                         TimeReal,
   eventEndTime                           TimeReal,
   maxSpeedValue                          SpeedMax,
   averageSpeedValue                      SpeedAverage,
   cardNumberAndGenDriverSlotBegin        FullCardNumberAndGeneration,
   similarEventsNumber                    SimilarEventsNumber
}
```

Namesto cardNumberDriverSlotBegin struktura podatkov druge generacije uporablja naslednji podatkovni element:

cardNumberAndGenDriverSlotBegin identificira kartico, vključno z njeno generacijo, vstavljeno v voznikovo režo ob začetku dogodka.

2.216. **VuOverSpeedingEventRecordArray**

Druga generacija:

informacija, shranjena v enoti v vozilu, povezana z dogodki prekoračitev hitrosti (zahteva 117 iz Priloge 1C).

```
VuOverSpeedingEventRecordArray ::= SEQUENCE {
   recordType                             RecordType,
   recordSize                             INTEGER(1..65535),
   noOfRecords                            INTEGER(0..65535),
   records                                SET SIZE(noOfRecords) OF
                                          VuOverSpeedingEventRecord
}
```

recordType označuje vrsto zapisa (VuOverSpeedingEventRecord).
Dodeljena vrednost: glej RecordType.

recordSize je v bajtih izražena velikost VuOverSpeedingEventRecord.

noOfRecords je število zapisov, ki jih vsebuje množica zapisov.

records je množica zapisov dogodkov prekoračitev hitrosti.

2.217. **VuPartNumber**

Številka dela enote v vozilu.

```
VuPartNumber ::= IA5String(SIZE(16))
```

Dodeljena vrednost: določi proizvajalec VU.

▼B

2.218. **VuPlaceDailyWorkPeriodData**

Prva generacija:

informacija, shranjena v enoti v vozilu, povezana s kraji začetkov in koncev dnevnih delovnih izmen voznikov (zahteva 087 iz Priloge 1B ter zahtevi 108 in 110 iz Priloge 1C).

```
VuPlaceDailyWorkPeriodData ::= SEQUENCE {
   noOfPlaceRecords                    INTEGER(0..255),
   vuPlaceDailyWorkPeriodRecords       SET SIZE(noOfPlaceRecords) OF
                                       VuPlaceDailyWorkPeriodRecord
}
```

noOfPlaceRecords je število zapisov v množici vuPlaceDailyWorkPeriodRecords.

vuPlaceDailyWorkPeriodRecords je množica zapisov o krajih.

2.219. **VuPlaceDailyWorkPeriodRecord**

Prva generacija:

informacija, shranjena v enoti v vozilu, povezana s krajem, kjer voznik začne ali konča dnevno delovno izmeno (zahteva 087 iz Priloge 1B ter zahtevi 108 in 110 iz Priloge 1C).

```
VuPlaceDailyWorkPeriodRecord ::= SEQUENCE {
   fullCardNumber                      FullCardNumber,
   placeRecord                         PlaceRecord
}
```

fullCardNumber je vrsta vozniške kartice, država izdajateljica in številka kartice.

placeRecord vsebuje informacije, povezane z vnesenim krajem.

Druga generacija:

informacija, shranjena v enoti v vozilu, povezana s krajem, kjer voznik začne ali konča dnevno delovno izmeno (zahteva 087 iz Priloge 1B ter zahtevi 108 in 110 iz Priloge 1C).

```
VuPlaceDailyWorkPeriodRecord ::= SEQUENCE {
   fullCardNumberAndGeneration         FullCardNumberAndGeneration,
   placeRecord                         PlaceRecord
}
```

Namesto fullCardNumber struktura podatkov druge generacije uporablja naslednji podatkovni element:

fullCardNumberAndGeneration je vrsta kartice, njena država izdajateljica, številka kartice in njena generacija, kot so shranjene na kartici.

▼B

2.220. **VuPlaceDailyWorkPeriodRecordArray**

Druga generacija:

informacija, shranjena v enoti v vozilu, povezana s kraji začetkov in koncev dnevne delovne izmene voznikov (zahtevi 108 in 110 iz Priloge 1C).

```
VuPlaceDailyWorkPeriodRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF
                                       VuPlaceDailyWorkPeriodRecord
}
```

recordType označuje vrsto zapisa (VuPlaceDailyWorkPeriodRecord). **Dodeljena vrednost**: glej RecordType.

recordSize je v bajtih izražena velikost VuPlaceDailyWorkPeriodRecord.

noOfRecords je število zapisov, ki jih vsebuje množica zapisov.

records je množica zapisov o krajih.

2.221. **VuPrivateKey**

Prva generacija:

zasebni ključ enote v vozilu.

```
VuPrivateKey ::= RSAKeyPrivateExponent
```

2.222. **VuPublicKey**

Prva generacija:

javni ključ enote v vozilu.

```
VuPublicKey ::= PublicKey
```

2.223. **VuSerialNumber**

Serijska številka enote v vozilu (zahteva 075 iz Priloge 1B in zahteva 93 iz Priloge 1C).

```
VuSerialNumber ::= ExtendedSerialNumber
```

2.224. **VuSoftInstallationDate**

Datum namestitve različice programske opreme enote v vozilu.

```
VuSoftInstallationDate ::= TimeReal
```

Dodeljena vrednost: ni določena.

▼B

2.225. **VuSoftwareIdentification**

Informacija, shranjena v enoti v vozilu, povezana z nameščeno programsko opremo.

```
VuSoftwareIdentification ::= SEQUENCE {
   vuSoftwareVersion                    VuSoftwareVersion,
   vuSoftInstallationDate               VuSoftInstallationDate
}
```

vuSoftwareVersion je različica programske opreme enote v vozilu.

vuSoftInstallationDate je datum namestitve programske opreme.

2.226. **VuSoftwareVersion**

Številka različice programske opreme enote v vozilu.

```
VuSoftwareVersion ::= IA5String(SIZE(4))
```

Dodeljena vrednost: ni določena.

2.227. **VuSpecificConditionData**

Prva generacija:

informacija, shranjena v enoti v vozilu, povezana s posebnimi stanji.

```
VuSpecificConditionData ::= SEQUENCE {
   noOfSpecificConditionRecords         INTEGER(0..2^16-1)
   specificConditionRecords             SET SIZE (noOfSpecificConditionRecords) OF
                                        SpecificConditionRecord
}
```

noOfSpecificConditionRecords je število zapisov v množici specificConditionRecords.

specificConditionRecords je množica zapisov o posebnih stanjih.

2.228. **VuSpecificConditionRecordArray**

Druga generacija:

informacija, shranjena v enoti v vozilu, povezana s posebnimi stanji (zahteva 130 iz Priloge 1C).

```
VuSpecificConditionRecordArray ::= SEQUENCE {
   recordType                           RecordType,
   recordSize                           INTEGER(1..65535),
   noOfRecords                          INTEGER(0..65535),
   records                              SET SIZE(noOfRecords) OF
                                        SpecificConditionRecord
}
```

recordType označuje vrsto zapisa (SpecificConditionRecord). **Dodeljena vrednost**: glej RecordType.

recordSize je v bajtih izražena velikost SpecificConditionRecord.

noOfRecords je število zapisov, ki jih vsebuje množica zapisov.

records je množica zapisov o posebnih stanjih.

▼B

2.229. **VuTimeAdjustmentData**

Prva generacija:

informacija, shranjena v enoti v vozilu, povezana z nastavljanji časa, opravljenimi izven okvira rednih kalibracij (zahteva 101 iz Priloge 1B).

```
VuTimeAdjustmentData ::= SEQUENCE {
   noOfVuTimeAdjRecords                    INTEGER(0..6),
   vuTimeAdjustmentRecords                 SET SIZE(noOfVuTimeAdjRecords) OF
                                           VuTimeAdjustmentRecord
}
```

noOfVuTimeAdjRecords je število zapisov v vuTimeAdjustmentRecords**.**

vuTimeAdjustmentRecords je množica zapisov o nastavljanju časa.

2.230. **VuTimeAdjustmentGNSSRecord**

Druga generacija:

informacija, shranjena v enoti v vozilu, povezana z nastavljanjem časa na podlagi časovnih podatkov iz GNSS (zahtevi 124 in 125 iz Priloge 1C).

```
VuTimeAdjustmentGNSSRecord ::= SEQUENCE {
   oldTimeValue                            TimeReal,
   newTimeValue                            TimeReal
}
```

oldTimeValue, newTimeValue sta stara in nova vrednost datuma in časa.

2.231. **VuTimeAdjustmentGNSSRecordArray**

Druga generacija:

informacija, shranjena v enoti v vozilu, povezana z nastavljanjem časa, opravljenim na podlagi časovnih podatkov iz GNSS (zahtevi 124 in 125 iz Priloge 1C).

```
VuTimeAdjustmentGNSSRecordArray ::= SEQUENCE {
   recordType                              RecordType,
   recordSize                              INTEGER(1..65535),
   noOfRecords                             INTEGER(0..65535),
   records                                 SET SIZE(noOfRecords) OF
                                           VuTimeAdjustmentGNSSRecord
}
```

recordType označuje vrsto zapisa (VuTimeAdjustmentGNSSRecord). **Dodeljena vrednost**: glej RecordType.

recordSize je v bajtih izražena velikost VuTimeAdjustmentGNSSRecord.

noOfRecords je število zapisov, ki jih vsebuje množica zapisov.

records je množica zapisov nastavljanja časa GNSS.

▼B

2.232. **VuTimeAdjustmentRecord**

Informacija, shranjena v enoti v vozilu, povezana z nastavljanjem časa, opravljenim izven okvira rednih kalibracij (zahteva 101 iz Priloge 1B ter zahtevi 124 in 125 iz Priloge 1C).

Prva generacija:

```
VuTimeAdjustmentRecord ::= SEQUENCE {
   oldTimeValue                          TimeReal,
   newTimeValue                          TimeReal,
   workshopName                          Name,
   workshopAddress                       Address,
   workshopCardNumber                    FullCardNumber
}
```

oldTimeValue, newTimeValue sta stara in nova vrednost datuma in časa.

workshopName, workshopAddress sta ime in naslov servisne delavnice.

workshopCardNumber identificira kartico servisne delavnice, uporabljeno za nastavljanje časa.

Druga generacija:

```
VuTimeAdjustmentRecord ::= SEQUENCE {
   oldTimeValue                          TimeReal,
   newTimeValue                          TimeReal,
   workshopName                          Name,
   workshopAddress                       Address,
   workshopCardNumberAndGeneration       FullCardNumberAndGeneration
}
```

Namesto workshopCardNumber struktura podatkov druge generacije uporablja naslednji podatkovni element.

workshopCardNumberAndGeneration identificira kartico servisne delavnice, uporabljeno za nastavljanje časa, vključno z njeno generacijo.

2.233. **VuTimeAdjustmentRecordArray**

Druga generacija:

informacija, shranjena v enoti v vozilu, povezana z nastavitvami časa, opravljenimi izven okvira rednih kalibracij (zahtevi 124 in 125 iz Priloge 1C).

```
VuTimeAdjustmentRecordArray ::= SEQUENCE {
   recordType                            RecordType,
   recordSize                            INTEGER(1..65535),
   noOfRecords                           INTEGER(0..65535),
   records                               SET SIZE(noOfRecords) OF
                                         VuTimeAdjustmentRecord
}
```

recordType označuje vrsto zapisa (VuTimeAdjustmentRecord). **Dodeljena vrednost**: glej RecordType.

recordSize je v bajtih izražena velikost VuTimeAdjustmentRecord.

▼B

noOfRecords je število zapisov, ki jih vsebuje množica zapisov.

records je množica zapisov nastavljanja časa.

2.234. **WorkshopCardApplicationIdentification**

Informacija, shranjena na kartici servisne delavnice, povezana z identifikacijo aplikacije kartice (zahtevi 307 in 330 iz Priloge 1C).

Prva generacija:

```
WorkshopCardApplicationIdentification ::= SEQUENCE {
   typeOfTachographCardId               EquipmentType,
   cardStructureVersion                 CardStructureVersion,
   noOfEventsPerType                    NoOfEventsPerType,
   noOfFaultsPerType                    NoOfFaultsPerType,
   activityStructureLength              CardActivityLengthRange,
   noOfCardVehicleRecords               NoOfCardVehicleRecords,
   noOfCardPlaceRecords                 NoOfCardPlaceRecords,
   noOfCalibrationRecords               NoOfCalibrationRecords
}
```

typeOfTachographCardId določa uporabljeno vrsto kartice.

cardStructureVersion določa različico uporabljene strukture na kartici.

noOfEventsPerType je število dogodkov posamezne vrste, ki jih lahko zapiše kartica.

noOfFaultsPerType je število napak posamezne vrste, ki jih lahko zapiše kartica.

activityStructureLength označuje število razpoložljivih bajtov za hranjenje zapisov dejavnosti.

noOfCardVehicleRecords je število zapisov vozila, ki jih lahko vsebuje kartica.

noOfCardPlaceRecords je število krajev, ki jih lahko zapiše kartica.

noOfCalibrationRecords je število zapisov o kalibraciji, ki jih lahko hrani kartica.

Druga generacija:

```
WorkshopCardApplicationIdentification ::= SEQUENCE {
   typeOfTachographCardId               EquipmentType,
   cardStructureVersion                 CardStructureVersion,
   noOfEventsPerType                    NoOfEventsPerType,
   noOfFaultsPerType                    NoOfFaultsPerType,
   activityStructureLength              CardActivityLengthRange,
   noOfCardVehicleRecords               NoOfCardVehicleRecords,
   noOfCardPlaceRecords                 NoOfCardPlaceRecords,
   noOfCalibrationRecords               NoOfCalibrationRecords,
   noOfGNSSCDRecords                    NoOfGNSSCDRecords,
   noOfSpecificConditionRecords         NoOfSpecificConditionRecords
}
```

Poleg elementov za prvo generacijo se uporabljajo naslednji podatkovni elementi:

noOfGNSSCDRecords je število zapisov neprekinjene vožnje GNSS, ki jih lahko hrani kartica.

▼B

noOfSpecificConditionRecords je število zapisov posebnih pogojev, ki jih lahko hrani kartica.

2.235. **WorkshopCardCalibrationData**

Informacija, shranjena na kartici servisne delavnice, povezana z dejavnostmi servisne delavnice, opravljenimi s kartico (zahteve 314, 316, 337 in 339 iz Priloge 1C).

```
WorkshopCardCalibrationData ::= SEQUENCE {
   calibrationTotalNumber              INTEGER(0 .. 2^16-1),
   calibrationPointerNewestRecord      INTEGER(0 .. NoOfCalibrationRecords-1),
   calibrationRecords                  SET SIZE(NoOfCalibrationRecords) OF
                                       WorkshopCardCalibrationRecord
}
```

calibrationTotalNumber je skupno število kalibracij, opravljenih s kartico.

calibrationPointerNewestRecord je indeks zadnjega posodobljenega zapisa o kalibraciji.

Dodeljena vrednost: število, ki ustreza številu zapisa o kalibraciji; začne se z vrednostjo ‘0’ za prvi zapis o kalibraciji v strukturi.

calibrationRecords je množica zapisov informacij o kalibraciji in/ali nastavljanju časa.

2.236. **WorkshopCardCalibrationRecord**

Informacija, shranjena na kartici servisne delavnice, povezana s kalibracijo, opravljeno s kartico (zahtevi 314 in 337 iz Priloge 1C).

Prva generacija:

```
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 je namen kalibracije.

vehicleIdentificationNumber je VIN.

vehicleRegistration vsebuje registrsko številko vozila in državo, kateri je registrirano.

wVehicleCharacteristicConstant je značilni koeficient vozila.

▼B

kConstantOfRecordingEquipment je konstanta zapisovalne naprave.

lTyreCircumference je dejanski obseg pnevmatik.

tyreSize je oznaka mer pnevmatik na vozilu.

authorisedSpeed je največja dovoljena hitrost vozila.

oldOdometerValue, newOdometerValue sta stara in nova vrednost števca prevožene poti.

oldTimeValue, newTimeValue sta stara in nova vrednost datuma in časa.

nextCalibrationDate je datum, na katerega naj se opravi naslednja kalibracija vrste, označene v CalibrationPurpose, pri pooblaščenem inšpekcijskem organu.

vuPartNumber, **vuSerialNumber** in **sensorSerialNumber** so podatkovni elementi za identifikacijo zapisovalne naprave.

Druga generacija:

```
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
}
```

Poleg elementov za prvo generacijo se uporabljajo naslednji podatkovni elementi:

sensorGNSSSerialNumber, ki identificira zunanjo GNSS opremo.

rcmSerialNumber, ki identificira modul za komunikacijo na daljavo.

sealDataCard nudi informacije o pečatih, ki so pritrjeni na različne sestavne dele vozila.

▼B

2.237. **WorkshopCardHolderIdentification**

Informacija, shranjena na kartici servisne delavnice, povezana z identifikacijo imetnika kartice (zahtevi 311 in 334 iz Priloge 1C).

```
WorkshopCardHolderIdentification ::= SEQUENCE {
   workshopName                        Name,
   workshopAddress                     Address,
   cardHolderName                      HolderName,
   cardHolderPreferredLanguage         Language
}
```

workshopName je ime servisne delavnice imetnika kartice.

workshopAddress je naslov servisne delavnice imetnika kartice.

cardHolderName je priimek in ime(na) imetnika (tj. ime mehanika).

cardHolderPreferredLanguage je izbrani jezik imetnika kartice.

2.238. **WorkshopCardPIN**

Osebna identifikacijska številka kartice servisne delavnice (zahtevi 309 in 332 iz Priloge 1C).

```
WorkshopCardPIN ::= IA5String(SIZE(8))
```

Dodeljena vrednost: koda PIN, znana imetniku, desno napolnjena z vrednostmi ‘FF’ do 8 bajtov.

2.239. **W-VehicleCharacteristicConstant**

Značilni koeficient vozila (opredelitev k)).

```
W-VehicleCharacteristicConstant ::= INTEGER(0..2^16-1))
```

Dodeljena vrednost: število impulzov na kilometer v območju od 0 do 64 255 pulzov/km.

2.240. **VuPowerSupplyInterruptionRecord**

Druga generacija:

informacija, shranjena v enoti v vozilu, povezana z dogodki izpada napajanja (zahteva 117 iz Priloge 1C).

```
VuPowerSupplyInterruptionRecord ::= SEQUENCE {
   eventType                           EventFaultType,
   eventRecordPurpose                  EventFaultRecordPurpose,
   eventBeginTime                      TimeReal,
   eventEndTime                        TimeReal,
   cardNumberAndGenDriverSlotBegin     FullCardNumberAndGeneration,
   cardNumberAndGenDriverSlotEnd       FullCardNumberAndGeneration,
   cardNumberAndGenCodriverSlotBegin   FullCardNumberAndGeneration,
   cardNumberAndGenCodriverSlotEnd     FullCardNumberAndGeneration,
   similarEventsNumber                 SimilarEventsNumber
}
```

eventType je vrsta dogodka.

eventRecordPurpose je namen, za katerega je bil ta dogodek zapisan.

eventBeginTime je datum in čas začetka dogodka.

▼B

eventEndTime je datum in čas konca dogodka.

cardNumberAndGenDriverSlotBegin identificira kartico, vključno z njeno generacijo, vstavljeno v voznikovo režo ob začetku dogodka.

cardNumberAndGenDriverSlotEnd identificira kartico, vključno z njeno generacijo, vstavljeno v voznikovo režo ob koncu dogodka.

cardNumberAndGenCodriverSlotBegin identificira kartico, vključno z njeno generacijo, vstavljeno v sovoznikovo režo ob začetku dogodka.

cardNumberAndGenCodriverSlotEnd identificira kartico, vključno z njeno generacijo, vstavljeno v sovoznikovo režo ob koncu dogodka.

similarEventsNumber je število podobnih dogodkov v danem dnevu.

2.241. **VuPowerSupplyInterruptionRecordArray**

Druga generacija:

informacija, shranjena v enoti v vozilu, povezana z dogodki izpada napajanja (zahteva 117 iz Priloge 1C).

```
VuPowerSupplyInterruptionRecordArray ::= SEQUENCE {
   recordType                           RecordType,
   recordSize                           INTEGER(1..65535),
   noOfRecords                          INTEGER(0..65535),
   records                              SET SIZE(noOfRecords) OF
                                        VuPowerSupplyInterruptionRecord
}
```

recordType označuje vrsto zapisa (VuPowerSupplyInterruptionRecord). **Dodeljena vrednost**: glej RecordType.

recordSize je v bajtih izražena velikost VuPowerSupplyInterruptionRecord.

noOfRecords je število zapisov, ki jih vsebuje množica zapisov.

records je množica zapisov o dogodkih izpada napajanja.

2.242. **VuSensorExternalGNSSCoupledRecordArray**

Druga generacija:

množica SensorExternalGNSSCoupledRecord in metapodatki, uporabljeni v protokolu za prenos.

```
VuSensorExternalGNSSCoupledRecordArray ::= SEQUENCE {
   recordType                           RecordType,
   recordSize                           INTEGER(1..65535),
   noOfRecords                          INTEGER(0..65535),
   records                              SET SIZE(noOfRecords) OF
                                        SensorExternalGNSSCoupledRecord
}
```

recordType označuje vrsto zapisa (SensorExternalGNSSCoupledRecord). **Dodeljena vrednost**: glej RecordType.

▼B

recordSize je v bajtih izražena velikost SensorExternalGNSSCoupledRecord.

noOfRecords je število zapisov, ki jih vsebuje množica zapisov.

records je množica zapisov o povezovanju tipala z zunanjim GNSS.

2.243. **VuSensorPairedRecordArray**

Druga generacija:

množica SensorPairedRecord in metapodatki, uporabljeni v protokolu za prenos.

```
VuSensorPairedRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF SensorPairedRecord
}
```

recordType označuje vrsto zapisa (SensorPairedRecord). **Dodeljena vrednost**: glej RecordType.

recordSize je v bajtih izražena velikost SensorPairedRecord.

noOfRecords je število zapisov, ki jih vsebuje množica zapisov.

records je množica zapisov o povezovanju tipala.

3. OPREDELITVE OBMOČIJ VREDNOSTI IN VELIKOSTI

Opredelitev vrednosti spremenljivk, uporabljenih pri opredelitvah v odstavku 2.

```
TimeRealRange ::= 2^32-1
```

4. NABORI ZNAKOV

IA5Strings uporabljajo znake ASCII, opredeljene v ISO/IEC 8824-1. Za čitljivost in lažje sklicevanje so po naraščajočih vrednostih navedeni spodaj. V primerih neskladnosti ima ISO/IEC 8824-1 prednost pred spodnjim informativnim zapisom.

```
  ! " # $ % & ' ( ) * + , - . / 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 { | } ~
```

Drugi nizi znakov (Address, Name, VehicleRegistrationNumber) uporabljajo tudi znake iz nabora decimalnih kod, v razponu 161 do 255 naslednjih 8-bitnih standardnih skupin znakov, ki jih določa številka kodne strani (*Code Page*): standardni nabor znakov	Kodna stran (decimalno)
ISO/IEC 8859-1 Latinica-1 zahodnoevropski	1
ISO/IEC 8859-2 Latinica-2 srednjeevropski	2
ISO/IEC 8859-3 Latinica-3 južnoevropski	3
ISO/IEC 8859-5 Latinica/cirilica	5
ISO/IEC 8859-7 Latinica/grški	7
ISO/IEC 8859-9 Latinica-5 turški	9

▼B

Drugi nizi znakov (Address, Name, VehicleRegistrationNumber) uporabljajo tudi znake iz nabora decimalnih kod, v razponu 161 do 255 naslednjih 8-bitnih standardnih skupin znakov, ki jih določa številka kodne strani (*Code Page*): standardni nabor znakov	Kodna stran (decimalno)
ISO/IEC 8859-13 Latinica-7 baltski obroč	13
ISO/IEC 8859-15 Latinica-9	15
ISO/IEC 8859-16 Latinica-10 jugovzhodnoevropski	16
KOI8-R Latinica/cirilica	80
KOI8-U Latinica/cirilica	85

5. KODIRANJE

Pri kodiranju po pravilih zapisa ASN.1 morajo biti vsi opredeljeni podatkovni tipi kodirani v skladu z ISO/IEC 8825-2, poravnana različica.

6. IDENTIFIKATORJI OBJEKTA IN IDENTIFIKATORJI APLIKACIJE

6.1. **Identifikatorji objekta**

Identifikatorji objekta (OID) iz tega poglavja so relevantni le za drugo generacijo. Ti OID so določeni v TR-03110-3 in so tu ponovno navedeni le zaradi celovitega prikaza. Te OID vsebuje poddrevo bsi-de:

```
bsi-de OBJECT IDENTIFIER ::= {
   itu-t(0) identified-organization(4) etsi(0)
   reserved(127) etsi-identified-organization(0) 7
}
```

Identifikatorji protokola za avtentikacijo enote v vozilu

```
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}
```

Primer: če se avtentikacija enote v vozilu opravi s SHA-384, je treba uporabiti identifikator objekta (v zapisu ASN.1) `bsi-de protocols(2) smartcard(2) 2 2 4`. Vrednost tega identifikatorja objekta v zapisu s pikami (*dot notation*) je `0.4.0.127.0.7.2.2.2.2.4`.

	Zapis s pikami (*Dot notation*)	Zapis v bajtih (*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

Identifikatorji protokola za avtentikacijo čipa

```
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}
```

Primer: če se avtentikacija čipa opravi z algoritmom ECDH, bo dolžina ključa seje AES 128 bitov. Ta ključ bo nato uporabljen v načinu delovanja CBC, da se zagotovi zaupnost, in z algoritmom CMAC, da se zagotovi avtentičnost podatkov. Zato je treba uporabiti identifikator objekta (v zapisu ASN.1) `bsi-de protocols(2) smartcard(2) 3 2 2`. Vrednost tega identifikatorja objekta v zapisu s pikami (*dot notation*) je `0.4.0.127.0.7.2.2.3.2.2`.

	Zapis s pikami (*Dot notation*)	Zapis v bajtih (*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. **Identifikatorji aplikacije**

Druga generacija:

identifikator aplikacije (AID) za zunanjo GNSS opremo (druga generacija) je podan z ‘FF 44 54 45 47 4D’. To je lastniški AID v skladu z ISO/IEC 7816-4.

Opomba: zadnjih pet bajtov kodira DTEGM za zunanjo GNSS opremo pametnega tahografa.

Identifikator aplikacije (AID) za drugo generacijo aplikacije tahografske kartice je podan z ‘FF 53 4D 52 44 54’. To je lastniški AID v skladu z ISO/IEC 7816-4.

▼B

Dodatek 2

SPECIFIKACIJA TAHOGRAFSKIH KARTIC

KAZALO

1. UVOD

1.1. Kratice

1.2. Viri

2. ELEKTRIČNE IN FIZIČNE LASTNOSTI

2.1. Napajalna napetost in poraba električnega toka

2.2. Napetost programiranja V_{pp}

2.3. Tvorba in frekvenca urnega signala

2.4. Kontakt I/O

2.5. Stanja kartice

3. STROJNA OPREMA IN KOMUNIKACIJA

3.1. Uvod

3.2. Protokol za prenos podatkov

3.2.1 Protokoli

3.2.2 ATR

3.2.3 PTS

3.3. Pravila dostopa

3.4. Pregled ukazov in kod napak

3.5. Opisi ukazov

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. STRUKTURA TAHOGRAFSKIH KARTIC

4.1. Glavna datoteka MF

4.2. Aplikacije vozniške kartice

4.2.1 Aplikacija vozniške kartice prve generacije

4.2.2 Aplikacija vozniške kartice druge generacije

4.3. Aplikacije kartice servisne delavnice

4.3.1 Aplikacija kartice servisne delavnice prve generacije

4.3.2 Aplikacija kartice servisne delavnice druge generacije

4.4. Aplikacije nadzorne kartice

4.4.1 Aplikacija nadzorne kartice prve generacije

4.4.2 Aplikacija nadzorne kartice druge generacije

4.5. Aplikacije kartice podjetja

4.5.1 Aplikacija kartice podjetja prve generacije

4.5.2 Aplikacija kartice podjetja druge generacije

1. UVOD

1.1. **Kratice**

Za namen tega dodatka se uporabljajo naslednje kratice:

AC	pogoji dostopa (Access conditions)
AES	napredni standard šifriranja (Advanced Encryption Standard)
AID	identifikator aplikacije (Application identificator)
ALW	vedno (Always)
APDU	podatkovna enota aplikacijskega protokola (struktura ukaza) (Application Protocol Data Unit)
ATR	odziv na ponastavitev (Answer To Reset)
AUT	avtenticiran (Authenticated).
C6, C7	kontakta kartice št. 6 in 7, opisana v ISO/IEC 7816-2
cc	urni cikli (clock cycles)
CHV	informacija o preverjanju imetnika kartice (Card holder Verification Information)
CLA	bajt razreda v ukazu APDU (Class byte of an APDU command)

▼B

DSRC	posebna komunikacija kratkega dosega (Dedicated Short Range Communication)
DF	namenska datoteka (Dedicated File) DF lahko vsebuje druge datoteke (EF ali DF)
ECC	kriptografija eliptične krivulje (Elliptic Curve Cryptography)
EF	osnovna datoteka (Elementary File)
etu	elementarna enota časa (elementary time unit)
G1	prva generacija
G2	druga generacija
IC	integrirano vezje (Integrated Circuit)
ICC	kartica z integriranim vezjem (Integrated Circuit Card)
ID	identifikator (Identifier)
IFD	vmesniška naprava (Interface Device)
IFS	velikost polja informacije (Information Field Size)
IFSC	velikost polja informacije za kartico (Information Field Size for the card)
IFSD	velikost polja informacije za napravo (za terminal) (Information Field Size Device (for the Terminal))
INS	bajt instrukcije v ukazu APDU (Instruction byte of an APDU command)
Lc	dolžina vhodnih podatkov za ukaz APDU (Length of the input data for a APDU command)
Le	dolžina pričakovanih podatkov (izhodni podatki za ukaz) (Length of the expected data)
MF	glavna datoteka (korenska DF) (Master File)
NAD	vozliščni naslov pri protokolu T=1 (Node Address used in T=1 protocol)
NEV	nikoli (Never)
P1-P2	bajtov parametrov (Parameter bytes)
PIN	osebna identifikacijska številka (Personal Identification Number)
PRO SM	zaščiteno z varnim sporočanjem (Protected with secure messaging)
PTS	izbira protokola prenosa (Protocol Transmission Selection)
RFU	rezervirano za prihodnjo uporabo (Reserved for Future Use)
RST	ponastavitev (kartice) (Reset of the card)
SFID	kratki identifikator EF (Short EF identifikator)
SM	varno sporočanje (Secure Messaging)
SW1-SW2	status bajtov (Status bytes)
TS	začetni znak ATR (Status bytes)
VPP	napetost programiranja (Programming Voltage)
VU	enota v vozilu (Vehicle Unit)
XXh	vrednost XX v šestnajstiškem zapisu (Value XX in hexadecimal notation)
‘XXh’	vrednost XX v šestnajstiškem zapisu (Value XX in hexadecimal notation)
||	simbol združevanja 03||04=0304

▼B

1.2. **Viri**

V tem dodatku se uporabljajo naslednji sklici:

ISO/IEC 7816-2 Identification cards – Integrated circuit(s) cards z contacts – Part 2: Dimensions and location of the contacts. ISO/IEC 7816-2:2007.

ISO/IEC 7816-3 Identification cards – Integrated circuit(s) cards z contacts – Part 3: Electrical interface and transmission protocols. ISO/IEC 7816-3:2006.

ISO/IEC 7816-4 Identification cards – Integrated circuit(s) cards z contacts – Part 4: Organization, security and commands for interchange. ISO/IEC 7816-4:2013 + Cor 1: 2014.

ISO/IEC 7816-6 Identification cards – Integrated circuit(s) cards z contacts – Part 6: Interindustry data elements for interchange. ISO/IEC 7816-6:2004 + Cor 1: 2006.

ISO/IEC 7816-8 Identification cards – Integrated circuit(s) cards z contacts – Part 8: Commands for security operations. ISO/IEC 7816-8:2004.

ISO/IEC 9797-2 Information technology – Security techniques – Message Authentication Codes (MACs) – Part 2: Mechanisms using a dedicated hash-function. ISO/IEC 9797-2:2011

2. ELEKTRIČNE IN FIZIČNE LASTNOSTI

TCS_01 Če ni določeno drugače, so vsi elektronski signali v skladu z ISO/IEC 7816-3.

TCS_02 Položaji in mere kontaktov kartice so v skladu z ISO/IEC 7816-2.

2.1. **Napajalna napetost in poraba električnega toka**

TCS_03 Kartica deluje v skladu s specifikacijami v okviru omejitev porabe iz ISO/IEC 7816-3.

TCS_04 Karzica deluje z Vcc = 3V (± 0.3V) ali z Vcc = 5V (± 0.5V).

Napetost se izbere v skladu z ISO/IEC 7816-3.

2.2. **Napetost programiranja V_{pp}**

TCS_05 Kartica ne zahteva napetosti programiranja na nožici C6. Pričakuje se, da nožica C6 v IFD ni priključena. Kontakt C6 je lahko na kartici priključen na V_{cc}, ne sme pa biti priključen na ozemljitev. Te napetosti se ne sme v nobenem primeru interpretirati.

2.3. **Tvorba in frekvenca urnega signala**

TCS_06 Kartica deluje v frekvenčnem območju od 1 do 5 MHz in lahko podpira višje frekvence. V eni seji s kartico se lahko urna frekvenca spreminja v območju± 2 %. Urno frekvenco tvori enota v vozilu, ne pa sama kartica. Obratovalni cikel se lahko spreminja v območju od 40 % do 60 %.

TCS_07 Pod pogoji, ki jih določa datoteka EFICC na kartici, se lahko zunanjo uro zaustavi. Prvi bajt glavnega dela datoteke EF ICC kodira pogoje za način Clockstop:

▼B

Nizka raven	Visoka raven		
Bit 3	Bit 2	Bit 1	
0	0	1	Ustavitev ure (Clockstop) dovoljena, ni prednostne ravni.
0	1	1	Ustavitev ure (Clockstop) dovoljena, prednostna raven visoka.
1	0	1	Ustavitev ure (Clockstop) dovoljena, prednostna raven nizka.
0	0	0	Ustavitev ure (Clockstop) ni dovoljena.
0	1	0	Ustavitev ure (Clockstop) dovoljena le pri visoki ravni.
1	0	0	Ustavitev ure (Clockstop) dovoljena le pri nizki ravni.

Biti 4 do 8 niso uporabljeni.

2.4. **Kontakt I/O**

TCS_08 Kontakt I/O C7 se uporablja za sprejem podatkov iz IFD in oddajanja podatkov v IFD. Med delovanjem je v oddajnem režimu le kartica ali le IFD. Tudi če sta obe enoti v režimu oddajanja, to ne poškoduje kartice. Kadar ne oddaja, se kartica preklopi v način sprejema.

2.5. **Stanja kartice**

TCS_09 Kadar je priključena napajalna napetost, kartica deluje v dveh stanjih:

stanju delovanja, kadar izvaja ukaze ali se povezuje z digitalno enoto,

stanju mirovanja ves preostali čas; v tem stanju mora kartica ohranjati vse podatke.

3. STROJNA OPREMA IN KOMUNIKACIJA

3.1. **Uvod**

Ta točka opisuje minimalne funkcionalne zahteve za tahografske kartice in enote v vozilu, ki zagotavljajo pravilno delovanje in interoperabilnost.

Tahografske kartice so, kolikor je mogoče, usklajene z ustreznimi veljavnimi standardi ISO/IEC (zlasti z ISO/IEC 7816). Vendar so ukazi in protokoli opisani v celoti, da se določijo morebitne omejitve rabe in razlike. Kadar ni označeno drugače, so določeni ukazi v celoti v skladu z navedenimi standardi.

3.2. **Protokol za prenos podatkov**

TCS_10 Protokol za prenos podatkov je v skladu z ISO/IEC 7816-3 za T = 0 in T = 1. Še zlasti VU prepozna zahteve za podaljšanje čakalnih časov, ki ji jih sporoči kartica.

3.2.1 *Protokoli*

TCS_11 Kartica zagotavlja oba protokola: **T = 0** in **T = 1**. Poleg njiju lahko kartica podpira druge kontaktno usmerjene protokole.

TCS_12 **T = 0** je privzeti protokol, za preklop na protokol **T = 1** je torej potreben ukaz **PTS**.

▼B

TCS_13 Naprave pri obeh protokolih podpirajo **neposredno konvencijo**. Neposredna konvencija je torej za kartico obvezna.

TCS_14 Pri ATR se bajt **Velikost polja informacije za kartico (*Information Field Size Card*)** predstavi v znaku TA3. Ta vrednost je najmanj ‘F0h’ (= 240 bajtov).

Za protokola veljajo naslednje omejitve:

TCS_15 **T = 0**

— Vmesniška naprava podpira odgovor na I/O od 400 cc po dvižnem robu signala na RST.

— Vmesniška naprava lahko prebere znake, ločene z 12 etu.

— Vmesniška naprava prebere napačni znak in njegovo ponovitev, če sta ločena s 13 etu. Če je zaznan napačen znak, lahko signal za napako na I/O nastopi med 1 etu in 2 etu. Naprava mora podpirati zakasnitev 1 etu.

— Vmesniška naprava mora sprejemati 33-bajtni ATR (TS+32)

— Če je v ATR prisoten TC1, mora biti za znake, poslane iz vmesniške naprave, podan tudi dodatni varovalni čas (Extra Guard Time), znakim ki jih pošlje kartica, pa so še vedno lahko ločeni z 12 etu. To velja tudi za znak ACK, ki ga pošlje kartica po znaku P3, oddanem iz vmesniške naprave.

— Vmesniška naprava upošteva znak NUL, ki ga pošlje kartica.

— Vmesniška naprava sprejema tudi komplementarni način ACK.

— Ukaza za pridobitev odziva (GET RESPONSE) ni mogoče uporabiti v verižnem načinu za pridobitev podatkov, katerih dolžina bi lahko presegla 255 bajtov.

TCS_16 **T = 1**

— Bajt NAD: se ne uporablja (NAD se nastavi na ‘00’).

— ABORT S-bloka: se ne uporablja.

— Napaka stanja VPP S-bloka: se ne uporablja.

— Skupna verižna dolžina podatkovnega polja ne presega 255 bajtov (kar zagotovi IFD).

— IFD nakaže IFSD takoj po ATR: IFD mora po ATR poslati zahtevek za IFS S-bloka, kartica pa mora poslati nazaj IFS S-bloka. Priporočena vrednost IFSD je 254 bajtov.

— Kartica ne bo zahtevala ponovne nastavitve IFS.

▼B

3.2.2 *ATR*

TCS_17 Naprava preverja bajte ATR v skladu z ISO/IEC 7816-3. Zgodovinskih znakov ATR se ne preverja.

Primer osnovnega bi-protokola ATR po ISO/IEC 7816-3.

Znak	Vrednost	Opombe
TS	‘3Bh’	Označuje neposredno konvencijo
T0	‘85h’	TD1 prisoten; prisotnih je 5 zgodovinskih bajtov
TD1	‘80h’	TD2 prisoten; uporabi se T = 0
TD2	‘11h’	TA3 prisoten; uporabi se T = 1
TA3	‘XXh’ (najmanj ‘F0h’)	Velikost polja informacije za kartico (IFSC)
TH1 do TH5	‘XXh’	Zgodovinski znaki
TCK	‘XXh’	Znak za preverjanje (razen OR)

TCS_18 Po odgovoru na ponastavitev (ATR) se implicitno izbere glavna datoteka (MF) in postane trenutni imenik.

3.2.3 *PTS*

TCS_19 Privzeti protokol je T=0. Za nastavitev protokola T=1 mora naprava kartici poslati PTS (znan tudi kot PPS).

TCS_20 Ker sta za kartico obvezna oba protokola T=0 in T=1, je za kartico obvezen tudi osnovni PTS za preklop protokolov.

PTS se lahko uporablja, kakor je navedeno v ISO/IEC 7816-3, za preklop na baudne hitrosti, višje od privzete baudne hitrosti, ki jo predlaga kartica v morebitnem ATR (bajt TA(1)).

Za kartico so višje baudne hitrosti neobvezne.

TCS_21 Če razen privzete ni podprta nobena druga baudna hitrost (ali če izbrana baudna hitrost ni podprta), se kartica na PTS odzove pravilno v skladu z ISO/IEC 7816-3 z izpustitvijo bajta PPS1.

Primeri osnovnih PTS za izbiro protokola so naslednji:

Znak	Vrednost	Opombe
PPSS	‘FFh’	Začetni znak (The Initiate Character).
PPS0	‘00h’ ali ‘01h’	PPS1 do PPS3 niso prisotni; ‘00h’ za izbiro T0, ‘01h’ za izbiro T1.
PK	‘XXh’	Kontrolni znak: ‘XXh’ = ‘FFh’ če PPS0 = ‘00h’, ‘XXh’ = ‘FEh’ če PPS0 = ‘01h’.

▼B

3.3. **Pravila dostopa**

TCS_22 Pravilo dostopa določa za način dostopa (tj. ukaz) ustrezne varnostne pogoje. Če so ti varnostni pogoji izpolnjeni, se obdela ustrezni ukaz.

TCS_23 Naslednji varnostni pogoji se uporabljajo za tahografsko kartico:

Kratica	Pomen
ALW	Dejanje je vedno mogoče in se lahko izvede brez omejitev. Ukaz in odziv APDU se pošljeta kot golo besedilo, tj. brez varnega sporočanja.
NEV	Dejanje ni nikoli mogoče.
PLAIN-C	Ukaz APDU se pošlje kot golo besedilo, tj. brez varnega sporočanja.
PWD	Dejanje se lahko izvede le, če je bil PIN kartice servisne delavnice uspešno preverjen, kar pomeni, da je nastavljeno stanje notranje varnosti kartice ‘PIN_Verified’. Ukaz mora biti poslan brez varnega sporočanja.
EXT-AUT-G1	Dejanje se lahko izvede le, če je bil ukaz External Authenticate za avtentikacijo prve generacije (glej tudi Del A iz Dodatka 11) uspešno izveden.
SM-MAC-G1	APDU (ukaz in odziv) se mora uporabiti z varnim sporočanjem prve generacije v načinu authentication-only (glej del A iz Dodatka 11).
SM-C-MAC-G1	Ukaz APDU se mora uporabiti z varnim sporočanjem prve generacije v načinu authentication-only (glej del A iz Dodatka 11)..
SM-R-ENC-G1	Odziv APDU se mora uporabiti z varnim sporočanjem prve generacije (glej Del A iz Dodatka 11), tj. ne vrne se sporočilo z avtentikacijsko kodo.
SM-R-ENC-MAC-G1	Ukaz APDU se mora uporabiti z varnim sporočanjem prve generacije v načinu najprej-kodiranje-nato-avtentikacija (encrypt-then-authenticate) (glej del A iz Dodatka 11).
SM-MAC-G2	APDU (ukaz in odziv) se mora uporabiti z varnim sporočanjem druge generacije v načinu authentication-only (glej del B iz Dodatka 11).
SM-C-MAC-G2	Ukaz APDU se mora uporabiti z varnim sporočanjem druge generacije v načinu authentication-only (glej Del B iz Dodatka 11).
SM-R-ENC-MAC-G2	Ukaz APDU se mora uporabiti z varnim sporočanjem druge generacije v načinu najprej-kodiranje-nato-avtentikacija (encrypt-then-authenticate) (glej del B iz Dodatka 11).

TCS_24 Ti varnostni pogoji so lahko povezani na naslednje načine:

IN: izpolnjeni morajo biti vsi varnostni pogoji.

ALI: izpolnjen mora biti najmanj eden varnostni pogoj.

Pravila dostopa za datotečni sistem, tj. ukazi SELECT, READ BINARY in UPDATE BINARY, so določena v poglavju 4. Pravila dostopa za preostale ukaze so določena v naslednjih tabelah.

▼B

TCS_25 V aplikaciji DF Tachograph G1 se uporabljajo naslednja pravila dostopa:

Ukaz	Vozniška kartica	Kartica servisne delavnice	Nadzorna kartica	Kartica podjetja
External Authenticate				
— Za avtentikacijo prve generacije	ALW	ALW	ALW	ALW
— Za avtentikacijo druge generacije	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	Ni relevantno	Ni relevantno	Ni relevantno	Ni relevantno
PSO: Compute Digital Signature	ALW OR SM-MAC-G2	ALW OR SM-MAC-G2	Ni relevantno	Ni relevantno
PSO: Hash	Ni relevantno	Ni relevantno	ALW	Ni relevantno
PSO: Hash of File	ALW OR SM-MAC-G2	ALW OR SM-MAC-G2	Ni relevantno	Ni relevantno
PSO: Verify Certificate	ALW	ALW	ALW	ALW
PSO: Verify Digital Signature	Ni relevantno	Ni relevantno	ALW	Ni relevantno
Verify	Ni relevantno	ALW	Ni relevantno	Ni relevantno

TCS_26 V aplikaciji DF Tachograph_G2 se uporabljajo naslednja pravila dostopa:

Ukaz	Vozniška kartica	Kartica servisne delavnice	Nadzorna kartica	Kartica podjetja
External Authenticate				
— Za avtentikacijo prve generacije	Ni relevantno	Ni relevantno	Ni relevantno	Ni relevantno
— Za avtentikacijo druge generacije	ALW	PWD	ALW	ALW
Internal Authenticate	Ni relevantno	Ni relevantno	Ni relevantno	Ni relevantno

▼B

Ukaz	Vozniška kartica	Kartica servisne delavnice	Nadzorna kartica	Kartica podjetja
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	Ni relevantno	ALW	ALW	Ni relevantno
PSO: Compute Digital Signature	ALW OR SM-MAC-G2	ALW OR SM-MAC-G2	Ni relevantno	Ni relevantno
PSO: Hash	Ni relevantno	Ni relevantno	ALW	Ni relevantno
PSO: Hash of File	ALW OR SM-MAC-G2	ALW OR SM-MAC-G2	Ni relevantno	Ni relevantno
PSO: Verify Certificate	ALW	ALW	ALW	ALW
PSO: Verify Digital Signature	Ni relevantno	Ni relevantno	ALW	Ni relevantno
Verify	Ni relevantno	ALW	Ni relevantno	Ni relevantno

TCS_27 V MF se uporabljajo naslednja pravila dostopa:

Ukaz	Vozniška kartica	Kartica servisne delavnice	Nadzorna kartica	Kartica podjetja
External Authenticate				
— Za avtentikacijo prve generacije	Ni relevantno	Ni relevantno	Ni relevantno	Ni relevantno
— Za avtentikacijo druge generacije	ALW	PWD	ALW	ALW
Internal Authenticate	Ni relevantno	Ni relevantno	Ni relevantno	Ni relevantno
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	Ni relevantno	Ni relevantno	Ni relevantno	Ni relevantno

▼B

Ukaz	Vozniška kartica	Kartica servisne delavnice	Nadzorna kartica	Kartica podjetja
PSO: Compute Digital Signature	Ni relevantno	Ni relevantno	Ni relevantno	Ni relevantno
PSO: Hash	Ni relevantno	Ni relevantno	Ni relevantno	Ni relevantno
PSO: Hash of File	Ni relevantno	Ni relevantno	Ni relevantno	Ni relevantno
PSO: Verify Certificate	ALW	ALW	ALW	ALW
Verify	Ni relevantno	ALW	Ni relevantno	Ni relevantno

TCS_28 Tahografska kartica lahko (a ne nujno) sprejme ukaz višje ravni varnosti, kot je raven, določena v varnostnih pogojih. Tj. če je varnostni pogoj ALW (ali PLAIN-C), kartica lahko sprejme ukaz z varnim sporočanjem (način šifriranja in/ali način avtentikacije). Če varnostni pogoj zahteva varno sporočanje v načinu avtentikacije, tahografska kartica lahko z varnim sporočanjem sprejme ukaz iste generacije v načinu avtentikacije in šifriranja.

Opomba: opisi ukaza nudijo več informacij o podpori ukazov za različne vrste tahografskih kartic in različne DF.

3.4. **Pregled ukazov in kod napak**

Ukazi in organizacija datotek so v skladu z ISO/IEC 7816-4 in iz njega izpeljani.

Ta oddelek opisuje naslednje pare ukazov-odzivov APDU. Različice ukaza, ki jih podpira aplikacija prve in druge generacije, so določene v ustreznih opisih ukaza.

Ukaz	INS
SELECT	‘A4h’
READ BINARY	‘B0h’, ‘B1h’
UPDATE BINARY	‘D6h’, ‘D7h’
GET CHALLENGE	‘84h’
VERIFY	‘20h’
GET RESPONSE	‘C0h’
PERFORM SECURITY OPERATION	‘2Ah’

▼B

Ukaz	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 Opisa stanja SW1, SW2 se vrneta v vsakem sporočilu z odzivom in označujeta stanje obdelave ukaza.

SW1	SW2	Pomen
90	00	Normalna obdelava.
61	XX	Normalna obdelava. XX = število razpoložljivih bajtov odziva
62	81	Opozorilo glede obdelave. Del vrnjenih podatkov je lahko poškodovanih.
63	00	Neuspešna avtentikacija (opozorilo)
63	CX	Napačen CHV (PIN). Števec preostalih poskusov je podan v ‘X’.
64	00	Napaka pri izvedbi – stanje trajnega pomnilnika nespremenjeno. Napaka celovitosti.
65	00	Napaka pri izvedbi – stanje trajnega pomnilnika spremenjeno.
65	81	Napaka pri izvedbi – stanje trajnega pomnilnika spremenjeno – Napaka pomnilnika.
66	88	Varnostna napaka: napačna kriptografska kontrolna vsota (med varnim sporočanjem) ali napačen certifikat (med preverjanjem certifikata) ali napačen kriptogram (med zunanjo avtentikacijo) ali napačen podpis (med preverjanjem podpisa)
67	00	Napačna dolžina (napačen Lc ali Le).

▼B

SW1	SW2	Pomen
68	82	Varno sporočanje ni podprto.
68	83	Pričakovan zadnji ukaz iz verige.
69	00	Prepovedan ukaz (pri T=0 ni razpoložljivega odziva)
69	82	Varnostni status ni zadovoljiv.
69	83	Metoda avtentikacije blokirana.
69	85	Pogoji uporabe niso izpolnjeni.
69	86	Ukaz ni dovoljen (ni trenutne EF).
69	87	Manjkajo pričakovani podatkovni objekti varnega sporočanja.
69	88	Nepravilni podatkovni objekti varnega sporočanja.
6A	80	Nepravilni parametri v podatkovnem polju.
6A	82	Datoteka ni najdena.
6A	86	Napačna parametra P1-P2.
6A	88	Podatki, na katere se sklicuje ukaz, niso najdeni.
6 B	00	Napačni parametri (zamik zunaj EF).
6C	XX	Napačna dolžina, SW2 označuje točno dolžino. Ni vrnjeno nobeno podatkovno polje.
6D	00	Koda instrukcije ni podprta ali ni veljavna.
6E	00	Razred ni podprt.
6F	00	Druge napake pri preverjanju

TCS_30 Če je izpolnjen več kot en pogoj za napako v enem ukazu APDU, kartica lahko vrne kateri koli ustrezen opis stanja.

3.5. **Opisi ukazov**

V tem poglavju so opisani obvezni ukazi tahografske kartice.

Druge pomembne podrobnosti, povezane z uporabljanimi kriptografskimi postopki, so navedene v Dodatku 11 Skupni varnostni mehanizmi za tahografe prve in druge generacije.

Vsi ukazi so opisani neodvisno od uporabljenega protokola (T=0 ali T=1). Bajti APDU CLA, INS, P1, P2, Lc in Le so vedno navedeni. Če pri določenem ukazu Lc ali Le ni potreben, so postavke dolžine, vrednosti in opisa prazne.

TCS_31 Če sta zahtevana oba bajta dolžine (Lc in Le), mora biti opisani ukaz razdeljen na dva dela, kadar IFD uporablja protokol T=0: IFD najprej pošlje opisani ukaz s P3=Lc + podatki, nato pa pošlje ukaz GET RESPONSE (glej poglavje 3.5.6) s P3=Le.

TCS_32 Če sta zahtevana bajta obeh dolžin in je Le=0 (varno sporočanje):

▼B

— Pri protokolu T=1 mora kartica odgovoriti na Le=0 tako, da pošlje vse razpoložljive izhodne podatke.

— Pri protokolu T=0 IFD pošlje prvi ukaz s P3=Lc + podatki; kartica nato odgovori (na ta implicitni Le=0) tako, da pošlje statusne bajte '**61La**', pri čemer je La število razpoložljivih bajtov za odziv. IFD nato za branje podatkov ustvari ukaz GET RESPONSE s P3 = La.

TCS_33 Tahografska kartica lahko v okviru neobvezne funkcije podpira podaljšana podatkovna polja v skladu z ISO/IEC 7816-4. Tahografska kartica, ki podpira podaljšana podatkovna polja,

— navaja podporo podaljšanega podatkovnega polja v ATR,

— navaja podprte velikosti vmesnega pomnilnika z informacijami o podaljšanem podatkovnem polju v EF ATR/INFO, glej TCS_146,

— navaja podprtost podaljšanih podatkovnih polj za T = 1 in/ali T = 0 v podaljšani dolžini EF, glej TCS_147,

— podpira podaljšana podatkovna polja za tahografsko aplikacijo prve in druge generacije.

Opombe:

vsi ukazi so določeni za polja kratke dolžine. Uporaba podaljšanih podatkovnih polj je razvidna iz ISO/IEC 7816-4.

Na splošno so ukazi določeni za nešifrirani način, tj. brez varnega sporočanja, saj je plast varnega sporočanja določena v Dodatku 11. Iz pravil dostopa za ukaz je razvidno, ali ukaz podpira varno sporočanje in ali ukaz podpira varno sporočanje prve in/ali druge generacije. Nekatere različice ukaza so opisane z varnim sporočanjem, da se prikaže njegova uporaba.

TCS_34 Enota v vozilu izvede celotni protokol medsebojne avtentikacije VU–kartica druge generacije za sejo, vključno s preverjanjem certifikata (če se zahteva) v DF Tachograph, DF Tachograph_G2 ali MF.

3.5.1 *SELECT*

Ta ukaz je v skladu z ISO/IEC 7816-4, a ima v primerjavi z opredelitvijo v tem standardu omejeno uporabo.

Ukaz SELECT FILE se uporablja:

— za izbiro aplikativne DF (obvezna izbira po imenu),

— za izbiro elementarne datoteke, ki ustreza podanemu ID datoteke.

3.5.1.1 Izbira po imenu (AID)

Ta ukaz omogoča izbiro aplikativne DF na kartici.

TCS_35 Ta ukaz se lahko izvede od koderkoli v datotečni strukturi (po ATR ali ob katerem koli drugem času).

▼B

TCS_36 Izbira aplikacije ponastavi trenutno varnostno okolje. Po opravljeni izbiri aplikacije trenutni javni ključ ni več izbran. Izgubljen je tudi pogoj dostopa EXT-AUT-G1. Če je bil ukaz izveden brez varnega sporočanja, prejšnji ključi varnega sporočanja niso več na voljo.

TCS_37 **Ukazno sporočilo**

Bajt	Dolžina	Vrednost	Opis
CLA	1	‘00h’	
INS	1	‘A4h’	
P1	1	‘04h’	Izbira po imenu (AID)
P2	1	‘0Ch’	Ni pričakovan noben odgovor
Lc	1	‘NNh’	Število bajtov, poslanih kartici (dolžina AID): ‘06h’ za tahografsko aplikacijo
#6-#(5 + NN)	NN	‘XX..XXh’	AID: ‘FF 54 41 43 48 4F’ za tahografsko aplikacijo prve generacije AID: ‘FF 53 41 52 44 4F’ za tahografsko aplikacijo druge generacije

Ukaz SELECT FILE ne potrebuje odziva (Pri T=1 je Le odsoten, pri T=0 pa odziv ni zahtevan).

TCS_38 **Sporočilo odziva (odziv ni zahtevan)**

Bajt	Dolžina	Vrednost	Opis
SW	2	‘XXXXh’	Opis stanja (SW1, SW2)

— Če je ukaz uspešen, kartica vrne sporočilo ‘**9000**’.

— Če ni najdena aplikacija, ki ustreza AID, se vrne stanje obdelave ‘**6A82**’.

— Pri T=1 se pri prisotnem bajtu Le vrne stanje ‘**6700**’.

— Pri T=0 se v primeru, če se po ukazu SELECT zahteva odziv, vrne stanje obdelave ‘**6900**’.

— Če se izbrana aplikacija šteje za poškodovano (v atributih datoteke je zaznana napaka celovitosti), se vrne stanje obdelave ‘**6400**’ ali ‘**6581**’.

3.5.1.2 Izbira elementarne datoteke z uporabo njenega identifikatorja datoteke

TCS_39 **Ukazno sporočilo**

TCS_40 Tahografska kartica podpira varno sporočanje druge generacije, kot je določeno v Delu B iz Dodatka 11 za to različico ukaza.

Bajt	Dolžina	Vrednost	Opis
CLA	1	‘00h’	
INS	1	‘A4h’	
P1	1	‘02h’	Izbira EF v okviru tekoče DF

▼B

Bajt	Dolžina	Vrednost	Opis
P2	1	‘0Ch’	Ni pričakovan noben odgovor
Lc	1	‘02h’	Število bajtov, poslanih kartici
#6-#7	2	‘XXXXh’	Identifikator datoteke

Ukaz SELECT ne potrebuje odziva (Pri T=1 je Le odsoten, pri T=0 pa odziv ni zahtevan).

TCS_41 **Sporočilo odziva (odziv ni zahtevan)**

Bajt	Dolžina	Vrednost	Opis
SW	2	‘XXXXh’	Opis stanja (SW1, SW2)

— Če je ukaz uspešen, kartica vrne sporočilo ‘**9000**’.

— Če ni najdena datoteka, ki ustreza identifikatorju, se vrne stanje obdelave ‘**6A82**’.

— Pri T = 1 se pri prisotnem bajtu Le vrne stanje ‘**6700**’.

— Pri T = 0 se v primeru, če se po ukazu SELECT zahteva odziv, vrne stanje obdelave ‘**6900**’.

— Če se izbrana datoteka šteje za poškodovano (v atributih datoteke je zaznana napaka celovitosti), se vrne stanje obdelave ‘**6400**’ ali ‘**6581**’.

3.5.2 *READ BINARY*

Ta ukaz je v skladu z ISO/IEC 7816-4, a ima v primerjavi z opredelitvijo v tem standardu omejeno uporabo.

Ukaz READ BINARY se uporablja za branje podatkov iz transparentne datoteke.

Odziv kartice obsega vrnjene prebrane podatke, neobvezno enkapsulirane v strukturi varnega sporočanja.

3.5.2.1 Ukaz z zamikom v P1-P2

Ta ukaz IFD omogoča branje podatkov iz trenutno izbrane EF brez varnega sporočanja.

Opomba: ta ukaz brez varnega sporočanja se lahko uporablja le za branje datoteke, ki podpira varnostni pogoj ALW za način dostopa za branje (Read).

TCS_42 **Ukazno sporočilo**

Bajt	Dolžina	Vrednost	Opis
CLA	1	‘00h’	
INS	1	‘B0h’	Read Binary
P1	1	‘XXh’	Zamik v bajtih od začetka datoteke: bajt z največjo težo

▼B

Bajt	Dolžina	Vrednost	Opis
P2	1	‘XXh’	Zamik v bajtih od začetka datoteke: bajt z najmanjšo težo
Le	1	‘XXh’	Pričakovana dolžina podatkov. Število bajtov, ki se preberejo.

Opomba: bit 8 v P1 mora biti nastavljen na 0.

TCS_43 **Sporočilo z odzivom**

Bajt	Dolžina	Vrednost	Opis
#1-#X	X	‘XX..XXh’	Prebrani podatki
SW	2	‘XXXXh’	Opis stanja (SW1, SW2)

— Če je ukaz uspešen, kartica vrne sporočilo ‘**9000**’.

— Če ni izbrana nobena EF, se vrne stanje obdelave ‘**6986**’.

— Če varnostni pogoji za izbrano datoteko niso izpolnjeni, se ukaz prekine s ‘**6982**’.

— Če zamik ni združljiv z velikostjo EF (zamik > velikost EF), se vrne stanje obdelave ‘**6B00**’.

— Če velikost podatkov, ki jih je treba prebrati, ni združljiva z velikostjo EF (zamik + Le > velikost EF), se vrne stanje obdelave ‘**6700**’ ali ‘**6Cxx**’, pri čemer je ‘xx’ točna dolžina.

— Če je zaznana napaka celovitosti v atributih datoteke, kartica šteje datoteko za poškodovano in nepopravljivo, vrne se stanje obdelave ‘**6400**’ ali ‘**6581**’.

— Če je zaznana napaka celovitosti v shranjenih podatkih, kartica vrne zahtevane podatke, stanje obdelave, ki se vrne, pa je‘**6281**’.

3.5.2.1.1 Ukaz z varnim sporočanjem (primeri)

Ta ukaz IFD omogoča branje podatkov iz trenutno izbrane EF z varnim sporočanjem, da se preveri celovitost prejetih podatkov in zaščiti njihova zaupnost, če je uporabljen varnostni pogoj SM-R-ENC-MAC-G1 (prva generacija) ali SM-R-ENC-MAC-G2 (druga generacija).

TCS_44 **Ukazno sporočilo**

Bajt	Dolžina	Vrednost	Opis
CLA	1	‘0Ch’	Zahtevano varno sporočanje.
INS	1	‘B0h’	Read Binary
P1	1	‘XXh’	P1 (zamik v bajtih od začetka datoteke): bajt z največjo težo
P2	1	‘XXh’	P2 (zamik v bajtih od začetka datoteke): bajt z najmanjšo težo

▼B

Bajt	Dolžina	Vrednost	Opis
Lc	1	‘XXh’	Dolžina vhodnih podatkov za varno sporočanje
#6	1	‘97h’	T_{LE}: oznaka za specifikacijo pričakovane dolžine.
#7	1	‘01h’	L_{LE}: dolžina pričakovane dolžine
#8	1	‘NNh’	Specifikacija pričakovane dolžine (originalni Le): Število bajtov, ki se preberejo.
#9	1	‘8Eh’	T_{CC}: oznaka za kriptografsko kontrolno vsoto
#10	1	‘XXh’	L_{CC}: dolžina naslednje kriptografske kontrolne vsote ‘04h’ za varno sporočanje prve generacije (glej Del A iz Dodatka 11) ‘08h’, ‘0Ch’ ali ‘10h’, odvisno od dolžine ključa AES za varno sporočanje druge generacije (glej Del B iz Dodatka 11).
#11-#(10+L)	L	‘XX..XXh’	Kriptografska kontrolna vsota
Le	1	‘00h’	Kakor določa ISO/EEC 7816-4.

TCS_45 **Sporočilo odziva, če se SM-R-ENC-MAC-G1 (prva generacija) / SM-R-ENC-MAC-G2 (druga generacija) ne zahteva in če je vhodni format varnega sporočanja pravilen:**

Bajt	Dolžina	Vrednost	Opis
#1	1	‘99h’	Oznaka za stanje obdelave (SW1-SW2) – neobvezno za varno sporočanje prve generacije
#2	1	‘02h’	Dolžina stanja obdelave
#3 – #4	2	‘XX XXh’	Stanje obdelave nezaščitenega odziva APDU
#5	1	‘81h’	T_{PV}: oznaka za nešifrirane podatke
#6	L	‘NNh’ ali ‘81 NNh’	L_{PV}: dolžina vrnjenih podatkov (=prvotni Le) L je 2 bajta, če je L_{PV}>127 bajtov.
#(6+L)-#(5+L+NN)	NN	‘XX..XXh’	Nešifrirana vrednost podatkov
#(6+L+NN)	1	‘8Eh’	T_{CC}: oznaka za kriptografsko kontrolno vsoto
#(7+L+NN)	1	‘XXh’	L_{CC}: dolžina naslednje kriptografske kontrolne vsote ‘04h’ za varno sporočanje prve generacije (glej Del A iz Dodatka 11). ‘08h’, ‘0Ch’ ali ‘10h’, odvisno od dolžine ključa AES za varno sporočanje druge generacije (glej Del B iz Dodatka 11).
#(8+L+NN)-#(7+M+L+NN)	O	‘XX..XXh’	Kriptografska kontrolna vsota
SW	2	‘XXXXh’	Opis stanja (SW1, SW2)

▼B

TCS_46 **Sporočilo odziva, če se SM-R-ENC-MAC-G1 (prva generacija) / SM-R-ENC-MAC-G2 (druga generacija) zahteva in če je vhodni format varnega sporočanja pravilen:**

Bajt	Dolžina	Vrednost	Opis
#1	1	‘87h’	$T_{PI\ CG}$: oznaka za šifrirane podatke (kriptogram)
#2	L	‘MMh’ ali ‘81 MMh’	$L_{PI\ CG}$: dolžina vrnjenih šifriranih podatkov (različna od originalne vednosti Le iz ukaza zaradi zapolnitve) L je 2 bajta, če je $L_{PI\ CG} > 127$ bajtov.
#(2+L)-#(1+L+MM)	MM	‘01XX..XXh’	Šifrirani podatki: zapolnitveni kazalnik in kriptogram
#(2+L+MM)	1	‘99h’	Oznaka za stanje obdelave (SW1-SW2) – neobvezno za varno sporočanje prve generacije
#(3+L+MM)	1	‘02h’	Dolžina stanja obdelave
#(4+L+MM) – #(5+L+MM)	2	‘XX XXh’	Stanje obdelave nezaščitenega odziva APDU
#(6+L+MM)	1	‘8Eh’	T_{CC}: oznaka za kriptografsko kontrolno vsoto
#(7+L+MM)	1	‘XXh’	L_{CC}: dolžina naslednje kriptografske kontrolne vsote ‘04h’ za varno sporočanje prve generacije (glej Del A iz Dodatka 11). ‘08h’, ‘0Ch’ ali ‘10h’, odvisno od dolžine ključa AES za varno sporočanje druge generacije (glej Del B iz Dodatka 11).
#(8+L+MM)-#(7+N+L+MM)	N	‘XX..XXh’	Kriptografska kontrolna vsota
SW	2	‘XXXXh’	Opis stanja (SW1, SW2)

Ukaz READ BINARY lahko vrne pravilna stanja obdelave, našteta v TCS_43 pod Oznako (*Tag*) ‘99h’, kot so opisana v TCS_59 z uporabo strukture za varno sporočanje.

Poleg tega lahko pride do nekaterih napak, povezanih posebej z varnim sporočanjem. V navedenem primeru se enostavno vrne stanje obdelave brez vključitve strukture za varno sporočanje.

TCS_47 **Sporočilo odziva pri nepravilnem vhodnem formatu varnega sporočanja**

Bajt	Dolžina	Vrednost	Opis
SW	2	‘XXXXh’	Opis stanja (SW1, SW2)

— Če ni na voljo nobenega ključa tekoče seje, se vrne stanje obdelave ‘**6A88**’. To se zgodi lahko v primeru, če ključ seje še ni bil ustvarjen ali če je veljavnost ključa seje iztekla (v tem primeru mora IFD ponovno izvesti postopek medsebojne avtentikacije za nastavitev novega ključa seje).

▼B

— Če nekateri pričakovani podatkovni objekti (kot so določeni zgoraj) manjkajo v formatu varnega sporočanja, se vrne stanje obdelave '**6987**': ta napaka nastopi, če manjka pričakovana oznaka ali če telo ukaza ni pravilno zgrajeno.

— Če so nekateri podatkovni objekti nepravilni, se vrne stanje obdelave '**6988**'. Ta napaka nastopi, če so prisotne vse zahtevane oznake, a se nekatere dolžine razlikujejo od pričakovanih.

— Če ni uspešno preverjanje kriptografske kontrolne vsote, se vrne stanje obdelave '**6688**'.

3.5.2.2 Ukaz s kratkim identifikatorjem EF (Elementary File)

Ta različica ukaza IFD omogoča, da izbere EF s kratkim identifikatorjem EF in da s tega EF prebere podatke.

TCS_48 Tahografska kartica to različico ukaza podpira za vse EF z določenim kratkim identifikatorjem EF. Ti kratki identifikatorji EF so določeni v poglavju 4.

TCS_49 **Ukazno sporočilo**

Bajt	Dolžina	Vrednost	Opis
CLA	1	'00h'	
INS	1	'B0h'	Read Binary
P1	1	'XXh'	Bit 8 je nastavljen na 1. Bita 7 in 6 sta nastavljena na 00. Bit 5 – 1 kodira kratki identifikator EF ustrezajočega EF.
P2	1	'XXh'	Kodira zamik od 0 do 255 bajtov v EF, na katero se sklicuje P1.
Le	1	'XXh'	Pričakovana dolžina podatkov. Število bajtov, ki se preberejo.

Opomba: kratki identifikatorji EF, ki se uporabljajo za tahografsko aplikacijo druge generacije, so določeni v poglavju 4.

Če P1 kodira kratki identifikator EF in je ukaz uspešen, identificirani EF postane trenutno izbrani EF (trenutni EF).

TCS_50 **Sporočilo odziva**

Bajt	Dolžina	Vrednost	Opis
#1-#L	L	'XX..XXh'	Prebrani podatki
SW	2	'XXXXh'	Opis stanja (SW1, SW2)

— Če je ukaz uspešen, kartica vrne sporočilo '**9000**'.

— Če ni najdena datoteka, ki ustreza kratkemu identifikatorju EF, se vrne stanje obdelave '**6A82**'.

— Če varnostni pogoji za izbrano datoteko niso izpolnjeni, se ukaz prekine s '**6982**'.

▼B

— Če zamik ni združljiv z velikostjo EF (zamik > velikost EF), se vrne stanje obdelave ‘**6B00**’.

— Če velikost podatkov, ki jih je treba prebrati, ni združljiva z velikostjo EF (zamik + Le > velikost EF), se vrne stanje obdelave ‘**6700**’ ali ‘**6Cxx**’, pri čemer je ‘xx’ točna dolžina.

— Če je zaznana napaka celovitosti v atributih datoteke, kartica šteje datoteko za poškodovano in nepopravljivo, vrne se stanje obdelave ‘**6400**’ ali ‘**6581**’.

— Če je zaznana napaka celovitosti v shranjenih podatkih, kartica vrne zahtevane podatke, stanje obdelave, ki se vrne, pa je‘**6281**’.

3.5.2.3 Ukaz z neparnim bajtom instrukcije

Ta različica ukaza IFD omogoča branje podatkov iz EF, ki imajo najmanj 32 768 bajtov.

TCS_51 Tahografska kartica, ki podpira EF z najmanj 32 768 bajtov, podpira to različico ukaza za te EF. Tahografska kartica lahko podpira to različico ukaza za druge EF razen EF Sensor_Installation_Data, glej TCS_156 in TCS_160.

TCS_52 **Ukazno sporočilo**

Bajt	Dolžina	Vrednost	Opis
CLA	1	‘00h’	
INS	1	‘B1h’	Read Binary
P1	1	‘00h’	Trenutni EF
P2	1	‘00h’	
Lc	1	‘NNh’	Dolžina Lc zamaknjenega podatkovnega objekta.
#6-#(5+NN)	NN	‘XX..XXh’	Zamaknjeni podatkovni objekt: Oznaka ‘54h’ Dolžina ‘01h’ ali ‘02h’ Vrednost zamika
Le	1	‘XXh’	Število bajtov, ki se preberejo.

IFD kodira dolžino zamaknjenega podatkovnega objekta z najmanjšim možnim številom oktetov, tj. z uporabo bajta dolžine ‘01h’ IFD kodira zamik od 0 do 255 in z uporabo bajta dolžine ‘02h’ zamik od ‘256’ do ‘65 535’ bajtov.

TCS_53 **Sporočilo z odzivom**

Bajt	Dolžina	Vrednost	Opis
#1-#L	L	‘XX..XXh’	Prebrani podatki so enkapsulirani v diskretnem podatkovnem objektu z oznako ‘53h’.
SW	2	‘XXXXh’	Opis stanja (SW1, SW2)

▼B

— Če je ukaz uspešen, kartica vrne sporočilo ‘**9000**’.

— Če ni izbrana nobena EF, se vrne stanje obdelave ‘**6986**’.

— Če varnostni pogoji za izbrano datoteko niso izpolnjeni, se ukaz prekine s ‘**6982**’.

— Če zamik ni združljiv z velikostjo EF (zamik > velikost EF), se vrne stanje obdelave ‘**6B00**’.

— Če velikost podatkov, ki jih je treba prebrati, ni združljiva z velikostjo EF (zamik + Le > velikost EF), se vrne stanje obdelave ‘**6700**’ ali ‘**6Cxx**’, pri čemer je ‘xx’ točna dolžina.

— Če je zaznana napaka celovitosti v atributih datoteke, kartica šteje datoteko za poškodovano in nepopravljivo, vrne se stanje obdelave ‘**6400**’ ali ‘**6581**’.

— Če je zaznana napaka celovitosti v shranjenih podatkih, kartica vrne zahtevane podatke, stanje obdelave, ki se vrne, pa je‘**6281**’.

3.5.2.3.1 Ukaz z varnim sporočanjem (primer)

Naslednji primer ponazarja uporabo varnega sporočanja, če se uporablja varnostni pogoj SM-MAC-G2.

TCS_54 Ukazno sporočilo

Bajt	Dolžina	Vrednost	Opis
CLA	1	‘0Ch’	Zahtevano varno sporočanje.
INS	1	‘B1h’	Read Binary
P1	1	‘00h’	Trenutni EF
P2	1	‘00h’	
Lc	1	‘XXh’	Dolžina polja zaščitenih podatkov
#6	1	‘B3h’	Oznaka za nešifrirano vrednost podatkov, kodirano v BER-TLV.
#7	1	‘NNh’	L_{PV}: dolžina poslanih podatkov
#(8)-#(7+NN)	NN	‘XX..XXh’	Nešifrirani podatki, kodirani v BER-TLV, tj. zamaknjeni podatkovni objekt z oznako ‘54’.
#(8+NN)	1	‘97h’	T_{LE}: oznaka za specifikacijo pričakovane dolžine
#(9+NN)	1	‘01h’	L_{LE}: dolžina pričakovane dolžine
#(10+NN)	1	‘XXh’	Specifikacija pričakovane dolžine (originalni Le): Število bajtov, ki se preberejo.
#(11+NN)	1	‘8Eh’	T_{CC}: Oznaka za kriptografsko kontrolno vsoto
#(12+NN)	1	‘XXh’	L_{CC}: Dolžina naslednje kriptografske kontrolne vsote ‘08h’, ‘0Ch’ ali ‘10h’, odvisno od dolžine ključa AES za varno sporočanje druge generacije (glej Del B iz Dodatka 11).
#(13+NN)-#(12+M+NN)	O	‘XX..XXh’	Kriptografska kontrolna vsota
Le	1	‘00h’	Kakor določa ISO/EEC 7816-4.

▼B

TCS_55 Sporočilo odziva, če je ukaz uspešen.

Bajt	Dolžina	Vrednost	Opis
#1	1	‘B3h’	Nešifrirani podatki, kodirani v BER-TLV.
#2	L	‘NNh’ ali ‘81 NNh’	L_{PV}: dolžina vrnjenih podatkov (=prvotni Le) L je 2 bajta, če je L_{PV}>127 bajtov.
#(2+L)-#(1+L+NN)	NN	‘XX..XXh’	Vrednost nešifriranih podatkov, kodiranih v BER-TLV, tj. prebranih podatkov, enkapsuliranih v diskretnem podatkovnem objektu z oznako ‘53h’.
#(2+L+NN)	1	‘99h’	Stanje obdelave nezaščitenega odziva APDU
#(3+L+NN)	1	‘02h’	Dolžina stanja obdelave
#(4+L+NN) – #(5+L+NN)	2	‘XX XXh’	Stanje obdelave nezaščitenega odziva APDU
#(6+L+NN)	1	‘8Eh’	T_{CC}: oznaka za kriptografsko kontrolno vsoto
#(7+L+NN)	1	‘XXh’	L_{CC}: dolžina naslednje kriptografske kontrolne vsote ‘08h’, ‘0Ch’ ali ‘10h’, odvisno od dolžine ključa AES za varno sporočanje druge generacije (glej Del B iz Dodatka 11).
#(8+L+NN)-#(7+M+L+NN)	O	‘XX..XXh’	Kriptografska kontrolna vsota
SW	2	‘XXXXh’	Opis stanja (SW1, SW2)

3.5.3 *UPDATE BINARY*

Ta ukaz je v skladu z ISO/IEC 7816-4, a ima v primerjavi z opredelitvijo v tem standardu omejeno uporabo.

Ukazno sporočilo UPDATE BINARY sproži posodobitev (brisanje + pisanje) bitov, ki so že prisotni v binarni EF, z biti, danimi v ukazu APDU.

3.5.3.1 Ukaz z zamikom v P1-P2

Ta ukaz omogoča IFD vpis podatkov v trenutno izbrano EF, ne da bi kartica preverjala celovitost prejetih podatkov.

Opomba: ta ukaz brez varnega sporočanja se lahko uporabi za posodobitev datoteke, ki podpira varnostni pogoj ALW za način dostopa za posodobitev.

TCS_56 **Ukazno sporočilo**

Bajt	Dolžina	Vrednost	Opis
CLA	1	‘00h’	
INS	1	‘D6h’	Binarno posodabljanje
P1	1	‘XXh’	Zamik v bajtih od začetka datoteke: bajt z največjo težo
P2	1	‘XXh’	Zamik v bajtih od začetka datoteke: bajt z najmanjšo težo

▼B

Bajt	Dolžina	Vrednost	Opis
Lc	1	‘NNh’	Dolžina podatkov, ki se posodobijo. Število bajtov, ki se zapišejo.
#6-#(5+NN)	NN	‘XX..XXh’	Podatki, ki naj se zapišejo.

Opomba: bit 8 v P1 mora biti nastavljen na 0.

TCS_57 **Sporočilo z odzivom**

Bajt	Dolžina	Vrednost	Opis
SW	2	‘XXXXh’	Opis stanja (SW1, SW2)

— Če je ukaz uspešen, kartica vrne sporočilo ‘**9000**’.

— Če ni izbrana nobena EF, se vrne stanje obdelave ‘**6986**’.

— Če varnostni pogoji za izbrano datoteko niso izpolnjeni, se ukaz prekine s ‘**6982**’.

— Če zamik ni združljiv z velikostjo EF (zamik > velikost EF), se vrne stanje obdelave ‘**6B00**’.

— Če velikost podatkov, ki se zapišejo, ni združljiva z velikostjo EF (zamik + Lc > velikost EF), se vrne stanje obdelave ‘**6700**’.

— Če je zaznana napaka celovitosti v atributih datoteke, kartica šteje datoteko za poškodovano in nepopravljivo, vrne se stanje obdelave ‘**6400**’ ali ‘**6500**’.

— Če je zapisovanje neuspešno, se vrne stanje obdelave ‘**6581**’.

3.5.3.1.1 Ukaz z varnim sporočanjem (primeri)

Ta ukaz omogoča IFD pisanje podatkov v trenutno izbrano EF, pri čemer kartica preveri celovitost prejetih podatkov. Ker se zaupnost ne zahteva, podatki niso šifrirani.

TCS_58 **Ukazno sporočilo**

Bajt	Dolžina	Vrednost	Opis
CLA	1	‘0Ch’	Zahtevano varno sporočanje.
INS	1	‘D6h’	Binarno posodabljanje
P1	1	‘XXh’	Zamik v bajtih od začetka datoteke: bajt z največjo težo.
P2	1	‘XXh’	Zamik v bajtih od začetka datoteke: bajt z najmanjšo težo.
Lc	1	‘XXh’	Dolžina polja zaščitenih podatkov
#6	1	‘81h’	T_{PV}: oznaka za nešifrirane podatke
#7	L	‘NNh’ ali ‘81 NNh’	L_{PV}: dolžina poslanih podatkov. L je 2 bajta, če je L_{PV} > 127 bajtov.

▼B

Bajt	Dolžina	Vrednost	Opis
#(7+L)-#(6+L+NN)	NN	‘XX..XXh’	Vrednost nešifriranih podatkov (ki naj se zapišejo)
#(7+L+NN)	1	‘8Eh’	T_{CC}: oznaka za kriptografsko kontrolno vsoto
#(8+L+NN)	1	‘XXh’	L_{CC}: dolžina naslednje kriptografske kontrolne vsote ‘04h’ za varno sporočanje prve generacije (glej Del A iz Dodatka 11). ‘08h’, ‘0Ch’ ali ‘10h’, odvisno od dolžine ključa AES za varno sporočanje druge generacije (glej Del B iz Dodatka 11).
#(9+L+NN)-#(8+M+L+NN)	O	‘XX..XXh’	Kriptografska kontrolna vsota
Le	1	‘00h’	Kakor določa ISO/EEC 7816-4.

TCS_59 **Sporočilo odgovora pri pravilnem vhodnem formatu varnega sporočanja**

Bajt	Dolžina	Vrednost	Opis
#1	1	‘99h’	T_{SW}: oznaka za opise stanja (ki se zaščitijo s CC)
#2	1	‘02h’	L_{SW}: dolžina vrnjenih opisov stanja
#3-#4	2	‘XXXXh’	Stanje obdelave nezaščitenega odziva APDU
#5	1	‘8Eh’	T_{CC}: oznaka za kriptografsko kontrolno vsoto
#6	1	‘XXh’	L_{CC}: Dolžina naslednje kriptografske kontrolne vsote ‘04h’ za varno sporočanje prve generacije (glej Del A iz Dodatka 11) ‘08h’, ‘0Ch’ ali ‘10h’, odvisno od dolžine ključa AES za varno sporočanje druge generacije (glej Del B iz Dodatka 11).
#7-#(6+L)	L	‘XX..XXh’	Kriptografska kontrolna vsota
SW	2	‘XXXXh’	Opis stanja (SW1, SW2)

„Pravilna“ stanja obdelave, opisana pri ukazu UPDATE BINARY brez varnega sporočanja (glej 3.5.3.1), se lahko vrnejo z uporabo zgoraj opisanih struktur sporočil odziva.

Poleg tega lahko pride do nekaterih napak, povezanih posebej z varnim sporočanjem. V navedenem primeru se enostavno vrne stanje obdelave brez vključitve strukture za varno sporočanje.

TCS_60 **Sporočilo odgovora ob napaki pri varnem sporočanju**

Bajt	Dolžina	Vrednost	Opis
SW	2	‘XXXX’	Opis stanja (SW1, SW2)

▼B

— Če ni na voljo nobenega ključa tekoče seje, se vrne stanje obdelave ‘**6A88**’.

— Če nekateri pričakovani podatkovni objekti (kot so določeni zgoraj) manjkajo v formatu varnega sporočanja, se vrne stanje obdelave ‘**6987**’: ta napaka nastopi, če manjka pričakovana oznaka ali če telo ukaza ni pravilno zgrajeno.

— Če so nekateri podatkovni objekti nepravilni, se vrne stanje obdelave ‘**6988**’. Ta napaka nastopi, če so prisotne vse zahtevane oznake, a se nekatere dolžine razlikujejo od pričakovanih.

— Če ni uspešno preverjanje kriptografske kontrolne vsote, se vrne stanje obdelave ‘**6688**’.

3.5.3.2 Ukaz s kratkim identifikatorjem EF

Ta različica ukaza IFD omogoča, da izbere EF s kratkim identifikatorjem EF in da s te EF zapiše podatke.

TCS_61 Tahografska kartica to različico ukaza podpira za vse EF z določenim kratkim identifikatorjem EF. Ti kratki identifikatorji EF so določeni v poglavju 4.

TCS_62 **Ukazno sporočilo**

Bajt	Dolžina	Vrednost	Opis
CLA	1	‘00h’	
INS	1	‘D6h’	Binarno posodabljanje
P1	1	‘XXh’	Bit 8 je nastavljen na 1. Bita 7 in 6 sta nastavljena na 00. Bit 5 – 1 kodira kratki identifikator EF ustrezajočega EF.
P2	1	‘XXh’	Kodira zamik od 0 do 255 bajtov v EF, na katero se sklicuje P1.
Lc	1	‘NNh’	Dolžina podatkov, ki se posodobijo. Število bajtov, ki se zapišejo.
#6-#(5+NN)	NN	‘XX..XXh’	Podatki, ki se zapišejo.

TCS_63 **Sporočilo z odzivom**

Bajt	Dolžina	Vrednost	Opis
SW	2	‘XXXXh’	Opis stanja (SW1, SW2)

Opomba: kratki identifikatorji EF, ki se uporabljajo za tahografsko aplikacijo druge generacije, so določeni v poglavju 4.

Če P1 kodira kratki identifikator EF in je ukaz uspešen, identificirani EF postane trenutno izbrani EF (trenutni EF).

▼B

— Če je ukaz uspešen, kartica vrne sporočilo ‘**9000**’.

— Če ni najdena datoteka, ki ustreza kratkemu identifikatorju EF, se vrne stanje obdelave ‘**6A82**’,

— Če varnostni pogoji za izbrano datoteko niso izpolnjeni, se ukaz prekine s ‘**6982**’.

— Če zamik ni združljiv z velikostjo EF (zamik > velikost EF), se vrne stanje obdelave ‘**6B00**’.

— Če velikost podatkov, ki se zapišejo, ni združljiva z velikostjo EF (zamik + Lc > velikost EF), se vrne stanje obdelave ‘**6700**’.

— Če je zaznana napaka celovitosti v atributih datoteke, kartica šteje datoteko za poškodovano in nepopravljivo, vrne se stanje obdelave ‘**6400**’ ali ‘**6581**’.

— Če je zapisovanje neuspešno, se vrne stanje obdelave ‘**6581**’.

3.5.3.3 Ukaz z neparnim bajtom instrukcije

Ta različica ukaza IFD omogoča zapis podatkov v EF, ki imajo najmanj 32 768 bajtov.

TCS_64 Tahografska kartica, ki podpira EF z najmanj 32 768 bajtov, podpira to različico ukaza za te EF. Tahografska kartica lahko podpira to različico ukaza za druge EF.

TCS_65 **Ukazno sporočilo**

Bajt	Dolžina	Vrednost	Opis
CLA	1	‘00h’	
INS	1	‘D7h’	Binarno posodabljanje
P1	1	‘00h’	Trenutni EF
P2	1	‘00h’	
Lc	1	‘NNh’	Lc dolžina podatkov v polju s podatki ukaza
#6-#(5+NN)	NN	‘XX..XXh’	Zamaknjeni podatkovni objekt z oznako ‘54h’ || Diskretni podatkovni objekt z oznako ‘53h’, ki enkapsulira podatke, ki se zapišejo.

IFD kodira dolžino zamaknjenega podatkovnega objekta in diskretnega podatkovnega objekta z najmanjšim možnim številom oktetov, tj. z uporabo bajta dolžine ‘01h’ IFD kodira zamik / dolžino od 0 do 255 in z uporabo bajta dolžine ‘02h’ z zamikom / dolžino od ‘256’ do ‘65 535’ bajtov.

TCS_66 **Sporočilo z odzivom**

Bajt	Dolžina	Vrednost	Opis
SW	2	‘XXXXh’	Opis stanja (SW1, SW2)

▼B

— Če je ukaz uspešen, kartica vrne sporočilo ‘**9000**’.

— Če ni izbrana nobena EF, se vrne stanje obdelave ‘**6986**’.

— Če varnostni pogoji za izbrano datoteko niso izpolnjeni, se ukaz prekine s ‘**6982**’.

— Če zamik ni združljiv z velikostjo EF (zamik > velikost EF), se vrne stanje obdelave ‘**6B00**’.

— Če velikost podatkov, ki se zapišejo, ni združljiva z velikostjo EF (zamik + Lc > velikost EF), se vrne stanje obdelave ‘**6700**’.

— Če je zaznana napaka celovitosti v atributih datoteke, kartica šteje datoteko za poškodovano in nepopravljivo, vrne se stanje obdelave ‘**6400**’ ali ‘**6500**’.

— Če je zapisovanje neuspešno, se vrne stanje obdelave ‘**6581**’.

3.5.3.3.1 Ukaz z varnim sporočanjem (primer)

Naslednji primer ponazarja uporabo varnega sporočanja, če se uporablja varnostni pogoj SM-MAC-G2.

TCS_67 Ukazno sporočilo

Bajt	Dolžina	Vrednost	Opis
CLA	1	‘0Ch’	Zahtevano varno sporočanje.
INS	1	‘D7h’	Binarno posodabljanje
P1	1	‘00h’	Trenutni EF
P2	1	‘00h’	
Lc	1	‘XXh’	Dolžina polja zaščitenih podatkov
#6	1	‘B3h’	Oznaka za nešifrirano vrednost podatkov, kodirano v BER-TLV.
#7	L	‘NNh’ ali ‘81 NNh’	L_{PV}: dolžina poslanih podatkov. L je 2 bajta, če je L_{PV} > 127 bajtov.
#(7+L)-#(6+L+NN)	NN	‘XX..XXh’	Nešifrirani podatki, kodirani v BER-TLV, tj. zamaknjeni podatkovni objekt z oznako ‘54’ ||. Diskretni podatkovni objekt z oznako ‘53h’, ki enkapsulira podatke, ki jih je treba zapisati.
#(7+L+NN)	1	‘8Eh’	T_{CC}: Oznaka za kriptografsko kontrolno vsoto
#(8+L+NN)	1	‘XXh’	L_{CC}: Dolžina naslednje kriptografske kontrolne vsote ‘08h’, ‘0Ch’ ali ‘10h’, odvisno od dolžine ključa AES za varno sporočanje druge generacije (glej Del B iz Dodatka 11).
#(9+L+NN)-#(8+M+L+NN)	O	‘XX..XXh’	Kriptografska kontrolna vsota
Le	1	‘00h’	Kakor določa ISO/EEC 7816-4.

▼B

TCS_68 Sporočilo odziva, če je ukaz uspešen.

Bajt	Dolžina	Vrednost	Opis
#1	1	‘99h’	T_{SW}: oznaka za opise stanja (ki se zaščitijo s CC)
#2	1	‘02h’	L_{SW}: dolžina vrnjenih opisov stanja
#3-#4	2	‘XXXXh’	Stanje obdelave nezaščitenega odziva APDU
#5	1	‘8Eh’	T_{CC}: oznaka za kriptografsko kontrolno vsoto
#6	1	‘XXh’	L_{CC}: dolžina naslednje kriptografske kontrolne vsote ‘08h’, ‘0Ch’ ali ‘10h’, odvisno od dolžine ključa AES za varno sporočanje druge generacije (glej Del B iz Dodatka 11).
#7-#(6+L)	L	‘XX..XXh’	Kriptografska kontrolna vsota
SW	2	‘XXXXh’	Opis stanja (SW1, SW2)

3.5.4 *GET CHALLENGE*

Ta ukaz je v skladu z ISO/IEC 7816-4, a ima v primerjavi z opredelitvijo v tem standardu omejeno uporabo.

Ukaz GET CHALLENGE zahteva od kartice, da pošlje poziv, ki bo uporabljen pri določenem varnostnem postopku, s katerim se kartici pošlje kriptogram ali šifrirane podatke.

TCS_69 Poziv, ki ga izda kartica, velja le za naslednji ukaz, ki uporablja poziv, poslan kartici.

TCS_70 **Ukazno sporočilo**

Bajt	Dolžina	Vrednost	Opis
CLA	1	‘00h’	
INS	1	‘84h’	INS
P1	1	‘00h’	P1
P2	1	‘00h’	P2
Le	1	‘08h’	Le (dolžina pričakovanega poziva)

TCS_71 **Sporočilo z odzivom**

Bajt	Dolžina	Vrednost	Opis
#1-#8	8	‘XX..XXh’	Poziv
SW	2	‘XXXXh’	Opis stanja (SW1, SW2)

— Če je ukaz uspešen, kartica vrne sporočilo ‘**9000**’.

— Če je Le različen od ‘08h’, je stanje obdelave ‘**6700**’.

— Če parametra P1-P2 nista pravilna, je stanje obdelave ‘**6A86**’.

▼B

3.5.5 *VERIFY*

Ta ukaz je v skladu z ISO/IEC 7816-4, a ima v primerjavi z opredelitvijo v tem standardu omejeno uporabo.

Le za kartico servisne delavnice se zahteva, da podpira ta ukaz.

Druge vrste tahografskih kartic lahko izvedejo ta ukaz ali pa tudi ne, vendar za te kartice ni personaliziranega referenčnega CHV. Zato te kartice tega ukaza ne morejo uspešno izvesti. Vedenje drugih vrst tahografskih kartic, ki niso kartice servisne delavnice, tj. vrne se koda napake, je zunaj področja uporabe te specifikacije, če se pošlje ta ukaz.

Ukaz VERIFY sproži na kartici primerjavo podatkov CHV (PIN), poslanih z ukazom, z referenčnim CHV, shranjenim na kartici.

TCS_72 PIN, ki ga vnese uporabnik, mora IFD kodirati v ASCII in na desni zapolniti z bajti ‘FFh’ do skupne dolžine 8 bajtov, glej tudi podatkovni tip WorkshopCardPIN iz Dodatka 1.

TCS_73 Tahografske aplikacije prve in druge generacije uporabljajo isti referenčni CHV.

TCS_74 Tahografska kartica preveri, ali je ukaz pravilno kodiran. Če ukaz ni pravilno kodiran, kartica ne primerja vrednosti CHV, ne zniža stanja števca preostalih poskusov CHV in ne ponastavi varnostnega stanja‘PIN_Verified’, ampak prekine ukaz. Ukaz je kodiran pravilno, če imajo bajti CLA, INS, P1, P2, Lc določene vrednosti, je Le odsoten in je podatkovno polje pravilne dolžine.

TCS_75 Če je ukaz uspešen, se števec preostalih poskusov CHV ponovno zažene. Začetna vrednost števca preostalih poskusov CHV je 5. Če je ukaz uspešen, kartica nastavi notranje varnostno stanje na ‘PIN_Verified’. Kartica ponastavi to varnostno stanje, če se kartica ponastavi ali če se koda CHV, poslana v ukazu, ne ujema s shranjenim referenčnim CHV.

Opomba: uporaba istega referenčnega CHV in globalnega varnostnega statusa preprečuje, da bi moral delavec servisne delavnice po izbiri druge tahografske aplikacije DF ponovno vnesti PIN.

TCS_76 Neuspešna primerjava se zapiše na kartico, tj. števec preostalih poskusov CHV se zniža za ena, da se omeji število nadaljnjih poskusov uporabe referenčnega CHV.

TCS_77 **Ukazno sporočilo**

Bajt	Dolžina	Vrednost	Opis
CLA	1	‘00h’	
INS	1	‘20h’	INS
P1	1	‘00h’	P1

▼B

Bajt	Dolžina	Vrednost	Opis
P2	1	‘00h’	P2 (preverjani CHV je implicitno znan)
Lc	1	‘08h’	Dolžina kode CHV, ki se pošilja
#6-#13	8	‘XX..XXh’	CHV

TCS_78 **Sporočilo z odzivom**

Bajt	Dolžina	Vrednost	Opis
SW	2	‘XXXXh’	Opis stanja (SW1, SW2)

— Če je ukaz uspešen, kartica vrne sporočilo ‘**9000**’.

— Če referenčni CHV ni najden, se vrne stanje obdelave ‘**6A88**’.

— Če je CHV blokiran (števec preostalih poskusov za CHV je nič), se vrne stanje obdelave ‘**6983**’. Ko določen CHV enkrat pride v to stanje, ga ni nikoli več mogoče uspešno predstaviti.

— Če je primerjava neuspešna, se števec preostalih poskusov zmanjša in se vrne stanje obdelave ‘**63CX**’ (X>0, pri čemer je X vrednost števca preostalih poskusov CHV).

— Če se šteje, da je referenčni CHV poškodovan, se vrne stanje obdelave ‘**6400**’ ali ‘**6581**’.

— Če je Le različen od ‘08h’, je stanje obdelave ‘**6700**’.

3.5.6 *GET RESPONSE*

Ta ukaz je v skladu s standardom ISO/IEC 7816-4.

Ta ukaz (potreben in razpoložljiv le pri protokolu T=0) se uporablja za prenos pripravljenih podatkov s kartice v vmesniško napravo (primer, ko ukaz vključuje tako Lc kot Le).

Ukaz GET RESPONSE mora biti izdan neposredno po ukazu za pripravo podatkov, sicer so podatki izgubljeni. Po izvedbi ukaza GET RESPONSE predhodno pripravljeni podatki niso več na voljo (razen ob napaki ‘**61xx**’ ali ‘**6Cxx**’, glej spodaj).

TCS_79 **Ukazno sporočilo**

Bajt	Dolžina	Vrednost	Opis
CLA	1	‘00h’	
INS	1	‘C0h’	
P1	1	‘00h’	
P2	1	‘00h’	
Le	1	‘XXh’	Število pričakovanih bajtov

▼B

TCS_80 **Sporočilo z odzivom**

Bajt	Dolžina	Vrednost	Opis
#1-#X	X	‘XX..XXh’	Podatki
SW	2	‘XXXXh’	Opis stanja (SW1, SW2)

— Če je ukaz uspešen, kartica vrne sporočilo ‘**9000**’.

— Če kartica ni pripravila nobenih podatkov, se vrne stanje obdelave ‘**6900**’ ali ‘**6F00**’.

— Če Le presega število razpoložljivih bajtov ali če je Le nič, se vrne stanje obdelave ‘**6Cxx**’, pri čemer ‘xx’ označuje natančno število razpoložljivih bajtov. V navedenem primeru ostanejo pripravljeni podatki na voljo za naslednji ukaz GET RESPONSE.

— Če Le ni nič in je manjši od števila razpoložljivih bajtov, kartica običajno pošlje zahtevano število bajtov in se vrne stanje obdelave ‘**61xx**’, pri čemer ‘xx’ pomeni število dodatnih bajtov, ki so še na voljo za naslednji ukaz GET RESPONSE.

— Če ukaz ni podprt (protokol T=1), kartica vrne stanje obdelave ‘**6D00**’.

3.5.7 *PSO: VERIFY CERTIFICATE*

Ta ukaz je v skladu z ISO/IEC 7816-8, a ima v primerjavi z opredelitvijo v tem standardu omejeno uporabo.

Ukaz VERIFY CERTIFICATE uporablja kartica, da pridobi od zunaj javni ključ in preveri njegovo veljavnost.

3.5.7.1 Ukaz za prvo generacijo – par odgovorov

TCS_81 To različico ukaza podpira le tahografska aplikacija prve generacije.

TCS_82 Če je ukaz VERIFY CERTIFICATE uspešen, se javni ključ shrani za nadaljnjo uporabo v varnem okolju. Ta ključ se s svojim identifikatorjem ključa izrecno nastavi z ukazom MSE (glej poglavje 3.5.11) za uporabo pri ukazih, povezanih z varnostjo (INTERNAL AUTHENTICATE, EXTERNAL AUTHENTICATE ali VERIFY CERTIFICATE).

TCS_83 V vsakem primeru ukaz VERIFY CERTIFICATE uporablja za odpiranje certifikata javni ključ, ki ga je pred tem izbral ukaz MSE. Ta javni ključ mora biti javni ključ države članice ali evropski javni ključ.

TCS_84 **Ukazno sporočilo**

Bajt	Dolžina	Vrednost	Opis
CLA	1	‘00h’	
INS	1	‘2Ah’	Izvedba varnostne operacije
P1	1	‘00h’	P1

▼B

Bajt	Dolžina	Vrednost	Opis
P2	1	‘AEh’	P2: podatki, ki niso kodirani z BER-TLV (združevanje podatkovnih elementov).
Lc	1	‘C2h’	Lc: dolžina certifikata, 194 bajtov
#6-#199	194	‘XX..XXh’	Certifikat: združevanje podatkovnih elementov (kot je opisano v Dodatku 11)

TCS_85 **Sporočilo z odzivom**

Bajt	Dolžina	Vrednost	Opis
SW	2	‘XXXXh’	Opis stanja (SW1, SW2)

— Če je ukaz uspešen, kartica vrne sporočilo ‘**9000**’.

— Če preverjanje certifikata ni uspešno, se vrne stanje obdelave ‘**6688**’. Proces preverjanja in odpiranja certifikata je opisan v Dodatku 11 za G1 in G2.

— Če v varnem okolju ni prisotnega javnega ključa, se vrne stanje obdelave ‘**6A88**’.

— Če se šteje, da je izbrani javni ključ (uporabljen za razvitje certifikata) poškodovan, se vrne stanje obdelave ‘**6400**’ ali ‘**6581**’.

— Le prva generacija: če ima izbrani javni ključ (uporabljen za odpiranje certifikata) CHA.LSB (`CertificateHolderAuthorisation.equipmentType`), ki je različen od ‘00’ (tj. ni javni ključ države članice ali evropski javni ključ), se vrne stanje obdelave ‘**6985**’.

3.5.7.2 Ukaz za drugo generacijo – par odgovorov

Odvisno od velikosti krivulje so lahko certifikati ECC tako dolgi, da jih ni mogoče prenesti v enem APDU. V tem primeru je treba uporabiti veriženje ukazov v skladu z ISO/IEC 7816-4 in prenesti certifikat v dveh zaporednih PSO: preverjanje APDU certifikata (Verify Certificate APDUs).

Struktura certifikata in parametri domene so opredeljeni v Dodatku 11.

TCS_86 Ukaz se lahko izvede le pri MF, DF Tachograph in DF Tachograph_G2, glej tudi TCS_33.

TCS_87 **Ukazno sporočilo**

Bajt	Dolžina	Vrednost	Opis
CLA	1	‘X0h’	CLA bajt označuje veriženje ukazov: ‘00h’ je edini ali zadnji ukaz verige ‘10h’ ni zadnji ukaz verige.
INS	1	‘2Ah’	Izvedba varnostne operacije
P1	1	‘00h’	
P2	1	‘BEh’	Preverjanje samoopisnega certifikata

▼B

Bajt	Dolžina	Vrednost	Opis
Lc	1	‘XXh’	Dolžina podatkov v polju s podatki ukaza, glej TCS_88 in TCS_89.
#6-#5+L	L	‘XX..XXh’	Kodirani podatki DER-TLV: podatkovni objekt telesa certifikata ECC kot prvi podatkovni objekt, združen s podatkovnim objektom podpisa certifikata ECC kot drugim podatkovnim objektom ali delom te združitve. Oznaka 7F21 in ustrezajoča dolžina se ne pošljeta. Zaporedje teh podatkovnih objektov je stalno.

TCS_88 Za kratke APDU se uporabljajo naslednje določbe: IFD uporabi najmanjše število APDU, ki je potrebno za pošiljanje ukaza in pošlje največje mogoče število bajtov v prvem ukazu APDU v skladu z vrednostjo bajta velikosti podatkovnega polja na kartici, glej TCS_14. Če se IFD vede drugače, je vedenje kartice zunaj področja uporabe.

TCS_89 Za podaljšano dolžino APDU se uporabljajo naslednje določbe: Če je certifikat prevelik za en APDU, mora kartica podpirati veriženje ukazov. IFD uporabi najmanjše število APDU, ki je potrebno za pošiljanje ukaza in pošlje največje mogoče število bajtov v prvem ukazu APDU. Če se IFD vede drugače, je vedenje kartice zunaj področja uporabe.

Opomba: v skladu z Dodatkom 11 kartica shrani certifikat ali relevantno vsebino certifikata in posodobi svoj currentAuthenticatedTime.

Struktura sporočil odziva in opisi stanja, kot so opredeljeni v TCS_85.

TCS_90 Poleg kod napak iz TCS_85, kartica lahko vrne naslednje kode napak:

— Če ima izbrani javni ključ (uporabljen za odpiranje certifikata) CHA.LSB (CertificateHolderAuthorisation.equipmentType), ki ni ustrezen za preverjanje certifikata v skladu z Dodatkom 11, se vrne stanje obdelave ‘**6985**’.

— Če je currentAuthenticatedTime kartice poznejši od datuma izteka certifikata, se vrne stanje obdelave ‘**6985**’.

— Če se pričakuje zadnji verige, kartica vrne stanje obdelave ‘**6883**’.

— Če so poslani nepravilni parametri v polju s podatki ukaza, kartica vrne stanje obdelave ‘**6A80**’ (uporablja se tudi, kadar podatkovni objekti niso poslani v določenem zaporedju).

▼B

3.5.8 *INTERNAL AUTHENTICATE*

Ta ukaz je v skladu s standardom ISO/IEC 7816-4.

TCS_91 Vse tahografske kartice podpirajo ta ukaz pri tahografu DF prve generacije. Ukaz je lahko dostopen v MF in / ali DF tahografa druge generacije, lahko pa tudi ni. Če je dostopen, se izvedba ukaza zaključi z ustrezno kodo napake, saj je zasebni ključ kartice (Card.SK) za avtentikacijski protokol prve generacije dostopen le v DF tahografa prve generacije.

Z ukazom INTERNAL AUTHENTICATE lahko IFD avtenticira kartico. Postopek avtentikacije je opisan v Dodatku 11. Vključuje naslednje izjave:

TCS_92 ukaz INTERNAL AUTHENTICATE uporablja zasebni ključ kartice (izbran implicitno) za podpisovanje avtentikacijskih podatkov, vključno s K1 (prvi element za dogovor o ključu seje) in RND1, ter uporablja trenutno izbrani javni ključ (izbran z zadnjim ukazom MSE) za šifriranje podpisa in oblikovanje avtentikacijskega žetona (podrobneje opisan v Dodatku 11).

TCS_93 **Ukazno sporočilo**

Bajt	Dolžina	Vrednost	Opis
CLA	1	‘00h’	CLA
INS	1	‘88h’	INS
P1	1	‘00h’	P1
P2	1	‘00h’	P2
Lc	1	‘10h’	Dolžina podatkov, poslanih kartici.
#6 – #13	8	‘XX..XXh’	Poziv, uporabljen za avtentikacijo kartice.
#14 -#21	8	‘XX..XXh’	VU.CHR (glej Dodatek 11)
Le	1	‘80h’	Dolžina podatkov, pričakovanih s kartice.

TCS_94 **Sporočilo z odzivom**

Bajt	Dolžina	Vrednost	Opis
#1-#128	128	‘XX..XXh’	Avtentikacijski žeton kartice (glej Dodatek 11)
SW	2	‘XXXXh’	Opis stanja (SW1, SW2)

— Če je ukaz uspešen, kartica vrne sporočilo ‘**9000**’.

— Če v varnem okolju ni prisoten noben javni ključ, se vrne stanje obdelave ‘**6A88**’.

— Če v varnem okolju ni prisoten noben zasebni ključ, se vrne stanje obdelave ‘**6A88**’.

— Če se VU.CHR ne ujema z identifikatorjem trenutnega javnega ključa, se vrne stanje obdelave ‘**6A88**’.

▼B

— Če se šteje, da je izbrani zasebni ključ poškodovan, se vrne stanje obdelave '**6400**' ali '**6581**'.

TCS_95 Če je ukaz INTERNAL AUTHENTICATE uspešen, se trenutni ključ seje (če obstaja) izbriše in ni več na voljo. Pogoj za razpoložljivost novega ključa seje je uspešna izvedba ukaza EXTERNAL AUTHENTICATE za avtentikacijski mehanizem prve generacije.

3.5.9 *EXTERNAL AUTHENTICATE*

Ta ukaz je v skladu s standardom ISO/IEC 7816-4.

Z ukazom EXTERNAL AUTHENTICATE lahko kartica avtenticira IFD. Postopek avtentikacije je opisan v Dodatku 11 za tahograf prve in druge generacije (avtentikacija VU).

TCS_96 Različico ukaza za mehanizem za medsebojno avtentikacijo prve generacije podpira le tahografska aplikacija prve generacije.

TCS_97 Različica ukaza za medsebojno avtentikacijo kartice in enote v vozilu se lahko izvede le pri MF, DF Tachograph in DF Tachograph_G2, glej tudi TCS_34.

TCS_98 **Ukazno sporočilo**

Bajt	Dolžina	Vrednost	Opis
CLA	1	'00h'	CLA
INS	1	'82h'	INS
P1	1	'00h'	Implicitno znani ključi in algoritmi
P2	1	'00h'	
Lc	1	'XXh'	Lc (dolžina podatkov, poslanih kartici)
#6-#(5+L)	L	'XX..XXh'	Avtentikacija prve generacije: kriptogram (glej Del A iz Dodatka 11). Avtentikacija druge generacije: podpis, ki ga je ustvaril IFD (glej Del B iz Dodatka 11).

TCS_99 **Sporočilo z odzivom**

Bajt	Dolžina	Vrednost	Opis
SW	2	'XXXXh'	Opis stanja (SW1, SW2)

— Če je ukaz uspešen, kartica vrne sporočilo '**9000**'.

— Če CHA trenutno nastavljenega javnega ključa ni združitev AID tahografske aplikacije in vrste opreme VU, se vrne stanje obdelave '**6F00**'.

— Če neposredno pred tem ukazom ni bil poslan ukaz GET CHALLENGE, se vrne stanje obdelave '**6985**'.

▼B

Tahografska aplikacija prve generacije lahko vrne naslednje dodatne kode napake:

— Če v varnem okolju ni prisotnega javnega ključa, se vrne stanje obdelave ‘**6A88**’.

— Če v varnem okolju ni prisoten noben zasebni ključ, se vrne stanje obdelave ‘**6A88**’.

— Če ni uspešno preverjanje kriptograma, se vrne stanje obdelave ‘**6688**’.

— Če se šteje, da je izbrani zasebni ključ poškodovan, se vrne stanje obdelave ‘**6400**’ ali ‘**6581**’.

Različica ukaza za avtentikacijo druge generacije lahko vrne naslednjo dodatno kodo napake:

— Če je bilo preverjanje podpisa neuspešno, kartica vrne sporočilo ‘**6300**’.

3.5.10 *GENERAL AUTHENTICATE*

Ta ukaz se uporablja za avtentikacijski protokol za čip druge generacije, ki je določen v Dodatku 11 iz dela B, in je v skladu s standardom ISO/IEC 7816-4.

TCS_100 Ukaz se lahko izvede le pri MF, DF Tachograph in DF Tachograph_G2, glej tudi TCS_34.

TCS_101 **Ukazno sporočilo**

Bajt	Dolžina	Vrednost	Opis
CLA	1	‘00h’	
INS	1	‘86h’	
P1	1	‘00h’	Implicitno znani ključi in protokol
P2	1	‘00h’	
Lc	1	‘NNh’	Lc: dolžina naslednjega podatkovnega polja
#6-#(5+L)	L	‘7Ch’ + L_{7C} + ‘80h’ + L_{80} + ‘XX..XXh’	DER-TLV kodirana kratkotrajna vrednost javnega ključa (glej Dodatek 11). VU pošlje podatkovne objekte v tem zaporedju.

TCS_102 **Sporočilo z odzivom**

Bajt	Dolžina	Vrednost	Opis
#1-#L	L	‘7Ch’ + L_{7C} + ‘81h’ + ‘08h’ + ‘XX..XXh’ + ‘82h’ + L_{82} + ‘XX..XXh’	DER-TLV kodirani podatki dinamične avtentikacije: enkratnik in avtentikacijski žeton (glej Dodatek 11).
SW	2	‘XXXXh’	Opis stanja (SW1, SW2)

— Če je ukaz uspešen, kartica vrne sporočilo ‘**9000**’.

— Kartica vrne stanje obdelave ‘**6A80**’, ki kaže na nepravilne parametre v podatkovnem polju.

▼B

— Kartica vrne stanje obdelave ‘**6982**’, če ukaz External Authenticate ni bil uspešno izveden.

Objekt odziva dinamične avtentikacije podatkov ‘7Ch’

— mora biti prisoten, če je operacija uspešna, tj. opis stanja je ‘**9000**’,

— mora biti odsoten v primeru napake pri izvajanju ali preverjanju, oziroma, če so opisi stanja v območju ‘**6400**’ – ‘**6FFF**’, in

— je lahko odsoten v primeru opozorila, tj. če so opisi stanja v območju ‘**6200**’ – ‘**63FF**’.

3.5.11 *MANAGE SECURITY ENVIRONMENT*

Ta ukaz se uporablja za nastavitev javnega ključa za avtentikacijo.

3.5.11.1 Ukaz za prvo generacijo – par odgovorov

Ta ukaz je v skladu s standardom ISO/IEC 7816-4. Uporaba ukaza pa je glede na s tem povezani standard omejena.

TCS_103 Ta ukaz podpira le tahografska aplikacija prve generacije.

TCS_104 Ključ, naveden v podatkovnem polju MSE, ostane trenutno izbrani javni ključ do naslednjega ukaza MSE, izbranega DF ali ponastavitve kartice.

TCS_105 Če referenčni javni ključ (še) ni prisoten na kartici, ostane varno okolje nespremenjeno.

TCS_106 **Ukazno sporočilo**

Bajt	Dolžina	Vrednost	Opis
CLA	1	‘00h’	CLA
INS	1	‘22h’	INS
P1	1	‘C1h’	P1: navedeni ključ, veljaven za vse kriptografske postopke
P2	1	‘B6h’	P2 (navedeni podatki o digitalnem podpisu)
Lc	1	‘0Ah’	Lc: dolžina naslednjega podatkovnega polja
#6	1	‘83h’	Oznaka za navajanje javnega ključa v asimetričnih primerih
#7	1	‘08h’	Dolžina navedbe ključa (identifikatorja ključa)
#8-#15	8	‘XX..XXh’	Identifikator ključa, kot je določen v Dodatku 11.

TCS_107 **Sporočilo z odzivom**

Bajt	Dolžina	Vrednost	Opis
SW	2	‘XXXXh’	Opis stanja (SW1, SW2)

▼B

— Če je ukaz uspešen, kartica vrne sporočilo ‘**9000**’.

— Če navedenega ključa ni v kartici, se vrne stanje obdelave ‘**6A88**’.

— Če nekateri pričakovani podatkovni objekti manjkajo v formatu varnega sporočanja, se vrne stanje obdelave ‘**6987**’. To se lahko zgodi, če manjka oznaka ‘83h’.

— Če so nekateri podatkovni objekti nepravilni, se vrne stanje obdelave ‘**6988**’. To se lahko zgodi, če dolžina identifikatorja ključa ni ‘08h’.

— Če se šteje, da je izbrani ključ poškodovan, se vrne stanje obdelave ‘**6400**’ ali ‘**6581**’.

3.5.11.2 Ukaz za drugo generacijo – par odgovorov

Za avtentikacijo druge generacije tahografska kartica podpira naslednjo MSE: nastavljene različice ukaza, skladne z ISO/IEC 7816-4. Te različice ukaza niso podprte za avtentikacijo prve generacije.

3.5.11.2.1 MSE:SET AT za avtentikacijo čipa

Naslednji ukaz MSE:SET AT se uporablja za izbiro parametrov za avtentikacijo čipa, ki jo nato izvede ukaz General Authenticate.

TCS_108 Ukaz se lahko izvede le pri MF, DF Tachograph in DF Tachograph_G2, glej tudi TCS_34.

TCS_109 **Ukazno sporočilo MSE:SET AT za avtentikacijo čipa**

Bajt	Dolžina	Vrednost	Opis
CLA	1	‘00h’	
INS	1	‘22h’	
P1	1	‘41h’	Nastavljeno za notranjo avtentikacijo
P2	1	‘A4h’	Avtentikacija
Lc	1	‘NNh’	Lc: dolžina naslednjega podatkovnega polja
#6-#(5+L)	L	‘80h’ + ‘0Ah’ + ‘XX..XXh’	DER-TLV kodirano sklicevanje na kriptografski mehanizem: identifikator objekta ali avtentikacija čipa (samo vrednost, oznaka ‘06h’ se opusti). Glej Dodatek 1 za vrednosti identifikatorjev objekta; uporablja se zapis v bajtih. Glej Dodatek 11 za navodila, kako izbrati enega od teh identifikatorjev objekta.

3.5.11.2.2 MSE:SET AT za avtentikacijo VU

Naslednji ukaz MSE:SET AT se uporablja za izbiro parametrov in ključev za avtentikacijo VU, ki jo nato opravi ukaz External Authenticate.

▼B

TCS_110 Ukaz se lahko izvede le pri MF, DF Tachograph in DF Tachograph_G2, glej tudi TCS_34.

TCS_111 **Ukazno sporočilo MSE:SET AT za avtentikacijo enote v vozilu**

Bajt	Dolžina	Vrednost	Opis
CLA	1	‘00h’	
INS	1	‘22h’	
P1	1	‘81h’	Nastavljeno za zunanjo avtentikacijo
P2	1	‘A4h’	Avtentikacija
Lc	1	‘NNh’	Lc: dolžina naslednjega podatkovnega polja
#6-#(5+L)	L	‘80h’ + ‘0Ah’ + ‘XX..XXh’	DER-TLV kodirano sklicevanje na kriptografski mehanizem: Identifikator objekta ali avtentikacija VU (samo vrednost, oznaka ‘06h’ se opusti). Glej Dodatek 1 za vrednosti identifikatorjev objekta; uporablja se zapis v bajtih. Glej Dodatek 11 za navodila, kako izbrati enega od teh identifikatorjev objekta.
		‘83h’ + ‘08h’ + ‘XX..XXh’	DER-TLV kodirano sklicevanje javnega ključa enote v vozilu s sklicevanjem na imetnika certifikata, ki je navedeno v njegovem certifikatu.
		‘91h’ + L_{91} + ‘XX..XXh’	DER-TLV kodirana stisnjena predstavitev kratkotrajnega javnega ključa VU, ki se uporablja med avtentikacijo čipa (glej Dodatek 11).

3.5.11.2.3 MSE:SET DST

Naslednji ukaz MSE:SET DST se uporablja za nastavitev javnega ključa za

— preverjanje podpisa iz naslednjega ukaza PSO: Verify Digital Signature ali

— za preverjanje podpisa certifikata iz naslednjega ukaza PSO: Verify Certificate.

TCS_112 Ukaz se lahko izvede le pri MF, DF Tachograph in DF Tachograph_G2, glej tudi TCS_33.

TCS_113 **Ukazno sporočilo MSE:SET DST**

Bajt	Dolžina	Vrednost	Opis
CLA	1	‘00h’	
INS	1	‘22h’	
P1	1	‘81h’	Nastavljeno za preverjanje
P2	1	‘B6h’	Digitalni podpis

▼B

Lc	1	‘NNh’	Lc: dolžina naslednjega podatkovnega polja
#6-#(5+L)	L	‘83h’ + ‘08h’ + ‘XX...XXh’	DER-TLV kodirano sklicevanje javnega ključa, tj. sklicevanje na imetnika certifikata v certifikatu javnega ključa (glej Dodatek 11).

Za vse različice ukaza so struktura sporočil odziva in opisi stanja podani z naslednjim:

TCS_114 **Sporočilo z odzivom**

Bajt	Dolžina	Vrednost	Opis
SW	2	‘XXXXh’	Opis stanja (SW1, SW2)

— Če je ukaz uspešen, kartica vrne sporočilo ‘**9000**’. Protokol je bil izbran in sprožen.

— ‘**6A80**’ označuje nepravilne parametre v polju s podatki ukaza.

— ‘**6A88**’ označuje, da navedeni podatki (tj. navedeni ključ) niso na voljo.

3.5.12 *PSO: HASH*

Ta ukaz se uporablja za prenos rezultatov izračunov zgostitve določenih podatkov na kartico. Ta ukaz se uporablja za preverjanje digitalnih podpisov. Zgoščena vrednost je začasno shranjena za naslednji ukaz PSO: Verify Digital Signature.

Ta ukaz je v skladu s standardom ISO/IEC 7816-8. Uporaba ukaza pa je glede na s tem povezani standard omejena.

Le za nadzorno kartico se zahteva, da podpira ta ukaz v DF Tachograph in DF Tachograph_G2.

Druge vrste tahografskih kartic lahko izvedejo ta ukaz, lahko pa tudi ne. Ukaz je lahko dostopen v MF, lahko pa tudi ni.

Aplikacija nadzorne kartice prve generacije podpira le SHA-1.

TCS_115 Začasno shranjena zgoščena vrednost se izbriše, če se s PSO izračuna nova zgoščena vrednost: ukaz HASH, če je izbran DF in se tahografska kartica ponastavi.

TCS_116 **Ukazno sporočilo**

Bajt	Dolžina	Vrednost	Opis
CLA	1	‘00h’	CLA
INS	1	‘2Ah’	Izvedba varnostne operacije
P1	1	‘90h’	Vrnitev zgoščene kode

▼B

Bajt	Dolžina	Vrednost	Opis
P2	1	‘A0h’	Oznaka: podatkovno polje vsebuje DO, pomembne za zgoščevanje
Lc	1	‘XXh’	Dolžina Lc naslednjega podatkovnega polja
#6	1	‘90h’	Oznaka za zgoščeno kodo
#7	1	‘XXh’	Dolžina zgoščene kode ‘14h’ v aplikaciji prve generacije (glej Del A iz Dodatka 11) ‘20h’, ‘30h’ or ‘40h’ v aplikaciji druge generacije (glej Del B iz Dodatka 11).
#8-#(7+L)	L	‘XX..XXh’	Zgoščena koda

TCS_117 **Sporočilo z odzivom**

Bajt	Dolžina	Vrednost	Opis
SW	2	‘XXXXh’	Opis stanja (SW1, SW2)

— Če je ukaz uspešen, kartica vrne sporočilo ‘**9000**’.

— Če nekateri pričakovani podatkovni objekti (predpisani zgoraj) manjkajo, se vrne stanje obdelave ‘**6987**’. To se lahko zgodi, če manjka oznaka ‘90h’.

— Če so nekateri podatkovni objekti nepravilni, se vrne stanje obdelave ‘**6988**’. Ta napaka nastopi, če je zahtevana oznaka prisotna, vendar se njena dolžina razlikuje od ‘14h’ za SHA-1, ‘20h’ za SHA-256, ‘30h’ za SHA-384, ‘40h’ za SHA-512 (aplikacija druge generacije).

3.5.13 *PERFORM HASH of FILE*

Ta ukaz ni v skladu z ISO/IEC 7816-8. Tako bajt CLA tega ukaza označuje, da gre za lastno uporabo ukaza PERFORM SECURITY OPERATION / HASH.

Le za vozniško kartico in kartico servisne delavnice se zahteva, da podpirata ta ukaz v DF Tachograph in DF Tachograph_G2.

Druge vrste tahografskih kartic lahko izvedejo ta ukaz, lahko pa tudi ne. Če kartica podjetja ali nadzorna kartica izvede ta ukaz, se ukaz izvede, kakor je določeno v tem poglavju.

Ukaz je lahko dostopen v MF, lahko pa tudi ni. V tem primeru se ukaz izvede, kot je določeno v tem poglavju, tj. ukaz ne dovoljuje izračuna zgoščene vrednosti, ampak se zaključi z ustrezno kodo napake.

TCS_118 Ukaz PERFORM HASH of FILE se uporablja za zgoščevanje podatkovnega polja trenutno izbranega transparentnega EF.

TCS_119 Tahografska kartica ta ukaz podpira le za EF, navedene v poglavju 4 pod DF_Tachograph in DF_Tachograph_G2 z naslednjo izjemo. Tahografska kartica ne podpira ukaza za EF Sensor_Installation_Data pri DF Tachograph_G2.

▼B

TCS_120 Rezultat postopka zgoščevanja se začasno shrani na kartici. Nato se lahko uporablja za pridobitev digitalnega podpisa iz datoteke s PSO: Ukaz COMPUTE DIGITAL SIGNATURE

TCS_121 Začasno shranjena zgoščena vrednost datoteke se izbriše, če se s PSO izračuna nova zgoščena vrednost datoteke: Ukaz Hash of File, če je izbran DF in je tahografska kartica ponastavljena.

TCS_122 Tahografska aplikacija prve generacije podpira SHA-1.

TCS_123 Tahografska aplikacija druge generacije podpira SHA-1 in SHA-2 (256, 384 in 512 bitov).

TCS_124 **Ukazno sporočilo**

Bajt	Dolžina	Vrednost	Opis
CLA	1	‘80h’	CLA
INS	1	‘2Ah’	Izvedba varnostne operacije
P1	1	‘90h’	Oznaka: Hash
P2	1	‘XXh’	P2: označuje algoritem, ki se uporabi za zgoščevanje podatkov v trenutno izbrani transparentni datoteki: ‘00h’ za SHA-1 ‘01h’ za SHA-256 ‘02h’ za SHA-384 ‘03h’ za SHA-512.

TCS_125 **Sporočilo z odzivom**

Bajt	Dolžina	Vrednost	Opis
SW	2	‘XXXXh’	Opis stanja (SW1, SW2)

— Če je ukaz uspešen, kartica vrne sporočilo ‘**9000**’.

— Če trenutni EF tega ukaza ne dovoljuje (EF Sensor_Installation_Data v DF Tachograph_G2), se vrne stanje obdelave ‘**6985**’.

— Če se šteje, da je izbrana EF poškodovana (napake celovitosti v atributih datoteke ali shranjenih podatkih), se vrne stanje obdelave ‘**6400**’ ali ‘**6581**’.

— Če izbrana datoteka ni transparentna ali ni trenutnega EF, se vrne stanje obdelave ‘**6986**’.

3.5.14 *PSO: COMPUTE DIGITAL SIGNATURE*

Ta ukaz se uporablja za izračun digitalnega podpisa prej izračunane zgoščene kode (glej *PERFORM HASH of FILE*, poglavje 3.5.13).

Le za vozniško kartico in kartico servisne delavnice se zahteva, da podpirata ta ukaz v DF Tachograph in DF Tachograph_G2.

▼B

Druge vrste tahografskih kartic lahko izvedejo ta ukaz ali pa tudi ne, vendar nimajo ključa podpisa. Zato te kartice ukaza ne morejo uspešno izvesti, ampak ga zaključijo z ustrezno kodo napake.

Ukaz je lahko dostopen v MF, lahko pa tudi ni. V tem primeru se ukaz zaključi z ustrezno kodo napake.

Ta ukaz je v skladu s standardom ISO/IEC 7816-8. Uporaba ukaza pa je glede na s tem povezani standard omejena.

TCS_126 Ta ukaz ne izračuna digitalnega podpisa predhodno izračunane zgoščene kode s PSO: ukaz HASH.

TCS_127 Zasebni ključ kartice se uporablja za izračun digitalnega podpisa in ga kartica implicitno pozna.

TCS_128 Tahografska aplikacija prve generacije izdela digitalni podpis z metodo zapolnitve v skladu s PKCS1 (za podrobnosti glej Dodatek 11).

TCS_129 Tahografska aplikacija druge generacije izračuna digitalni podpis na osnovi eliptične krivulje (za podrobnosti glej Dodatek 11).

TCS_130 **Ukazno sporočilo**

Bajt	Dolžina	Vrednost	Opis
CLA	1	‘00h’	CLA
INS	1	‘2Ah’	Izvedba varnostne operacije
P1	1	‘9Eh’	Digitalni podpis, ki ga je treba vrniti.
P2	1	‘9Ah’	Oznaka: podatkovno polje vsebuje podatke, ki se podpišejo. Ker ni vključenega nobenega podatkovnega polja, se predpostavlja, da so podatki že na kartici (zgostitev datoteke) (hash of file).
Le	1	‘NNh’	Dolžina pričakovanega podpisa

TCS_131 **Sporočilo z odzivom**

Bajt	Dolžina	Vrednost	Opis
#1-#L	L	‘XX..XXh’	Podpis prej izračunane zgoščene vrednosti
SW	2	‘XXXXh’	Opis stanja (SW1, SW2)

— Če je ukaz uspešen, kartica vrne sporočilo ‘**9000**’.

— Če se šteje, da je implicitno izbrani zasebni ključ poškodovan, se vrne stanje obdelave ‘**6400**’ ali ‘**6581**’.

— Če zgoščena vrednost, izračunana v prejšnjem ukazu Perform Hash of File ni na voljo, se vrne stanje obdelave ‘**6985**’.

▼B

3.5.15 *PSO: VERIFY DIGITAL SIGNATURE*

Ta ukaz se uporablja za preverjanje digitalnega podpisa, ki je podan v vhodnih podatkih, katerih zgoščena vrednost je kartici znana. Kartica implicitno pozna algoritem podpisa.

Ta ukaz je v skladu s standardom ISO/IEC 7816-8. Uporaba ukaza pa je glede na s tem povezani standard omejena.

Le za nadzorno kartico se zahteva, da podpira ta ukaz v DF Tachograph in DF Tachograph_G2.

Druge vrste tahografskih kartic lahko izvedejo ta ukaz, lahko pa tudi ne. Ukaz je lahko dostopen v MF, lahko pa tudi ni.

TCS_132 Ukaz VERIFY DIGITAL SIGNATURE vedno uporablja javni ključ, izbran s predhodnim ukazom Manage Security Environment MSE: SET DST in prejšnja zgoščena vrednost, vnesena s PSO: ukaz HASH.

TCS_133 **Ukazno sporočilo**

Bajt	Dolžina	Vrednost	Opis
CLA	1	‘00h’	CLA
INS	1	‘2Ah’	Izvedba varnostne operacije
P1	1	‘00h’	
P2	1	‘A8h’	Oznaka: podatkovno polje vsebuje DO, pomembne za preverjanje
Lc	1	‘83h’	Dolžina Lc naslednjega podatkovnega polja
6	1	‘9Eh’	Oznaka za digitalni podpis
#7-#8	2	‘81 XXh’	Dolžina digitalnega podpisa: 128 bajtov, kodiranih v skladu z Delom A iz Dodatka 11 za tahografsko aplikacijo prve generacije. Odvisno od izbrane krivulje za tahografsko aplikacijo druge generacije (glej Del B iz Dodatka 11).
#9-#(8+L)	L	‘XX..XXh’	Vsebina digitalnega podpisa

TCS_134 **Sporočilo z odzivom**

Bajt	Dolžina	Vrednost	Opis
SW	2	‘XXXXh’	Opis stanja (SW1, SW2)

— Če je ukaz uspešen, kartica vrne sporočilo ‘**9000**’.

— Če preverjanje podpisa ni uspešno, se vrne stanje obdelave ‘**6688**’. Postopek preverjanja je opisan v Dodatku 11.

— Če ni izbran noben javni ključ, se vrne stanje obdelave ‘**6A88**’.

— Če nekateri pričakovani podatkovni objekti (predpisani zgoraj) manjkajo, se vrne stanje obdelave ‘**6987**’. To se lahko zgodi, če manjka katera od zahtevanih oznak.

▼B

— Če ni razpoložljive kode za obdelavo ukaza (zaradi predhodnega PSO: ukaz Hash), se vrne stanje obdelave ‘**6985**’.

— Če so nekateri podatkovni objekti nepravilni, se vrne stanje obdelave ‘**6988**’. To se lahko zgodi, če je nepravilna katera od dolžin zahtevanih podatkovnih objektov.

— Če se šteje, da je izbrani javni ključ poškodovan, se vrne stanje obdelave ‘**6400**’ ali ‘**6581**’.

3.5.16 *PROCESS DSRC MESSAGE*

Ta ukaz se uporablja za preverjanje celovitosti in avtentičnosti sporočila DSRC in dešifriranje podatkov, sporočenih iz VU nadzornemu organu ali servisni delavnici prek povezave DSRC. Kartica izdela ključ za šifriranje in ključ MAC, ki se uporabljata za zaščito sporočila DSRC, kot je opisano v poglavju 13 Dela B iz Dodatka 11.

Le za nadzorno kartico in kartico servisne delavnice se zahteva, da podpirata ta ukaz v DF Tachograph_G2.

Druge vrste tahografskih kartic lahko izvedejo ta ukaz ali pa tudi ne, vendar te kartice nimajo glavnega ključa DSRC. Zato te kartice ukaza ne morejo uspešno izvesti, ampak ga zaključijo z ustrezno kodo napake.

Ukaz je lahko dostopen v MF in / ali DF tahografu, lahko pa tudi ni. V tem primeru se ukaz zaključi z ustrezno kodo napake.

TCS_135 Glavni ključ DSRC je dostopen le v DF Tachograph_G2, tj. nadzorna kartica in kartica servisne delavnice podpirata uspešno izvedbo ukaza le v DF Tachograph_G2.

TCS_136 Ukaz le dešifrira podatke DSRC in preveri kriptografsko kontrolno vsoto, vendar ne interpretira vhodnih podatkov.

TCS_137 Zaporedje podatkovnih objektov v polju s podatki ukaza je določeno s to specifikacijo.

TCS_138 **Ukazno sporočilo**

Bajt	Dolžina	Vrednost	Opis
CLA	1	‘80h’	Lastniški CLA
INS	1	‘2Ah’	Izvedba varnostne operacije
P1	1	‘80h’	Podatki odziva: nešifrirana vrednost
P2	1	‘B0h’	Podatki ukaza: nešifrirana vrednost, kodirana v BER-TLV, vključno s SM DO
Lc	1	‘NNh’	Dolžina Lc naslednjega podatkovnega polja

▼B

Bajt	Dolžina	Vrednost	Opis
#6-#(5+L)	L	‘87h’ + L_{87} + ‘XX..XXh’	DER-TLV kodirani bajt indikatorja zapolnitve-vsebine, ki mu sledi kodirani prenos podatkov tahografa. Za bajt indikatorja zapolnitve-vsebine se uporablja vrednost ‘00h’ (‘brez dodatnih indikatorjev’ v skladu s standardom ISO/IEC 7816-4:2013, tabela 52.). Za mehanizem šifriranja glej poglavje 13 Dela B iz Dodatka 11. Dovoljene vrednosti za dolžino L_{87} so večkratniki bloka AES, povečani za 1 za bajt indikatorja zapolnitve-vsebine, tj. od 17 bajtov do vključno 193 bajtov. *Opomba:* glej ISO/IEC 7816-4:2013, tabela 49 za podatkovni objekt SM z oznako ‘87h’.
		‘81h’ + ‘10h’	DER-TLV kodirana nadzorna referenčna predloga za zaupnost, v kateri se združujejo naslednji podatkovni elementi (glej Dodatek 1 DSRCSecurityData in poglavje 13 Dela B iz Dodatka 11): — 4-bajtni časovni žig — 3-bajtni števec — 8-bajtna serijska številka VU — 1-bajtna različica DSRC glavnega ključa. *Opomba:* glej ISO/IEC 7816-4:2013, tabela 49 za podatkovni objekt SM z oznako ‘81h’.
		‘8Eh’ + L_{8E} + ‘XX..XXh’	DER-TLV kodiran MAC s sporočilom DSRC. Za MAC algoritem in izračun glej poglavje 13 Dela B iz Dodatka 11. *Opomba:* glej ISO/IEC 7816-4:2013, tabela 49 za podatkovni objekt SM z oznako ‘8Eh’.

TCS_139 **Sporočilo z odzivom**

Bajt	Dolžina	Vrednost	Opis
#1-#L	L	‘XX..XXh’	Odsotni (v primeru napake) ali dešifrirani podatki (odstranjena zapolnitev)
SW	2	‘XXXXh’	Opis stanja (SW1, SW2)

— Če je ukaz uspešen, kartica vrne sporočilo ‘**9000**’.

— ‘**6A80**’ označuje nepravilne parametre v polju s podatki ukaza (uporablja se tudi, kadar podatkovni objekti niso poslani v določenem zaporedju).

— ‘**6A88**’ označuje, da navedeni podatki niso na voljo, tj. navedeni glavni ključ DSRC ni na voljo.

— ‘**6900**’ označuje, da preverjanje kriptografske kontrolne vsote ali dešifriranje podatkov ni bilo uspešno.

4. STRUKTURA TAHOGRAFSKIH KARTIC

Ta odstavek določa strukture datotek tahografskih kartic za hrambo dosegljivih podatkov.

▼B

Ne določa notranjih struktur, ki so odvisne od proizvajalcev kartic, kot so npr. glave datotek, niti shranjevanja in obdelave podatkovnih elementov, potrebnih le za interno rabo, npr. `EuropeanPublicKey`, `CardPrivateKey`, `TdesSessionKey` or `WorkshopCardPin`.

TCS_140 Tahografska kartica druge generacije gosti glavno datoteko MF in enakovrstno tahografsko aplikacijo prve in druge generacije (npr. aplikacije vozniških kartic).

TCS_141 Tahografska kartica podpira najmanj najmanjše število zapisov, določenih za ustrezajoče aplikacije, in ne podpira več zapisov, kot je največje število zapisov, določeno za ustrezajoče aplikacije.

Največje in najmanjše število zapisov je določeno v tem poglavju za različne aplikacije.

Za varnostne pogoje, ki se uporabljajo v pravilih dostopa v tem poglavju, glej poglavje 3.3. Na splošno način dostopa „read“ označuje ukaz READ BINARY s sodim bajtom INS in lihim, če je le-ta podprt, z izjemo EF Sensor_Installation_Data na kartici servisne delavnice, glej TCS_156 in TCS_160. Način dostopa „update“ označuje ukaz Update Binary s sodim bajtom INS in lihim, če je le-ta podprt, način dostopa „select“ pa ukaz SELECT.

4.1. Glavna datoteka MF

TCS_142 Po personalizaciji ima glavna datoteka naslednjo strukturo trajnih datotek in naslednja pravila dostopa do datotek:

Opomba: kratki identifikator SFID je podan kot decimalno število, tj. vrednost 30 ustreza vrednosti 11110 v binarnem zapisu.

			Pravila dostopa	
Datoteka	**ID datoteke**	**SFID**	**Read / Select**	**Posodobitev**
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	

V tej tabeli se za varnostni pogoj uporablja naslednja kratica:

SC1 ALW OR SM-MAC-G2

TCS_143 Vse strukture EF so transparentne.

TCS_144 Glavna datoteka MF ima naslednjo podatkovno strukturo:

▼B

Datoteka/podatkovni element	Št. zapisov	Velikost (v bajtih) Min.	Maks.	Privzete vrednosti
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 Elementarna datoteka EF DIR vsebuje naslednje podatkovne objekte, povezane z aplikacijo: ‘61 08 4F 06 FF 54 41 43 48 4F 61 08 4F 06 FF 53 4D 52 44 54’.

TCS_146 Elementarna datoteka EF ATR/INFO je prisotna, če tahografska kartica v svojem ATR označuje, da podpira podaljšana podatkovna polja. V tem primeru EF ATR/INFO vsebuje podatkovni objekt z informacijami o podaljšanju (DO‘7F66’), kot je določen v klavzuli 12.7.1. iz standarda ISO/IEC 7816-4:2013.

TCS_147 Elementarna datoteka EF Extended_length je prisotna, če tahografska kartica v svojem ATR označuje, da podpira podaljšana podatkovna polja. V tem primeru EF vsebuje naslednji podatkovni objekt ‘02 01 xx’, kjer vrednost ‘xx’ označuje, ali so podaljšana podatkovna polja podprta za protokol T = 1 in / ali T = 0.

Vrednost ‘01’ označuje, da so podaljšana podatkovna polja podprta za protokol T = 1.

Vrednost ‘10’ označuje, da so podaljšana podatkovna polja podprta za protokol T = 0.

Vrednost ‘11’ označuje, da so podaljšana podatkovna polja podprta za protokol T = 1 in T = 0.

4.2. Aplikacije vozniške kartice

4.2.1 *Aplikacija vozniške kartice prve generacije*

TCS_148 Po personalizaciji ima vozniška kartica prve generacije naslednjo strukturo trajnih datotek in naslednja pravila dostopa do datotek:

		Pravila dostopa		
Datoteka	ID datoteke	Branje	Select	Posodobitev
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

Za varnostne pogoje se v tej tabeli uporabljajo naslednje kratice:

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 Vse strukture EF so transparentne.

TCS_150 Aplikacija vozniške kartice prve generacije ima naslednjo podatkovno strukturo:

Datoteka/podatkovni element	Št. zapisov	Velikost (v bajtih) Min.	Maks.	Privzete vrednosti
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 Naslednje vrednosti, s katerimi so podane velikosti v zgornji tabeli, so najmanjše in največje vrednosti števil zapisov, ki jih mora uporabljati podatkovna struktura vozniške kartice za aplikacijo prve generacije:

		Min.	Maks.
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 bajti (28 dni * 93 sprememb dejavnosti)	13 776 bajtov (28 dni * 240 sprememb dejavnosti)

4.2.2 *Aplikacija vozniške kartice druge generacije*

TCS_152 Po personalizaciji ima vozniška kartica druge generacije naslednjo strukturo trajnih datotek in naslednja pravila dostopa do datotek.

Opomba: kratki identifikator SFID je podan kot decimalno število, tj. vrednost 30 ustreza vrednosti 11110 v binarnem zapisu.

			Pravila dostopa	
Datoteka	**ID datoteke**	**SFID**	**Read / Select**	**Posodobitev**
└─ 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

V tej tabeli se za varnostni pogoj uporablja naslednja kratica:

SC1 ALW OR SM-MAC-G2.

TCS_153 Vse strukture EF so transparentne.

TCS_154 Aplikacija vozniške kartice druge generacije ima naslednjo podatkovno strukturo:

▼B

Datoteka/podatkovni element	Št. zapisov	Velikost (v bajtih) Min.	Maks.	Privzete vrednosti
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 Naslednje vrednosti, s katerimi so podane velikosti v zgornji tabeli, so najmanjše in največje vrednosti števil zapisov, ki jih mora uporabljati podatkovna struktura vozniške kartice za aplikacijo druge generacije:

		Min	**Maks.**
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 bajti (28 dni * 93 sprememb dejavnosti)	13 776 bajtov (28 dni * 240 sprememb dejavnosti)
n_7	NoOfCardVehicleUnitRecords	84	200
n_8	NoOfGNSSCDRecords	252	336
n_9	NoOfSpecificConditionRecords	56	112

4.3. **Aplikacije kartice servisne delavnice**

4.3.1 *Aplikacija kartice servisne delavnice prve generacije*

TCS_156 Po personalizaciji ima kartica servisne delavnice prve generacije naslednjo strukturo trajnih datotek in naslednja pravila dostopa do datotek:

▼B

Datoteka	ID datoteke	Pravila dostopa		
		Branje	Select	Posodobitev
└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

Za varnostne pogoje se v tej tabeli uporabljajo naslednje kratice:

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 Za ukaz READ BINARY s sodim bajtom INS:

(PLAIN-C AND SM-R-ENC-G1) ALI (SM-C-MAC-G1 AND SM-R-ENC-MAC-G1) ALI

(SM-C-MAC-G2 IN SM-R-ENC-MAC-G2)

Za ukaz READ BINARY z lihim bajtom INS: NEV

TCS_157 Vse strukture EF so transparentne.

TCS_158 Kartica servisne delavnice ima naslednjo podatkovno strukturo:

▼B

Datoteka/podatkovni element	Št. zapisov	Velikost (v bajtih) Min.	Maks.	Privzete vrednosti
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		*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 Naslednje vrednosti, s katerimi so podane velikosti v zgornji tabeli, so najmanjše in največje vrednosti števil zapisov, ki jih mora uporabljati podatkovna struktura kartice servisne delavnice za aplikacijo prve generacije:

		Min.	Maks.
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 bajtov (1 dan* 93 sprememb dejavnosti)	492 bajtov (1 dan* 240 sprememb dejavnosti)

4.3.2 *Aplikacija kartice servisne delavnice druge generacije*

TCS_160 Po personalizaciji ima kartica servisne delavnice druge generacije naslednjo strukturo trajnih datotek in naslednja pravila dostopa do datotek:

Opomba: kratki identifikator SFID je podan kot decimalno število, tj. vrednost 30 ustreza vrednosti 11110 v binarnem zapisu.

			Pravila dostopa		
Datoteka	**ID datoteke**	**SFID**	**Branje**	**Select**	**Posodobitev**
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

Za varnostne pogoje se v tej tabeli uporabljajo naslednje kratice:

SC1 ALW OR SM-MAC-G2

SC5 Za ukaz READ BINARY s sodim bajtom INS: SM-C-MAC-G2 IN SM-R-ENC-MAC-G2

Za ukaz READ BINARY z lihim bajtom INS: NEV

TCS_161 Vse strukture EF so transparentne.

TCS_162 Kartica servisne delavnice druge generacije ima naslednjo podatkovno strukturo:

Datoteka/podatkovni element	Št. zapisov	Velikost (v bajtih) Min.	Maks.	Privzete vrednosti
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 Naslednje vrednosti, s katerimi so podane velikosti v zgornji tabeli, so najmanjše in največje vrednosti števil zapisov, ki jih mora uporabljati podatkovna struktura vozniške kartice za aplikacijo druge generacije:

		Min.	Maks.
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 bajtov (1 dan* 93 sprememb dejavnosti)	492 bajtov (1 dan* 240 sprememb dejavnosti)
n_7	NoOfCardVehicleUnitRecords	4	8
n_8	NoOfGNSSCDRecords	18	24
n_9	NoOfSpecificConditionRecords	2	4

4.4. Aplikacije nadzorne kartice

4.4.1 *Aplikacija nadzorne kartice prve generacije*

TCS_164 Po personalizaciji ima nadzorna kartica prve generacije naslednjo strukturo trajnih datotek in naslednja pravila dostopa do datotek:

		Pravila dostopa		
Datoteka	**ID datoteke**	**Branje**	**Select**	**Posodobitev**
└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

Za varnostne pogoje se v tej tabeli uporabljajo naslednje kratice:

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 Vse strukture EF so transparentne.

TCS_166 Aplikacija nadzorne kartice prve generacije ima naslednjo podatkovno strukturo:

▼B

Datoteka/podatkovni element	Št. zapisov	Velikost (v bajtih) Min.	Maks.	
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 Naslednje vrednosti, s katerimi so podane velikosti v zgornji tabeli, so najmanjše in največje vrednosti števil zapisov, ki jih mora uporabljati podatkovna struktura nadzorne kartice za aplikacijo prve generacije:

		Min.	Maks.
n_7	NoOfControlActivityRecords	230	520

4.4.2 *Aplikacija nadzorne kartice druge generacije*

TCS_168 Po personalizaciji ima nadzorna kartica druge generacije naslednjo strukturo trajnih datotek in naslednja pravila dostopa do datotek:

Opomba: kratki identifikator SFID je podan kot decimalno število, tj. vrednost 30 ustreza vrednosti 11110 v binarnem zapisu.

▼B

			Pravila dostopa	
Datoteka	**ID datoteke**	**SFID**	**Read / Select**	**Posodobitev**
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

V tej tabeli se za varnostni pogoj uporablja naslednja kratica:

SC1 ALW OR SM-MAC-G2.

TCS_169 Vse strukture EF so transparentne.

TCS_170 Aplikacija nadzorne kartice druge generacije ima naslednjo podatkovno strukturo:

Datoteka/podatkovni element	**Št. zapisov**	**Velikost (v bajtih) Min.**	**Maks.**	
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 Naslednje vrednosti, s katerimi so podane velikosti v zgornji tabeli, so najmanjše in največje vrednosti števil zapisov, ki jih mora uporabljati podatkovna struktura vozniške kartice za aplikacijo druge generacije:

▼B

		Min.	Maks.
n_7	NoOfControlActivityRecords	230	520

4.5. **Aplikacije kartice podjetja**

4.5.1 *Aplikacija kartice podjetja prve generacije*

TCS_172 Po personalizaciji ima kartica podjetja prve generacije naslednjo strukturo trajnih datotek in naslednja pravila dostopa do datotek.

		Pravila dostopa		
Datoteka	**ID datoteke**	**Branje**	**Select**	**Posodobitev**
└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

Za varnostne pogoje se v tej tabeli uporabljajo naslednje kratice:

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 Vse strukture EF so transparentne.

TCS_174 Aplikacija kartice podjetja prve generacije ima naslednjo podatkovno strukturo:

Datoteka/podatkovni element	**Št. zapisov**	**Velikost (v bajtih) Min.**	**Maks.**	**Privzete vrednosti**
└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 Naslednje vrednosti, s katerimi so podane velikosti v zgornji tabeli, so najmanjše in največje vrednosti števil zapisov, ki jih mora uporabljati podatkovna struktura kartice podjetja za aplikacijo prve generacije:

		Min.	Maks.
n_8	NoOfCompanyActivityRecords	230	520

4.5.2 *Aplikacija kartice podjetja druge generacije*

TCS_176 Po personalizaciji ima kartica podjetja druge generacije naslednjo strukturo trajnih datotek in naslednja pravila dostopa do datotek.

Opomba: kratki identifikator SFID je podan kot decimalno število, tj. vrednost 30 ustreza vrednosti 11110 v binarnem zapisu.

			Pravila dostopa	
Datoteka	**ID datoteke**	**SFID**	**Read / Select**	**Posodobitev**
└─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

V tej tabeli se za varnostni pogoj uporablja naslednja kratica:

SC1 ALW OR SM-MAC-G2

TCS_177 Vse strukture EF so transparentne.

TCS_178 Kartica podjetja druge generacije ima naslednjo podatkovno strukturo:

Datoteka/podatkovni element	**Št. zapisov**	**Velikost (v bajtih) Min.**	**Maks.**	**Privzete vrednosti**
└─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 Naslednje vrednosti, s katerimi so podane velikosti v zgornji tabeli, so najmanjše in največje vrednosti števil zapisov, ki jih mora uporabljati podatkovna struktura kartice podjetja za aplikacijo druge generacije:

		Min.	Maks.
n_8	NoOfCompanyActivityRecords	230	520

▼B

Dodatek 3

PIKTOGRAMI

PIC_001 Tahograf lahko neobvezno uporablja naslednje piktograme in kombinacije piktogramov (ali piktograme in kombinacije piktogramov, ki so si dovolj podobni, da se jih lahko nedvoumno prepozna):

1. OSNOVNI PIKTOGRAMI

	Ljudje	**Ukrepi**	**Načini delovanja**
	Podjetje		Način dela v podjetju
	Nadzornik	Nadzor	Nadzorni način
	Voznik	Vožnja	Delovni način
	Servisna delavnica / postaja za preskušanje	Pregled/kalibracija	Način kalibracije
	Proizvajalec		

	Dejavnosti	**Trajanje**
	Na voljo	Tekoče obdobje razpoložljivosti
	Vožnja	Čas neprekinjene vožnje
	Počitek	Tekoče obdobje počitka
	Drugo delo	Tekoča delovna izmena
	Odmor	Skupni čas odmorov
	Neznano	

	Oprema	**Funkcije**
	Voznikova reža	
	Sovoznikova reža	
	Kartica	
	Ura	
	Prikazovalnik	Prikazovanje
	Zunanji pomnilnik	Prenos podatkov
	Napajanje	
	Tiskalnik/izpis	Tiskanje
	Tipalo	
	Velikost pnevmatik	
	Vozilo/enota v vozilu	
	GNSS oprema	
	Oprema za odkrivanje na daljavo	
	Vmesnik ITS	

▼B

	Posebni pogoji
OUT	Zunaj področja uporabe
	Prevoz s trajektom/vlakom

	Razno		
!	Dogodki		Napake
	Začetek dnevne delovne izmene		Konec dnevne delovne izmene
	Lokacija		
M	Ročni vnos voznikovih dejavnosti		
	Varnost		
	Hitrost		
	Čas		
Σ	Skupno / vsota		

	Kvalifikatorji
24h	Dnevno
I	Tedensko
II	Dvotedensko
	Od do

2. KOMBINACIJE PIKTOGRAMOV

	Razno		
	Lokacija nadzora		
	Lokacija začetka dnevne delovne izmene		Lokacija konca dnevne delovne izmene
	Od časa		Do časa
	Od vozila		
OUT	Začetek stanja zunaj področja uporabe	OUT	Konec stanja zunaj področja uporabe

	Kartice
	Vozniška kartica
	Kartica podjetja
	Nadzorna kartica
	Kartica servisne delavnice
– – –	Ni kartice

	Vožnja
	Vožnja s posadko
I	Čas vožnje v enem tednu
II	Čas vožnje v dveh tednih

▼B

	Izpisi
24h	Dnevni izpis voznikovih dejavnosti s kartice
24h	Dnevni izpis voznikovih dejavnosti iz VU
	Izpis dogodkov in napak s kartice
	Izpis dogodkov in napak iz VU
	Izpis tehničnih podatkov
	Izpis prekoračitev hitrosti
	Dogodki
	Vstavitev neveljavne kartice
	Navzkrižje med karticami
	Časovno prekrivanje
	Vožnja brez ustrezne kartice
	Vstavitev kartice med vožnjo
	Zadnja seja s kartico nepravilno zaključena
	Prekoračitev hitrosti
	Izpad napajanja
	Napaka v podatkih o gibanju
	Navzkrižje v gibanju vozila
	Kršenje varnosti
	Nastavljanje časa (s strani servisne delavnice)
	Nadzor prekoračitev hitrosti
	Napake
1	Napaka kartice (voznikova reža)
2	Napaka kartice (sovoznikova reža)
	Napaka na prikazovalniku
	Napaka pri prenosu podatkov
	Napaka na tiskalniku
	Napaka na tipalu
	Notranja napaka VU
	Napaka GNSS
	Napaka pri odkrivanju na daljavo
	Postopek ročnega vnosa
	Še vedno ista dnevna delovna izmena?
	Konec prejšnje delovne izmene?
	Potrdite ali vnesite lokacijo konca delovne izmene.
	Vnesite čas začetka.
	Vnesite lokacijo začetka delovne izmene.

Opomba: dodatne kombinacije piktogramov za oblikovanje blokov izpisa ali identifikatorjev zapisov so opredeljene v Dodatku 4.

▼B

Dodatek 4

IZPISI

KAZALO

1. SPLOŠNO

2. SPECIFIKACIJA BLOKOV PODATKOV

3. SPECIFIKACIJE IZPISOV

3.1. Dnevni izpis vozniških dejavnosti s kartice

3.2. Dnevni izpis voznikovih dejavnosti iz VU

3.3. Izpis dogodkov in napak s kartice

3.4. Izpis dogodkov in napak iz VU

3.5. Izpis tehničnih podatkov

3.6. Izpis prekoračitev hitrosti

3.7. Zgodovina vstavljenih kartic

1. SPLOŠNO

Vsak izpis sestavlja zaporedje različnih podatkovnih blokov, ki jih lahko označuje identifikator bloka.

Podatkovni blok vsebuje enega ali več zapisov, ki jih lahko označuje identifikator zapisa.

PRT_001 Kadar je tik pred identifikatorjem zapisa identifikator bloka, se identifikator zapisa ne natisne.

PRT_002 Če določen podatek ni znan ali se ga ne sme natisniti zaradi omejitev pravic dostopa do podatkov, se namesto podatka natisnejo presledki.

PRT_003 Če vsebina celotne vrstice ni znana ali je ni treba natisniti, se tiskanje celotne vrstice opusti.

PRT_004 Numerični podatki se tiskajo desno poravnano, s presledki, ki ločujejo tisočice in milijone, in brez vodilnih ničel.

PRT_005 Nizi znakov se tiskajo levo poravnano in so po potrebi zapolnjeni s presledki, da dosežejo zahtevano dolžino, ali odrezani iz istega razloga (pri imenih in naslovih).

PRT_006 Če je zaradi dolžine besedila potreben prelom vrstice, bi se morala nova natisnjena vrstica začeti s posebnim znakom (pika na srednji višini „•“).

2. SPECIFIKACIJA BLOKOV PODATKOV

V tem poglavju se uporabljajo naslednji dogovori o zapisu formatov:

— **krepko** natisnjeni znaki označujejo golo besedilo, ki se natisne (v natisu je prikaz znakov normalen),

▼B

— normalni znaki označujejo spremenljivke (piktograme ali podatke), ki se jih pri tiskanju nadomesti z njihovimi vrednostmi,

— imenom spremenljivk so dodani podčrtaji, ki prikažejo dolžino, ki je na voljo za spremenljivko,

— datumi so prikazani v formatu „dd/mm/llll“ (dan, mesec, leto). Lahko se uporablja tudi format „dd.mm.llll“,

— Izraz „identifikacija kartice“ pomeni sestav naslednjih podatkov: tip kartice, prikazan s kombinacijo piktogramov, kodo države izdajateljice kartice, poševnico in številko kartice, zaporedno številko zamenjave in podaljšanja kartice, ki sta ločeni s presledkom:

P	■	x	x	x	/	x	x	x	x	x	x	x	x	x	x	x	x	x		x		x
Kombinacija piktogramov		Koda države članice izdajateljice				Prvih 14 znakov številke kartice (ki lahko vključujejo zaporedno številko)														Zaporedna številka zamenjave		Zaporedna številka podaljšanja

▼B

PRT_007 Izpisi so v skladu z naslednjimi pomeni in formati sestavljeni iz naslednjih podatkovnih blokov in/ali zapisov podatkov:

Številka bloka ali zapisa Pomen	Data Format
1 ***Datum in čas tiskanja dokumenta***	▼ dd/mm/yyyy hh:mm **(UTC)**
2 ***Vrsta izpisa*** Identifikator bloka Kombinacija piktogramov izpisa (glej dodatek 3), nastavitev naprave za omejevanje hitrosti (samo pri izpisu prekoračitev hitrosti)	----------▼---------- Picto xxx **km/h**
3 ***Identifikacija imetnika kartice.*** Identifikator bloka. P= people pictogram Priimek imetnika kartice Ime(na) imetnika kartice (če je relevantno) Identifikacija kartice Datum izteka veljavnosti vozniške kartice (če je relevantno) in številka generacije (GEN 1 ali GEN 2) (*)	----------P---------- P Last_Name_____ First_Name_____ Card_Identification_____ dd/mm/yyyy - GEN 2

Če kartica ni osebna in ne vsebuje priimka imetnika kartice, se namesto tega natisne ime podjetja ali servisne delavnice ali nadzornega organa.

(*) Številka generacije kartice se lahko natisne le s pametnim tahografom.

4 ***Identifikacija vozila.*** Identifikator bloka VIN Država članica, v kateri je vozilo registrirano in VRN	----------🚙---------- 🚙 VIN_____ Nat/VRN_____
5 ***Identifikacija enote vozila.*** Identifikator bloka Ime proizvajalca enote vozila (VU) Kataloška številka VU Številka generacije VU (*)	----------⊟---------- ⊟ VU_Manufacturer_____ VU_Kataloška_številka__ GEN 2

(*) Številka generacije kartice se lahko natisne le s pametnim tahografom.

6 ***Zadnja kalibracija tahografa*** Identifikator bloka Ime servisne delavnice Identifikacija kartice servisne delavnice Datum kalibracije	----------🔧---------- 🔧 Last_Name_____ Card_Identification_____ 🔧 dd/mm/yyyy

▼B

7 ***Zadnji nadzor (s strani inšpektorja)***

Identifikator bloka

Identifikacija nadzornikove kartice

Datum, čas in vrsta nadzora

```
----------▫----------
Card_Identification_____
▫ dd/mm/yyyy hh:mm ppppp
```

Vrsta nadzora: kombinacija, ki jo sestavlja največ pet piktogramov. Vrsta nadzora je lahko ena od naslednjih (ali kombinacija večih): ▪: prenos podatkov s kartice, ↧: prenos podatkov z VU, ▼: tiskanje, □: prikaz, ⊤: cestno preverjanje kalibracije

8 ***Voznikove dejavnosti, shranjene na kartici v časovnem zaporedju***

Identifikator bloka

Datum, za katerega se zahteva izpis (koledarski dan) + števec dnevne prisotnosti kartice

```
----------⊙----------
    dd/mm/yyyy  xxx
```

8a *Stanje zunaj področja uporabe na začetku danega dne* (pustite prazno, če ni odprtega stanja zunaj področja uporabe)

```
----------OUT-----------
```

8.1 *Obdobje, v katerem kartica ni bila vstavljena*

8,1 a Identifikator zapisa (začetek obdobja)

8.1b *Neznano obdobje* Čas začetka, trajanje

8.1c *Ročno vnesena dejavnost*.

Piktogram dejavnosti, čas začetka, trajanje.

```
  --------------------
?       hh:mm hhhmm
A       hh:mm hhhmm
```

8.2 *Vstavitev kartice v režo S*

Identifikator zapisa; S = piktogram reže

Država članica, v kateri je vozilo registrirano in VRN

Stanje števca prevožene poti ob vstavitvi kartice

```
  ---------S---------
▲ Nat/VRN___________
  x xxx xxx km
```

8.3 *Dejavnost (v času vstavljene kartice)*

Piktogram dejavnosti, čas začetka, trajanje, stanje posadke (piktogram posadke, če je stanje POSADKA, prazno, če je stanje POSAMEZNIK)

```
A       hh:mm hhhmm ⊙⊙
```

8,3 a *Posebno stanje* Čas vnosa, piktogram posebnega stanja (ali kombinacija piktogramov).

```
        hh:mm ---pppp---
```

8.4 *Izvlek kartice*

Stanje števca prevožene poti in razdalja, prevožena od zadnje vstavitve, za katero je znano stanje števca prevožene poti.

```
  x xxx xxx km; x xxx km
```

9 ***Voznikove dejavnosti, shranjene v VU po režah v časovnem zaporedju***

Identifikator bloka

Datum, za katerega se zahteva izpis (koledarski dan)

Stanje števca prevožene poti ob 00:00 in 24:00

```
----------⊙----------
       dd/mm/yyyy
x xxx xxx - x xxx xxx km
```

10 ***Dejavnosti, opravljene s kartico v reži S***

Identifikator bloka

10 a *Stanje zunaj področja uporabe na začetku danega dne* (pustite prazno, če ni odprtega stanja zunaj področja uporabe)

```
----------S----------
----------OUT-----------
```

10.1 *Obdobje, v katerem v reži S ni bilo vstavljene kartice*

Identifikator zapisa

Ni vstavljene kartice

Stanje števca prevožene poti ob začetku obdobja

```
  --------------------
⊙▪---
  x xxx xxx km
```

10.2 *Vstavitev kartice*

Identifikator zapisa vstavitve kartice

Priimek voznika

```
  --------------------
⊙ Last_Name_____________
```

▼B

	Osebno ime voznika	First_Name_____
	Identifikacija vozniške kartice	Card_Identification_____
	Datum izteka veljavnosti vozniške kartice (če je relevantno) in številka generacije (GEN 1 ali GEN 2) (*)	dd/mm/yyyy - GEN 2
	Država članica, v kateri je vozilo registrirano in registracijska številka prejšnjega vozila	Nat/VRN_____
	Datum in čas izvleka kartice iz prejšnjega vozila	dd/mm/yyyy hh:mm
	Prazna vrstica	
	Stanje števca prevožene poti ob vstavitvi kartice, zastavica ročnega vnosa voznikovih dejavnosti (M: da, prazno: ne)	x xxx xxx **km** M
	Če na dan, za katerega se izdela izpis, ni bila vstavljena vozniška kartica, se za blok 10.2 odčitajo podatki stanja števca prevožene poti iz zadnje razpoložljive vstavitve kartice pred danim dnem.	
10.3	*Dejavnost*	
	Piktogram dejavnosti, čas začetka, trajanje, stanje posadke (piktogram posadke, če je stanje POSADKA, prazno, če je stanje POSAMEZNIK)	A hh:mm hh**h**mm ⊙⊙
10,3 a	*Posebno stanje* Čas vnosa, piktogram posebnega stanja (ali kombinacija piktogramov).	hh:mm ---pppp---
10.4	*Izvlek kartice ali konec stanja „brez kartice“*	
	Stanje števca prevožene poti ob izvleku kartice ali koncu obdobja „brez kartice“ in razdalja, prevožena od vstavitve ali od začetka obdobja „brez kartice“.	x xxx xxx **km**; x xxx **km**

(*) Številka generacije kartice se lahko natisne le s pametnim tahografom.

11	***Dnevni povzetek***	
	Identifikator bloka	----------Σ----------
11.1	***Povzetek obdobij VU brez kartice v voznikovi reži***	
	Identifikator bloka	1⊙▬---
11.2	***Povzetek obdobij VU brez kartice v sovoznikovi reži***	
	Identifikator bloka	2⊙▬---
11.3	***Dnevni povzetek VU za posameznega voznika***	
	Identifikator zapisa	----------
	Priimek voznika	⊙ Last_Name_____
	Osebno(-a) ime(-na) voznika	First_Name_____
	Identifikacija vozniške kartice	Card_Identification_____
11.4	*Vnos kraja, v katerem se dnevna delovna izmena začne in/ali konča*	
	pi= piktogram kraja začetka/konca, čas, država, regija,	pihh:mm Cou Reg
	Števec prevožene poti	x xxx xxx **km**
11.5	*Vnos kraja, v katerem se dnevna delovna izmena začne in/ali konča*	
	in po 3 urah časa neprekinjene vožnje	hh:mm
	Števec prevožene poti	x xxx xxx **km**

11.6	*Skupne vrednosti po dejavnostih (s kartice)*	
	Skupni čas vožnje, prevožena pot	⊙ hh**h**mm x xxx **km**
	Skupno trajanje dela in razpoložljivosti	✱ hh**h**mm ⧈ hh**h**mm
	Skupno trajanje počitka in neznanih dejavnosti	⊢ hh**h**mm ? hh**h**mm
	Skupno trajanje dejavnosti posadke	⊙⊙ hh**h**mm
11.7	*Skupne vrednosti po dejavnostih (obdobja brez kartice v voznikovi reži)*	
	Skupni čas vožnje, prevožena pot	⊙ hh**h**mm x xxx **km**
	Skupno trajanje dela in razpoložljivosti	✱ hh**h**mm ⧈ hh**h**mm
	Skupno trajanje počitka	⊢ hh**h**mm

▼B

11.8	*Skupne vrednosti po dejavnostih (obdobja brez kartice v sovoznikovi reži)*	
	Skupno trajanje dela in razpoložljivosti	⚒ hh**h**mm ⧈ hh**h**mm
	Skupno trajanje počitka	⊢ hh**h**mm
11.9	*Skupne vrednosti po dejavnostih (za vsakega voznika, upoštevani sta obe reži)*	
	Skupni čas vožnje, prevožena pot	⊙ hh**h**mm x xxx **km**
	Skupno trajanje dela in razpoložljivosti	⚒ hh**h**mm ⧈ hh**h**mm
	Skupno trajanje počitka	⊢ hh**h**mm
	Skupno trajanje dejavnosti posadke	⊙⊙ hh**h**mm

Kadar se za trenutni dan zahteva dnevni izpis, se dnevni povzetek izračuna iz podatkov, ki so na voljo ob času izpisa.

12	***Dogodki in/ali napake, shranjeni na kartici***	
12.1	Identifikator bloka zadnjih 5 „dogodkov in napak“ s kartice	----------!×▪----------
12.2	Identifikator bloka vseh zapisanih „dogodkov“ na kartici	----------!▪----------
12.3	Identifikator bloka vseh zapisanih „napak“ na kartici	----------×▪----------
12.4	*Zapis dogodka in/ali napake*	
	Identifikator zapisa Piktogram dogodka/napake, namen zapisa, datum in čas začetka Koda dodatnega dogodka/napake (če obstaja), trajanje Država članica, v kateri je registrirano vozilo, pri katerem se je dogodek ali napaka zgodil, in registracijska številka tega vozila.	---------- Pic (p) dd/mm/yyyy hh:mm !xx hh**h**mm 🚩 Nat/VRN_____

13	***Dogodki in/ali napake, ki so v enoti v vozilu (VU) shranjeni ali v teku***	
13.1	Identifikator bloka zadnjih 5 „dogodkov in napak“ iz VU	----------!×🚩----------
13.2	Identifikator bloka vseh zapisanih ali tekočih „dogodkov“ v VU	----------!🚩----------
13.3	Identifikator bloka vseh zapisanih ali tekočih „napak“ v VU	----------×🚩----------
13.4	*Zapis dogodka in/ali napake*	
	Identifikator zapisa Piktogram dogodka/napake, namen zapisa, datum in čas začetka Koda dodatnega dogodka/napake (če je relevantno), število podobnih dogodkov istega dne, trajanje Identifikacija kartic, vstavljenih ob začetku ali ob koncu dogodka ali napake (do 4 vrstice, brez ponavljanja istih številk kartic) Primer, ko ni bilo vstavljene kartice. Podatki, ki jih določi proizvajalec	---------- Pic (p) dd/mm/yyyy hh:mm !xx (xxx) hh**h**mm Card_Identification_____ Card_Identification_____ Card_Identification_____ Card_Identification_____ ▪--- < Literal><ErrorCode>

Namen zapisa (p) je numerična koda, ki pojasnjuje, zakaj je bil zapisan dogodek ali napaka; kodiran v skladu s podatkovnim elementom `EventFaultRecordPurpose`.

`Literal` je posebno besedilo, ki ga določi proizvajalec tahografa, z dolžino največ 12 znakov.

The `ErrorCode` je posebna koda napake, ki jo določi proizvajalec tahografa, z dolžino največ 12 znakov.

▼B

14	***Identifikacija VU***	
	Identifikator bloka	----------B----------
	Ime proizvajalca enote vozila (VU)	B Name_____
	Naslov proizvajalca VU	Address_____
	Kataloška številka VU	PartNumber_____
	Homologacijska številka VU	Apprv_____
	Serijska številka VU	S/N_____
	Leto izdelave VU	yyyy
	Verzija in datum namestitve programske opreme VU	V xxxx dd/mm/yyyy
15	***Identifikacija tipala***	
	Identifikator bloka	----------Л----------
15.1	*Povezovanje zapisov*	
	Serijska številka tipala	Л S/N_____
	Homologacijska številka tipala	Apprv_____
	Datum povezave tipala	dd/mm/yyyy hh:mm
16	***Identifikacija GNSS***	
	Identifikator bloka	----------▚----------
16.1	*Zapis povezovanja*	
	Serijska številka zunanje GNSS opreme	▚ S/N_____
	Homologacijska številka zunanje GNSS opreme	Apprv_____
	Datum povezave zunanje GNSS opreme	dd/mm/yyyy hh:mm
17	***Podatki o kalibraciji***	
	Identifikator bloka	----------T----------
17.1	*Zapis o kalibraciji*	
	Identifikator zapisa	----------
	Servisna delavnica, ki je opravila kalibriranje	T Workshop_name_____
	Naslov servisne delavnice	Workshop_address_____
	Identifikacija kartice servisne delavnice	Card_Identification_____
	Datum izteka veljavnosti kartice servisne delavnice	dd/mm/yyyy
	Prazna vrstica	
	Datum kalibracije + namen kalibracije	T dd/mm/yyyy (p)
	VIN	A VIN_____
	Država članica, v kateri je vozilo registrirano, in registrska številka vozila	Nat/VRN_____
	Značilni koeficient vozila	w xx xxx Imp/km
	Konstanta zapisovalne naprave	k xx xxx Imp/km
	Effective circumference of wheel tyres	l xx xxx mm
	Velikost nameščenih pnevmatik	● TyreSize_____
	Nastavitev naprave za omejevanje hitrosti	> xxx km/h
	Staro in novo stanje števca prevožene poti	x xxx xxx – x xxx xxx km

Namen kalibracije (p) je numerična koda, ki pojasnjuje, zakaj so bili ti kalibracijski parametri zapisani; kodirana je v skladu s podatkovnim elementom `CalibrationPurpose`.

▼B

18	***Nastavljanje časa***	
	Identifikator bloka	----------◷----------
18.1	*Zapis nastavljanja časa*	
	Identifikator zapisa	----------
	Stari datum in čas	!◷ dd/mm/yyyy hh:mm
	Novi datum in čas	◷ dd/mm/yyyy hh:mm
	Servisna delavnica, ki je opravila nastavljanje časa	Workshop_name_____
	Naslov servisne delavnice	Workshop_address_____
	Identifikacija kartice servisne delavnice	Card_Identification_____
	Datum izteka veljavnosti kartice servisne delavnice	dd/mm/yyyy
19	***Najnovejši dogodek in napaka, zapisana v enoti vozila***	
	Identifikator bloka	----------!×A----------
	Datum in čas najnovejšega dogodka	! dd/mm/yyyy hh:mm
	Datum in čas najnovejše napake	× dd/mm/yyyy hh:mm
20	***Informacije o nadzoru prekoračitev hitrosti***	
	Identifikator bloka	----------»»----------
	Datum in čas zadnjega NADZORA PREKORAČITVE HITROSTI	»▫dd/mm/yyyy hh:mm
	Datum/čas prve prekoračitve hitrosti in število takih dogodkov od takrat	»»dd/mm/yyyy hh:mm (nnn)
21	***Zapis prekoračitve hitrosti***	
21.1	Identifikator bloka „prva prekoračitev hitrosti po zadnji kalibraciji“	--------»»T---------
21.2	Identifikator bloka „5 najresnejših prekoračitev hitrosti v zadnjih 365 dneh“	-------»»(365)------
21.3	Identifikator bloka „najresnejša prekoračitev hitrosti za vsakega od 10 zadnjih dni nastopov“	-------»»(10)-------
21.4	Identifikator zapisa	----------
	Datum, čas in trajanje	»»dd/mm/yyyy hh:mm hhhmm
	Največja in povprečna hitrost, število podobnih dogodkov v danem dnevu	xxx km/h xxx km/h(xxx)
	Priimek voznika	◙ Last_Name_____
	Osebno(-a) ime(-na) voznika	First_Name_____
	Identifikacija vozniške kartice	Card_Identification_____
21.5	Če v bloku ni nobenega zapisa prekoračitve hitrosti.	»---
22	***Ročno vpisani podatki***	
	Identifikator bloka	----------
22.1	Kraj nadzora	▫• .....
22.2	Podpis nadzornika	▫ .....
22.3	Od časa	◷+ .....
22.4	Do časa	+◷ .....
22.5	Podpis voznika	◙ .....

„Ročno vneseni podatki“; nad ročno vneseno postavko vstavite dovolj praznih vrstic, da se lahko zapišejo zahtevane informacije ali doda podpis.

▼B

23 ***Najnovejše kartice, vstavljene v enoto vozila***

Identifikator bloka

23.1 Vstavljena kartica

Identifikator zapisa

Vrsta kartice, ustvarjanje, verzija, proizvajalec (*)

Identifikacija kartice

Serijska številka kartice

Datum in čas zadnje vstavitve kartice

```
-------- ⊟◪◔ --------

----
↑ <gen> <version> <MC>
Identifikacija kartice
Serijska številka kartice
dd/mm/yyyy hh:mm
```

(*) (vse v eni vrstici)

pri čemer je:

vrsta kartice: piktogram, en znak + presledek

gen: GEN1 ali GEN2, 4 znaki + presledek

verzija: do 10 znakov

MC: koda proizvajalca, 3 znaki

3. SPECIFIKACIJE IZPISOV

V tem poglavju se uporabljajo naslednji dogovori o zapisovanju:

N	Številka bloka ali zapisa N
N	Številka bloka ali zapisa N, ponovljena, kolikor krat je potrebno
X/Y	Izpis ustreznega bloka ali zapisa X in/ali Y, ponovljen, kolikor krat je potrebno.

3.1. **Dnevni izpis vozniških dejavnosti s kartice**

PRT_008 Dnevni izpis vozniških dejavnosti s kartice je v skladu z naslednjim formatom:

1	Datum in čas izpisanega dokumenta
2	Vrsta izpisa
3	Identifikacija nadzornika (če je v VU vstavljena nadzorna kartica)
3	Identifikacija voznika (s kartice, ki se izpisuje + GEN)
4	Identifikacija vozila (vozilo, iz katerega se opravi izpis)
5	Identifikacija VU (VU, iz katere se opravi izpis + GEN)
6	Zadnja kalibracija te VU
7	Zadnji nadzor voznika, ki se nadzoruje
8	Ločilo voznikovih dejavnosti
8a	Stanje zunaj področja uporabe na začetku tega dneva
8.1a/8.1b/8.1c/8.2/ 8.3/8.3a/8.4	Voznikove dejavnosti v časovnem zaporedju
11	Ločilo dnevnega povzetka

▼B

11.4	Vneseni kraji v časovnem zaporedju
11.5	Podatki GNSS
11.6	Skupne vrednosti dejavnosti
12.1	Ločilo dogodkov ali napak s kartice
12.4	Zapisi dogodkov/napak (zadnjih 5 dogodkov ali napak, shranjenih na kartici)
13.1	Ločilo dogodkov ali napak iz VU
13.4	Zapisi dogodkov/napak (zadnjih 5 dogodkov ali napak, ki so v VU shranjene ali so v teku)
22.1	Kraj nadzora
22.2	Podpis nadzornika
22.5	Podpis voznika

3.2. **Dnevni izpis voznikovih dejavnosti iz VU**

PRT_009 Dnevni izpis voznikovih dejavnosti iz VU je v skladu z naslednjim formatom:

1	Datum in čas izpisanega dokumenta
2	Vrsta izpisa
3	Identifikacija imetnika kartice (za vse kartice, vstavljene v VU + GEN)
4	Identifikacija vozila (vozilo, iz katerega se opravi izpis)
5	Identifikacija VU (VU, iz katere se opravi izpis + GEN)
6	Zadnja kalibracija te VU
7	Zadnji nadzor na tem tahografu
9	Ločilo voznikovih dejavnosti
10	Ločilo voznikove reže (reža 1)
10 a	Stanje zunaj področja uporabe na začetku tega dneva
10.1/10.2/10.3/ 10.3a/10.4	Dejavnosti v časovnem zaporedju (voznikova reža)
10	Ločilo sovoznikove reže (reža 2)
10 a	Stanje zunaj področja uporabe na začetku tega dneva
10.1/10.2/10.3/ 10.3a/10.4	Dejavnosti v časovnem zaporedju (sovoznikova reža)
11	Ločilo dnevnega povzetka
11.1	Povzetek obdobij brez kartice v voznikovi reži
11.4	Vneseni kraji v časovnem zaporedju
11.5	Podatki GNSS

▼B

11.6	Skupne vrednosti dejavnosti
11.2	Povzetek obdobij brez kartice v sovoznikovi reži
11.4	Vneseni kraji v časovnem zaporedju
11.5	Podatki GNSS
11.7	Skupne vrednosti dejavnosti
11.3	Povzetek dejavnosti za voznika, vključno z obema režama
11.4	Vnosi krajev tega voznika v časovnem zaporedju
11.5	Podatki GNSS
11.8	Skupne vrednosti po dejavnostih za tega voznika
13.1	Ločilo dogodkov in napak
12.4	Zapisi dogodkov/napak (zadnjih 5 dogodkov ali napak, ki so v VU shranjene ali so v teku)
13.1	Kraj nadzora
22.2	Podpis nadzornika
22.3	Od časa (prostor, na katerem lahko voznik brez kartice označi, katera obdobja se nanašajo nanj)
22.4	Do časa
22.5	Podpis voznika

3.3. **Izpis dogodkov in napak s kartice**

PRT_010 Dnevni izpis dogodkov in napak s kartice je v skladu z naslednjim formatom:

1	Datum in čas izpisanega dokumenta
2	Vrsta izpisa
3	Identifikacija nadzornika (če je v VU + GEN vstavljena nadzorna kartica)
3	Identifikacija voznika (iz kartice, iz katere teče izpis)
4	Identifikacija vozila (vozilo, iz katerega se opravi izpis)
12.2	Ločilo dogodkov
12.4	Zapisi dogodkov (vsi dogodki, shranjeni na kartici)
12.3	Ločilo napak
12.4	Zapisi napak (vse napake, shranjene na kartici)
22.1	Kraj nadzora
22.2	Podpis nadzornika
22.5	Podpis voznika

▼B

3.4. **Izpis dogodkov in napak iz VU**

PRT_011 Dnevni izpis dogodkov in napak iz VU je v skladu z naslednjim formatom:

1	Datum in čas izpisanega dokumenta
2	Vrsta izpisa
3	Identifikacija imetnika kartice (za vse kartice, vstavljene v VU + GEN)
4	Identifikacija vozila (vozilo, iz katerega se opravi izpis)
13.2	Ločilo dogodkov
13.4	Zapisi dogodkov (vsi dogodki, shranjeni v VU ali v teku)
13.3	Ločilo napak
13.4	Zapisi napak (vse napake, shranjeni v VU ali v teku)
22.1	Kraj nadzora
22.2	Podpis nadzornika
22.5	Podpis voznika

3.5. **Izpis tehničnih podatkov**

PRT_012 Izpis tehničnih podatkov je v skladu z naslednjim formatom:

1	Datum in čas izpisanega dokumenta
2	Vrsta izpisa
3	Identifikacija imetnika kartice (za vse kartice, vstavljene v VU + GEN)
4	Identifikacija vozila (vozilo, iz katerega se opravi izpis)
14	Identifikacija VU
15	Identifikacija tipala
15.1	Podatki o povezovanju tipala (vsi razpoložljivi podatki v časovnem zaporedju)
16	Identifikacija GNSS
16.1	Podatki o povezovanju zunanje GNSS opreme (vsi razpoložljivi podatki v časovnem zaporedju)
17	Ločilo podatkov o kalibraciji
17.1	Zapisi kalibracije (vsi razpoložljivi zapisi v časovnem zaporedju)
18	Ločilo nastavljanj časa
18.1	Zapisi nastavljanj časa (vsi razpoložljivi zapisi iz dejavnosti nastavljanja časa in dejavnosti kalibracije)
19	Najnovejši dogodek in napaka, zapisana v enoti vozila

▼B

3.6. **Izpis prekoračitev hitrosti**

PRT_013 Izpis prekoračitev hitrosti je v skladu z naslednjim formatom:

1	Datum in čas izpisanega dokumenta
2	Vrsta izpisa
3	Identifikacija imetnika kartice (za vse kartice, vstavljene v VU + GEN)
4	Identifikacija vozila (vozilo, iz katerega se opravi izpis)
20	Informacije o nadzoru prekoračitev hitrosti
21.1	Identifikator podatkov o prekoračitvi hitrosti
21.4/21.5	Prva prekoračitev hitrosti po zadnji kalibraciji
21.2	Identifikator podatkov o prekoračitvi hitrosti
21.4/21.5	5 najresnejših dogodkov prekoračitve hitrosti v zadnjih 365 dneh
21.3	Identifikator podatkov o prekoračitvi hitrosti
21.4/21.5	Najresnejši dogodek na vsakega od 10 zadnjih dni nastopov dogodkov
22.1	Kraj nadzora
22.2	Podpis nadzornika
22.5	Podpis voznika

3.7. **Zgodovina vstavljenih kartic**

PRT_014 Izpis zgodovine vstavljenih kartic je v skladu z naslednjim formatom:

1	Datum in čas izpisanega dokumenta
2	Vrsta izpisa
3	Identifikacija imetnika kartice (za vse kartice, vstavljene v VU)
23	Najnovejše kartice, vstavljene v VU
23.1	Vstavljene kartice (do 88 zapisov)
12.3	Ločilo napak

▼B

Dodatek 5

PRIKAZOVALNIK

V tem poglavju se uporabljajo naslednji dogovori o zapisu formatov:

— **krepko** natisnjeni znaki označujejo neformatirano besedilo, ki se prikaže (prikazovanje z normalnimi znaki),

— normalni znaki označujejo spremenljivke (piktograme ali podatke), ki se jih za prikazovanje nadomesti z njihovimi vrednostmi:

  — dd mm yyyy: dan, mesec, leto,

  — hh: ure,

  — mm: minute,

  — D: piktogram trajanja

  — EF: kombinacija piktogramov dogodkov ali napak,

  — O: piktogram načina delovanja.

DIS_001 Tahograf prikazuje podatke z naslednjimi formati:

Podatki	Format
Privzeti prikazovalnik	
Lokalni čas	hh:mm
Način delovanja	O
Informacije, povezane z voznikom	1 Dhh**h**mm ‖hh**h**mm
Informacije, povezane s sovoznikom	2Dhh**h**mm
Začetek pogoja zunaj področja veljavnosti	OUT
Opozorilni prikazovalnik	
Preseženi čas neprekinjene vožnje	1 ⊙hh**h**mm ‖hh**h**mm
Dogodek ali napaka	EF
Drugi prikazovalniki	
Datum UTC Čas	UTC ⊙dd/mm/yyyy ali UTC ⊙dd.mm.yyyy hh:mm
Čas neprekinjene vožnje in skupni čas odmorov voznika	1 ⊙hh**h**mm ‖hh**h**mm
Čas neprekinjene vožnje in skupni čas odmorov sovoznika	2 ⊙hh**h**mm ‖hh**h**mm
Skupni čas vožnje voznika v prejšnjem in trenutnem tednu	1 ⊙‖ hhh**h**mm
Skupni čas vožnje sovoznika v prejšnjem in trenutnem tednu	2 ⊙‖ hhh**h**mm

▼B

Dodatek 6

ČELNI PRIKLJUČEK ZA KALIBRACIJO IN PRENOS PODATKOV

KAZALO

1. STROJNA OPREMA

1.1 Priključek

1.2 Razporeditev kontaktov

1.3 Bločni diagram

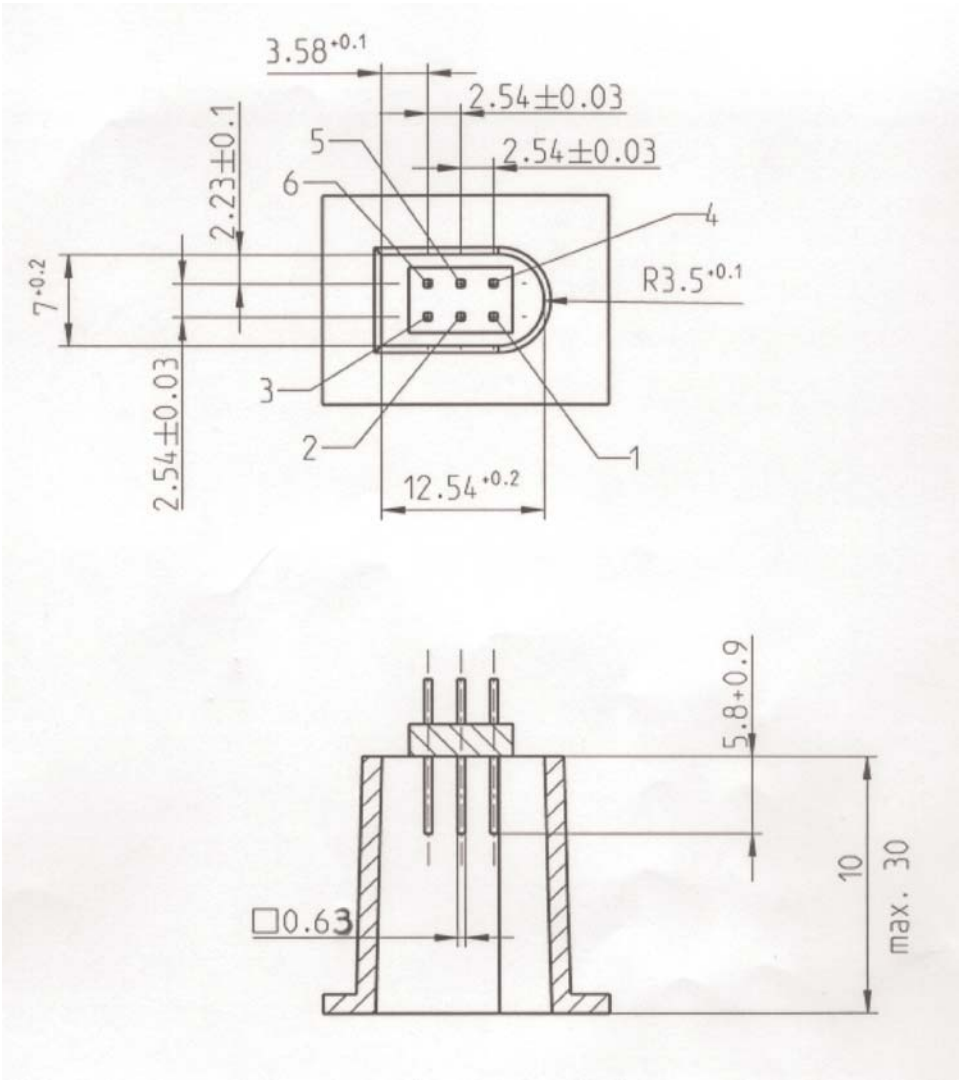
2. VMESNIK ZA PRENOS PODATKOV

3. KALIBRACIJSKI VMESNIK

1. STROJNA OPREMA

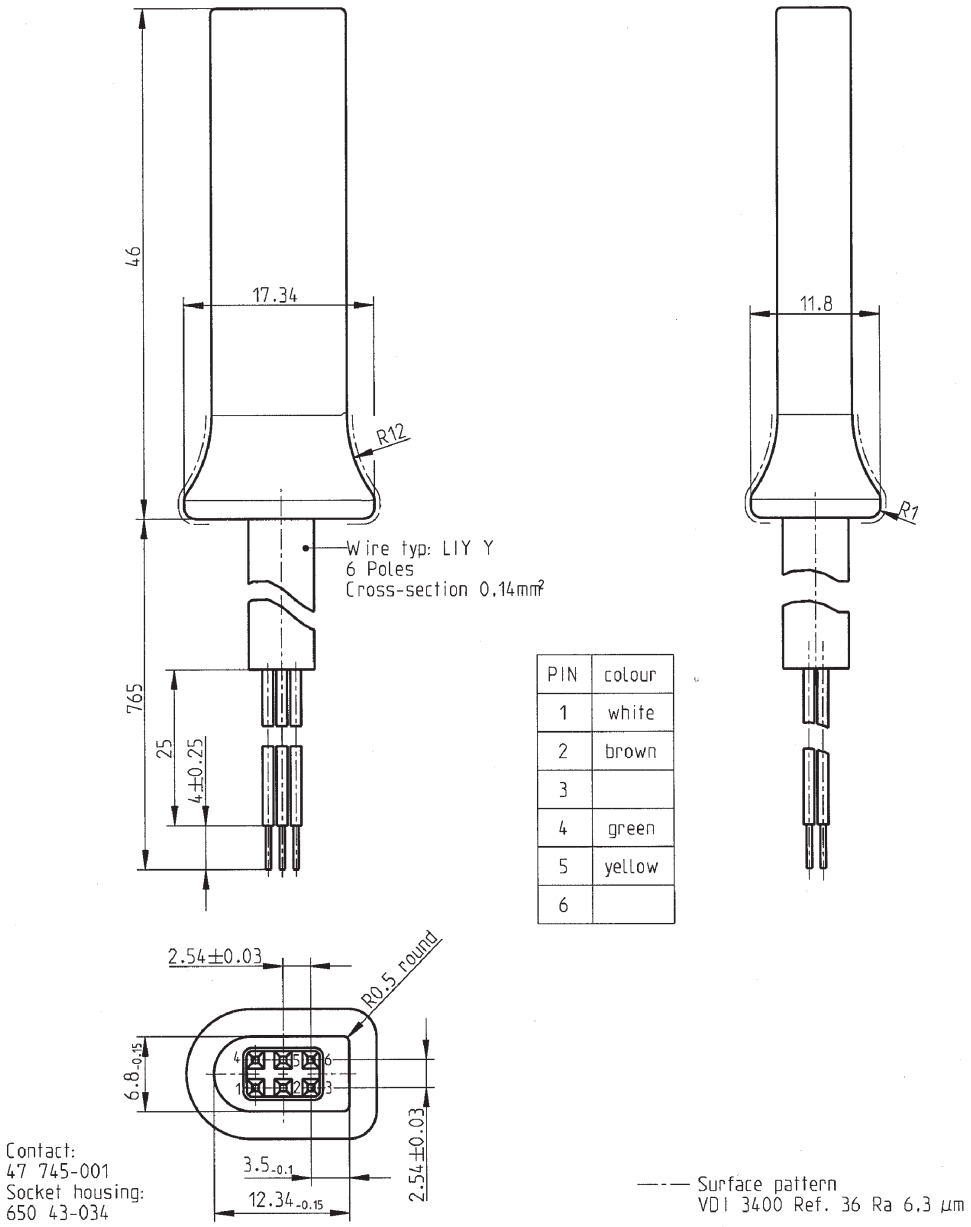
1.1 **Priključek**

INT_001 Priključek za prenos podatkov/kalibracijo je priključek s šestimi nožicami, dosegljiv na čelni plošči, ne da bi bilo treba kateri koli del tahografa izključiti, in skladen z naslednjo risbo (vse mere so v milimetrih):



▼B

Naslednji diagram prikazuje tipični 6-polni vtikač:



PIN	colour
1	white
2	brown
3	
4	green
5	yellow
6	

1.2 **Razporeditev kontaktov**

INT_002 Kontakti so razporejeni v skladu z naslednjo tabelo:

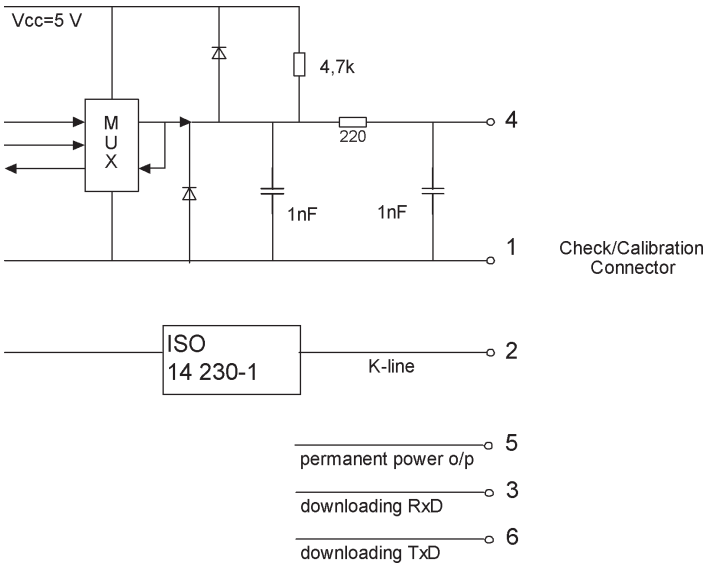
Nožica	Opis	Opomba
1	Akumulator – minus	Priključen na negativni pol akumulatorja vozila
2	Podatkovna komunikacija	Linija K (ISO 14230-1)
3	RxD – prenos podatkov	Vnos podatkov v tahograf
4	Vhodni/izhodni signal	Kalibracija

▼B

Nožica	Opis	Opomba
5	Trajni napajalni izhod	Določeno območje napetosti je napetost napeljave v vozilu, znižano za 3 V zaradi padca napetosti na zaščitnih vezjih. Izhod 40 mA
6	TxD – prenos podatkov	Iznos podatkov iz tahografa

1.3 **Bločni diagram**

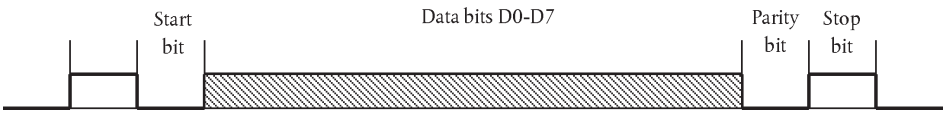
INT_003 Bločni diagram je skladen z naslednjim:



2. VMESNIK ZA PRENOS PODATKOV

INT_004 Vmesnik za prenos podatkov ustreza specifikacijam RS232.

INT_005 Vmesnik za prenos podatkov uporablja en začetni bit, 8 podatkovnih bitov (prvi bit je bit z najmanjšo težo (LSB)), en parnostni in en končni bit.



Organizacija podatkovnih bajtov

Začetni bit: en bit na logični ravni 0;

Podatkovni biti: se prenašajo tako, da je LSB prvi;

Parnostni bit: soda parnost;

Končni bit: en bit na logični ravni 1.

Kadar se pošiljajo numerični podatki, ki jih sestavlja več bajtov, se najprej prenese bajt z največjo težo, nazadnje pa bajt z najmanjšo težo.

INT_006 Baudna hitrost prenosa mora biti nastavljiva v območju od 9 600 bit/s do 115 200 bit/s. Pošiljanje poteka z najvišjo možno hitrostjo, baudna hitrost se ob začetku komunikacije nastavi na 9 600 bit/s.

▼B

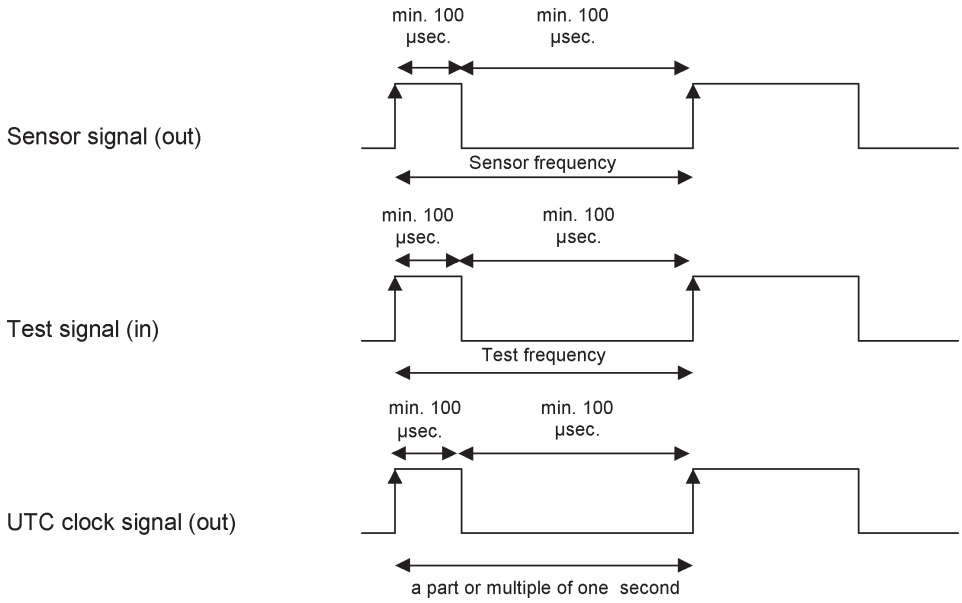
3. KALIBRACIJSKI VMESNIK

INT_007 Komunikacijski podatki so v skladu z ISO 14230-1 Road vehicles – Diagnostic systems – Keyword protocol 2000 – Part 1: Physical layer, First edition: 1999.

INT_008 Vhodno/izhodni signal je skladen z naslednjimi električnimi specifikacijami:

Parameter	Minimum	Tipično	Maksimum	Opomba
U_{low} (vhodno)			1,0 V	I = 750 µA
U_{high} (vhodno)	4 V			I = 200 µA
Frekvenca			4 kHz	
U_{low} (izhodno)			1,0 V	I = 1 mA
U_{high} (izhodno)	4 V			I = 1 mA

INT_009 Vhodno/izhodni signal je skladen z naslednjimi časovnimi diagrami:



▼B

Dodatek 7

PROTOKOLI ZA PRENOS PODATKOV

KAZALO

1. UVOD

1.1. Področje uporabe

1.2. Kratice in zapisovanje

2. PRENOS PODATKOV IZ VU

2.1. Postopek prenosa

2.2. Protokol za prenos podatkov

2.2.1 Struktura sporočil

2.2.2 Vrste sporočil

2.2.2.1 *Start Communication Request* (SID 81)

2.2.2.2 *Positive Response Start Communication* (SID C1)

2.2.2.3 *Start Diagnostic Session Request* (SID 10)

2.2.2.4 *Positive Response Start Diagnostic* (SID 50)

2.2.2.5 *Link Control Service* (SID 87)

2.2.2.6 *Link Control Positive Response* (SID C7)

2.2.2.7 *Request Upload* (SID 35)

2.2.2.8 *Positive Response Request Upload* (SID 75)

2.2.2.9 *Transfer Data Request* (SID 36)

2.2.2.10 *Positive Response Transfer Data* (SID 76)

2.2.2.11 *Request Transfer Exit* (SID 37)

2.2.2.12 *Positive Response Request Transfer Exit* (SID 77)

2.2.2.13 *Stop Communication Request* (SID 82)

2.2.2.14 *Positive Response Stop Communication* (SID C2)

2.2.2.15 *Acknowledge Sub Message* (SID 83)

2.2.2.16 *Negative Response* (SID 7F)

2.2.3 Potek sporočil

2.2.4 Časovni razpored

▼B

2.2.5 Obravnava napak

2.2.5.1 Faza začetka komunikacije

2.2.5.2 Faza komunikacije

2.2.6 Vsebina sporočila odziva

2.2.6.1 Positive Response Transfer Data Overview

2.2.6.2 Positive Response Transfer Data Activities

2.2.6.3 Positive Response Transfer Data Events and Faults

2.2.6.4 Positive Response Transfer Data Detailed Speed

2.2.6.5 Positive Response Transfer Data Technical Data

2.3. Hramba datoteke na zunanjem pomnilniškem mediju (ESM)

3. PROTOKOL ZA PRENOS PODATKOV S TAHOGRAFSKIH KARTIC

3.1. Področje uporabe

3.2. Opredelitve pojmov

3.3. Prenos podatkov s kartice

3.3.1 Inicializacijsko zaporedje

3.3.2 Zaporedje za nepodpisane podatkovne datoteke

3.3.3 Zaporedje za podpisane podatkovne datoteke

3.3.4 Zaporedje za ponastavitev števca kalibracij

3.4. Format hrambe podatkov

3.4.1 Uvod

3.4.2 Format datoteke

4. PRENOS PODATKOV S TAHOGRAFSKE KARTICE PREKO ENOTE V VOZILU

1. UVOD

Ta dodatek določa postopke, ki se uporabljajo pri različnih vrstah prenosov podatkov na zunanje pomnilniške medije, in protokole, ki jih je treba izvajati za zagotovitev pravilnega prenosa podatkov in polne združljivosti formatov prenesenih podatkov, tako da jih vsak nadzornik lahko pregleda in pred analiziranjem preveri njihovo avtentičnost in celovitost.

1.1. **Področje uporabe**

Podatke se v zunanji pomnilniški medij (ESM) lahko prenaša:

— iz enote v vozilu z inteligentno namensko opremo (IDE), priključeno na VU,

— s tahografske kartice z IDE, opremljeno z vmesniško napravo (IFD),

▼B

— s kartice preko enote v vozilu z IDE, priključeno na VU.

Da bi se lahko preverilo avtentičnost in celovitost prenesenih podatkov, shranjenih na ESM, se podatki prenašajo s pripetim podpisom v skladu z Dodatkom 11 Skupni varnostni mehanizmi. Prenesejo se tudi identifikacija in varnostni certifikati (države članice in opreme) izvorne opreme (VU ali kartice). Oseba, ki preveri podatke, mora imeti lasten varnostni evropski javni ključ, ki ga je pridobila neodvisno.

DDP_001 Podatki, ki se prenesejo v eni seji prenosa, morajo biti shranjeni na ESM v eni sami datoteki.

1.2. **Kratice in zapisovanje**

V tem dodatku so uporabljene naslednje kratice:

AID Identifikator aplikacije (*Application Identifier*)

ATR Odgovor na ponastavitev (*Answer to Reset*)

CS Bajt kontrolne vsote (*Checksum byte*)

DF Namenska datoteka (*Dedicated File*)

DS_ Diagnostična seja (*Diagnostic Session*)

EF Elementarna datoteka (*Elementary File*)

ESM Zunanji pomnilniški medij (*External Storage Medium*)

FID Identifikator datoteke (ID datoteke) (*File Identifier*)

FMT Formatni bajt (prvi bajt glave sporočila) (*Format Byte*)

ICC Kartica z integriranim vezjem (*Integrated Circuit Card*)

IDE Inteligentna namenska oprema (*Intelligent Dedicated Equipment*): oprema, ki se uporablja za prenos podatkov na ESM (npr. osebni računalnik)

IFD Vmesniška naprava (*Interface Device*)

KWP Protokol s ključnimi besedami 2000 (*Keyword Protocol 2000*)

LEN Bajt dolžine (zadnji bajt glave sporočila) (*Length Byte*)

PPS Izbor parametrov protokola (*Protocol Parameter Selection*)

PSO Izvedba varnostne operacije (*Perform Security Operation*)

SID Identifikator storitve (*Service Identifier*)

SRC Izvorni bajt (*Source byte*)

TGT Ciljni bajt (*Target Byte*)

TLV Vrednost dolžine oznake (*Tag Length Value*)

TREP Parameter odziva na zahtevek za prenos (*Transfer Response Parameter*)

TRTP Parameter zahtevka za prenos (*Transfer Request Parameter*)

VU Enota v vozilu (*Vehicle Unit*)

▼B

2. PRENOS PODATKOV IZ VU

2.1. **Postopek prenosa**

Za prenos podatkov iz VU operater izvede naslednje postopke:

— vstavi svojo tahografsko kartico v režo VU (*),

— priključi IDE na priključek VU za prenos podatkov,

— vzpostavi povezavo med IDE in VU,

— v IDE izbere podatke, ki naj se prenesejo, in pošlje zahtevek v VU,

— zaključi sejo prenosa podatkov.

2.2. **Protokol za prenos podatkov**

Protokol je strukturiran kot sodelovanje nadrejenega in podrejenega udeleženca (*master-slave*), pri čemer je IDE nadrejeni, VU pa podrejeni udeleženec.

Struktura, vrste in tok sporočil temeljijo v glavnem na protokolu ključnih besed 2000 (KWP) (ISO 14230-2 *Road vehicles – Diagnostic systems – Keyword protocol 2000 – Part 2*: *Data link layer*).

Aplikativna raven v glavnem temelji na sedanjem osnutku ISO 14229-1 (*Road vehicles – Diagnostic systems – Part 1: Diagnostic services, version 6 of 22 February 2001*).

2.2.1 *Struktura sporočil*

DDP_002 Vsa sporočila, ki si jih izmenjujeta IDE in VU, so formatirana tako, da jih sestavljajo trije deli:

— glava, ki jo sestavljajo formatni bajt (FMT), ciljni bajt (TGT), izvorni bajt (SRC) in po potrebi še bajt dolžine (LEN),

— podatkovno polje, ki ga sestavljajo bajt identifikatorja storitve (SID) in spremenljivo število podatkovnih bajtov, ki lahko vključujejo neobvezni bajt diagnostične seje (DS_) ali neobvezni bajt parametrov prenosa (TRTP ali TREP).

— kontrolna vsota, ki jo sestavlja bajt kontrolne vsote (CS).

Glava				Podatkovno polje					Kontrolna vsota
FMT	TGT	SRC	LEN	SID	DATA	…	…	…	CS
4 bajti				Največ 255 bajtov					1 bajt

Bajta TGT in SRC predstavljata fizična naslova prejemnika in tvorca sporočila. Vrednosti sta F0 Hex za IDE in EE Hex za VU.

Bajt LEN je dolžina podatkovnega polja.

Bajt kontrolne vsote je 8-bitni rezultat ostanka vsote po modulu 256 vseh bajtov sporočila razen bajta CS samega.

Bajti FMT, SID, DS_, TRTP in TREP so opredeljeni nižje v tem dokumentu.

(*) Vstavljena kartica sproži ustrezne pravice dostopa do funkcij prenosa in podatkov. Omogočen pa mora biti prenos podatkov z vozniške kartice, vstavljene v eno od rež VU, četudi v drugi reži ni vstavljena nobena druga vrsta kartice.

▼B

DDP_003 Če mora sporočilo prenesti več podatkov, kot je na voljo prostora v podatkovnem polju, se sporočilo pošlje v več delnih sporočilih. Vsako delno sporočilo ima glavo, isti bajt SID in bajt TREP ter 2-bajtni števec delnih sporočil, ki kaže zaporedno številko delnega sporočila v celotnem sporočilu. Da se omogoči preverjanje napak in prekinitev prenosa, IDE potrdi vsako delno sporočilo. IDE lahko delno sporočilo sprejme, zahteva njegovo ponovno posredovanje, zahteva od VU, naj ponovno začne prenos, ali prekine prenos.

DDP_004 Če zadnje delno sporočilo v svojem podatkovnem polju vsebuje natanko 255 bajtov, mora biti priloženo še končno delno sporočilo s praznim podatkovnim poljem (razen bajtov SID in TREP ter števca delnih sporočil), ki označi konec celotnega sporočila.

Primer:

Glava	SID	TREP	Sporočilo	CS
4 bajti	Daljše od 255 bajtov			

To sporočilo bo preneseno v naslednji obliki:

Glava	SID	TREP	00	01	Delno sporočilo 1	CS
4 bajti	255 bajtov					

Glava	SID	TREP	00	02	Delno sporočilo 2	CS
4 bajti	255 bajti					

…

Glava	SID	TREP	xx	yy	Delno sporočilo n	CS
4 bajti	Manj kot 255 bajtov					

ali v naslednji:

Glava	SID	TREP	00	01	Delno sporočilo 1	CS
4 bajti	255 bajti					

Glava	SID	TREP	00	02	Delno sporočilo 2	CS
4 bajti	255 bajti					

…

Glava	SID	TREP	xx	yy	Delno sporočilo n	CS
4 bajti	255 bajti					

Glava	SID	TREP	xx	yy + 1	CS
4 bajti	4 bajti				

▼B

2.2.2 *Vrste sporočil*

Komunikacijski protokol za prenos podatkov med VU in IDE zahteva izmenjavo osmih različnih vrst sporočil.

Ta sporočila pregledno prikazuje naslednja tabela.

Struktura sporočil	Največ 4 bajti Glava				Največ 255 bajtov Podatki			1 bajt Kontro-lna vsota
IDE -> <- VU	FMT	TGT	SRC	LEN	SID	DS_/TRTP	DATA	CS
Start Communication Request	81	EE	F0		81			E0
Positive Response Start Communication	80	F0	EE	03	C1		EA, 8F	9B
Start Diagnostic Session Request	80	EE	F0	02	10	81		F1
Positive Response Start Diagnostic	80	F0	EE	02	50	81		31
Link Control Service								
Verify Baud Rate (stage 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
Positive Response Verify Baud Rate	80	F0	EE	02	C7		01	28
Transition Baud Rate (stage 2)	80	EE	F0	03	87		02,03	ED
Request Upload	80	EE	F0	0A	35		00,00,00,00,00, FF,FF,FF,FF	99
Positive Response Request Upload	80	F0	EE	03	75		00,FF	D5
Transfer Data Request								
Overview	80	EE	F0	02	36	01		97
Activities	80	EE	F0	06	36	02	Date	CS
Events & Faults	80	EE	F0	02	36	03		99
Detailed Speed	80	EE	F0	02	36	04		9 A
Technical Data	80	EE	F0	02	36	05		9 B
Card download	80	EE	F0	02	36	06	Slot	CS
Positive Response Transfer Data	80	F0	EE	Len	76	TREP	Data	CS
Request Transfer Exit	80	EE	F0	01	37			96
Positive Response Request Transfer Exit	80	F0	EE	01	77			D6

▼B

Struktura sporočil	Največ 4 bajti Glava				Največ 255 bajtov Podatki			1 bajt Kontrolna vsota
IDE -> <- VU	FMT	TGT	SRC	LEN	SID	DS_/TRTP	DATA	CS
Stop Communication Request	80	EE	F0	01	82			E1
Positive Response Stop Communication	80	F0	EE	01	C2			21
Acknowledge sub message	80	EE	F0	Len	83		Data	CS
Negative responses								
General reject	80	F0	EE	03	7F	Sid Req	10	CS
Service not supported	80	F0	EE	03	7F	Sid Req	11	CS
Sub function not supported	80	F0	EE	03	7F	Sid Req	12	CS
Incorrect Message Length	80	F0	EE	03	7F	Sid Req	13	CS
Conditions not correct or Request sequence error	80	F0	EE	03	7F	Sid Req	22	CS
Request out of range	80	F0	EE	03	7F	Sid Req	31	CS
Upload not accepted	80	F0	EE	03	7F	Sid Req	50	CS
Response pending	80	F0	EE	03	7F	Sid Req	78	CS
Data not available	80	F0	EE	03	7F	Sid Req	FA	CS

Opombe:

— Sid Req = Sid zadevnega zahtevka.

— TREP = TRTP zadevnega zahtevka.

— Temne celice pomenijo, da se nič ne prenese.

— Izraz nalaganje („*upload*“ glede na IDE) se uporablja zaradi skladnosti z ISO 14229. Pomeni isto kot prenos („*download*“ glede na VU).

— Morebitni 2-bajtni števci delnih sporočil v tej tabeli niso prikazani.

— Reža je številka reže, bodisi ‘1’ (kartica na voznikovi reži) ali ‘2’ (kartica na sovoznikovi reži).

— Kadar reža ni določena, VU izbere režo št. 1, če je vanjo vstavljena kartica, režo 2 pa le v primeru, da jo je posebej izbral uporabnik.

2.2.2.1 *Start Communication Request* (SID 81)

DDP_005 To sporočilo pošlje IDE za vzpostavitev komunikacijske povezave z VU. Začetna komunikacija vedno poteka s hitrostjo 9 600 baudov (dokler baudne hitrosti ne spremenijo ustrezen *Link control services*).

▼B

2.2.2.2 *Positive Response Start Communication* (SID C1)

DDP_006 To sporočilo pošlje VU kot pozitivni odziv na zahtevek *Start Communication Request*. Sporočilo vsebuje dva ključna bajta 'EA', '8F', ki kažeta, da enota podpira protokol, pri katerem glava vsebuje podatke o izvoru, cilju in dolžini.

2.2.2.3 *Start Diagnostic Session Request* (SID 10)

DDP_007 Sporočilo *Start Diagnostic Session Request* pošlje IDE in z njim zahteva novo diagnostično sejo z VU. Podfunkcija „privzeta seja" (81 hex) pomeni, da se začne standardna diagnostična seja.

2.2.2.4 *Positive Response Start Diagnostic* (SID 50)

DDP_008 Sporočilo *Positive Response Start Diagnostic* pošlje VU kot pozitivni odziv na *Diagnostic Session Request*.

2.2.2.5 *Link Control Service* (SID 87)

DDP_052 *Link Control Service* uporablja IDE za sprožitev spremembe baudne hitrosti. Ta sprememba se izvede v dveh korakih. V prvem koraku IDE predlaga spremembo baudne hitrosti in predlaga novo. Po prejemu pozitivnega sporočila od VU pošlje IDE v VU potrditev spremembe baudne hitrosti (drugi korak). Nato IDE spremeni baudno hitrost na novo vrednost. Po prejemu potrditve VU spremeni baudno hitrost na novo vrednost.

2.2.2.6 *Link Control Positive Response* (SID C7)

DDP_053 Sporočilo *Link Control Positive Response* pošlje VU kot pozitivni odziv na zahtevek *Link Control Service* (prvi korak). Na zahtevek za potrditev (drugi korak) ni odziva VU.

2.2.2.7 *Request Upload* (SID 35)

DDP_009 IDE s sporočilom *Request Upload* VU sporoči, da je bil zahtevan prenos. Za izpolnitev zahtev ISO 14229 so vključeni podatki o naslovu, velikosti in podrobnostih formata zahtevanih podatkov. Ker teh podatkov IDE pred začetkom prenosa podatkov ne pozna, je pomnilniški naslov nastavljen na 0, format na nešifrirani in nekomprimirani format, pomilniška velikost pa na največjo.

2.2.2.8 *Positive Response Request Upload* (SID 75)

DDP_010 Sporočilo *Positive Response Request Upload* pošlje VU, da bi sporočil IDE, da je VU pripravljena za prenos podatkov. Zaradi izpolnitve zahtev iz ISO 14229 so v sporočilu s pozitivnim odzivom vključeni podatki, ki IDE sporočajo, da bodo naslednja sporočila *Positive Response Transfer Data* vsebovala največ 00FF hex bajtov.

▼B

2.2.2.9 *Transfer Data Request* (SID 36)

DDP_011 Sporočilo *Transfer Data Request* pošlje IDE; da bi VU sporočil, katera vrsta podatkov se prenese. Enobajtni parameter TRTP navaja vrsto prenosa.

Obstaja šest vrst prenosa podatkov:

— pregled (*Overview*, TRTP 01),

— dejavnosti na določen dan (*Activities of a specified date*, TRTP 02),

— dogodki in napake (*Events and faults*, TRTP 03),

— podrobni podatki o hitrosti (*Detailed speed*, TRTP 04),

— tehnični podatki (*Technical data*, TRTP 05),

— prenos podatkov s kartice (*Card download*, TRTP 06).

DDP_054 IDE med sejo prenosa podatkov obvezno zahteva prenos podatkov iz pregleda (TRTP 01), saj le to zagotavlja zapis certifikatov VU v preneseno datoteko (in preverjanje digitalnega podpisa).

V drugem primeru (TRTP 02) sporočilo *Transfer Data Request* vsebuje podatek o koledarskem dnevu (v formatu`TimeReal`), za katerega se prenesejo podatki.

2.2.2.10 *Positive Response Transfer Data* (SID 76)

DDP_012 Sporočilo *Positive Response Transfer Data* pošlje VU kot odziv na sporočilo *Transfer Data Request*. Sporočilo vsebuje zahtevane podatke s parametrom TREP, ki ustreza TRTP iz zahtevka.

DDP055 V prvem primeru (TREP 01) VU pošlje v IDE podatke, ki pomagajo operaterju izbrati podatke, ki jih želi prenesti v nadaljevanju. To sporočilo vsebuje naslednje podatke:

— varnostni certifikati,

— identifikacija vozila,

— trenutni datum in čas VU,

— najpoznejši in najzgodnejši datum, za katerega je mogoče prenesti podatke (podatki VU),

— znak prisotnosti kartic v VU,

— predhodni prenosi podatkov za potrebe podjetja,

— blokade s strani podjetja,

— predhodni nadzori.

▼B

2.2.2.11 *Request Transfer Exit* (SID 37)

DDP_013 Sporočilo *Request Transfer Exit* pošlje IDE; da z njim sporoči VU, da je seja prenosa podatkov zaključena.

2.2.2.12 *Positive Response Request Transfer Exit* (SID 77)

DDP_014 Sporočilo *Positive Response Request Transfer Exit* pošlje VU, da potrdi prejem zahtevka *Request Transfer Exit*.

2.2.2.13 *Stop Communication Request* (SID 82)

DDP_015 Sporočilo *Stop Communication Request* pošlje IDE, da prekine komunikacijsko povezavo z VU.

2.2.2.14 *Positive Response Stop Communication* (SID C2)

DDP_016 Sporočilo *Positive Response Stop Communication* pošlje VU, da potrdi prejem zahtevka *Stop Communication Request*.

2.2.2.15 *Acknowledge Sub Message* (SID 83)

DDP_017 Sporočilo *Acknowledge Sub Message* pošlje IDE, da potrdi prejem vsakega dela sporočila, ki se prenaša v več delnih sporočilih. Podatkovno polje vsebuje SID, prejet od VU, in naslednjo 2-bajtno kodo:

— MsgC + 1 potrjuje pravilni prejem številke delnega sporočila MsgC.

IDE od VU zahteva, da pošlje naslednje delno sporočilo.

— MsgC kaže, da je med prejemanjem številke delnega sporočila MsgC prišlo do težave.

IDE od VU zahteva, da delno sporočilo pošlje še enkrat.

— FFFF zahteva prekinitev pošiljanja sporočila.

To lahko uporabi IDE, da prekine prenašanje sporočila VU iz kateregakoli razloga.

Zadnje delno sporočilo (bajt LEN < 255) se lahko potrdi s katerokoli od teh kod ali ostane nepotrjeno.

Odgovori VU, ki bodo obsegali več delnih sporočil, so:

— *Positive Response Transfer Data* (SID 76)

▼B

2.2.2.16 *Negative Response* (SID 7F)

DDP_018 Sporočilo *Negative Response* pošlje VU kot odziv na zgornja sporočila z zahtevkom, kadar VU zahtevka ne more izpolniti. Podatkovno polje sporočila vsebuje SID odziva (7F), SID zahtevka in kodo, ki določa vzrok za negativni odziv. Na voljo so naslednje kode:

— 10 *General reject* (splošna zavrnitev)

Akcije ni mogoče izvesti iz razloga, ki spodaj ni naveden.

— 11 *Service not supported* (storitev ni podprta)

SID zahtevka ni razumljiv.

— 12 *Sub function not supported* (podfunkcija ni podprta)

Bajt DS_ ali TRTP zahtevka ni razumljiv ali pa ni nadaljnjih delnih sporočil za prenos.

— 13 *Incorrect message length* (nepravilna dolžina sporočila)

Dolžina sprejetega sporočila je napačna.

— 22 *Conditions not correct or request sequence error* (nepravilni pogoji ali napaka v zaporedju zahtevkov)

Zahtevana storitev ni aktivna ali pa ni pravilno zaporedje sporočil z zahtevkom.

— 31 *Request out of range* (zahtevek izven območja)

Zapis parametra zahtevka (podatkovno polje) ni veljaven.

— 50 *Upload not accepted* (prenos ni sprejet)

Zahtevka ni mogoče izpolniti (VU ni v ustreznem načinu delovanja ali pa ima notranjo napako).

— 78 *Response pending* (čakanje na odgovor)

Zahtevane akcije ni mogoče zaključiti pravočasno in VU ni pripravljena za sprejem novega zahtevka.

— FA *Data not available* (podatki niso na voljo)

Podatkovni objekt iz zahtevka za prenos podatkov ni na voljo v VU (npr. kartica ni vstavljena itd.)

2.2.3 *Potek sporočil*

Značilni potek sporočil običajnim postopkom prenosa podatkov je naslednji:

IDE		VU
Start Communication Request	⇨	
	⇦	Positive Response
Start Diagnostic Service Request	⇨	
	⇦	Positive Response
Request Upload	⇨	
	⇦	Positive Response

▼B

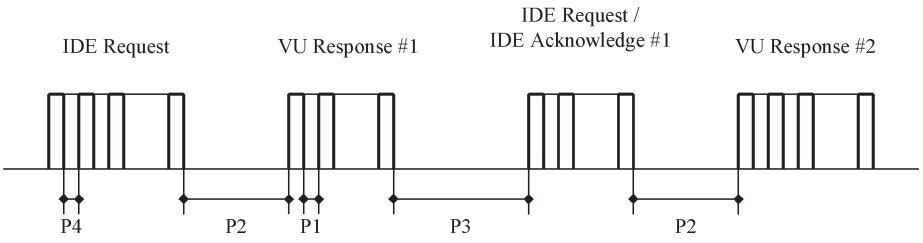
IDE		VU
Transfer Data Request Overview	⇨	
	⇦	Positive Response
Transfer Data Request #2	⇨	
	⇦	Positive Response #1
Acknowledge Sub Message #1	⇨	
	⇦	Positive Response #2
Acknowledge Sub Message #2	⇨	
	⇦	Positive Response #m
Acknowledge Sub Message #m	⇨	
	⇦	Positive Response (Data Field<255 Bytes)
Acknowledge Sub Message (optional)	⇨	
…		
Transfer Data Request #n	⇨	
	⇦	Positive Response
Request Transfer Exit	⇨	
	⇦	Positive Response
Stop Communication Request	⇨	
	⇦	Positive Response

2.2.4 *Časovni razpored*

DDP_019 Med običajnim delovanjem so pomembni časovni parametri, prikazani v naslednjem diagramu:

Diagram 1

Potek sporočil, časovni razpored



Pri čemer je:

P1 = čas med bajti v odzivu VU

P2 = čas med koncem zahtevka IDE in začetkom odziva VU ali med koncem potrditve IDE in začetkom naslednjega odziva VU.

P3 = čas med koncem odziva VU in začetkom novega zahtevka IDE, ali med koncem odziva VU in začetkom potrditve IDE, ali med koncem zahtevka IDE in začetkom novega zahtevka IDE; če se VU ne odzove.

P4 = čas med bajti zahtevka IDE.

P5 = podaljšana vrednost P3 za prenos podatkov s kartice

▼B

Dovoljene vrednosti časovnih parametrov so navedene v naslednji tabeli (razširjeni nabor časovnih parametrov KWP, uporabljen pri fizičnem naslavljanju za hitrejšo komunikacijo).

Časovni razpored Parameter časovnega razporeda	Spodnja mejna vrednost (ms)	Zgornja mejna vrednost (ms)
P1	0	20
P2	20	1 000 (*)
P3	10	5 000
P4	5	20
P5	10	20 minut

(*) Če se VU odzove z *Negative Response*, ki vsebuje kodo s pomenom „zahtevek pravilno prejet, čakanje na odgovor“, se ta vrednost zviša na vrednost, ki je enaka zgornji mejni vrednosti P3.

2.2.5 *Obravnava napak*

Če pri izmenjavi sporočil pride do napake, se shema poteka sporočil spremeni glede na to, kateri del opreme je zaznal napako in glede na sporočilo, ki je povzročilo napako.

Diagrama 2 in 3 prikazujeta postopke obravnave napak za VU in IDE.

2.2.5.1 Faza začetka komunikacije

DDP_020 Če IDE zazna napako v fazi začetka komunikacije, bodisi v časovnem razporedu ali v bitnem toku, počaka obdobje P3min in nato ponovno pošlje zahtevek.

DDP_021 Če VU zazna napako v zaporedju, ki ga prejema iz IDE, ne pošlje odziva in počaka naslednje sporočilo *Start Communication Request*, ki ga mora prejeti najpozneje v obdobju P3.

2.2.5.2 Faza komunikacije

Opredelimo lahko dve območji obravnave napak:

1. **VU zazna napako prenosa IDE.**

DDP_022 Pri vsakem sprejetem sporočilu VU zaznava napake časovnega poteka, napake v formatu bajtov (npr. kršitve pravil glede začetnih ali končnih bitov) in napake v okviru (prejeto napačno število bajtov, napaka v bajtu kontrolne vsote).

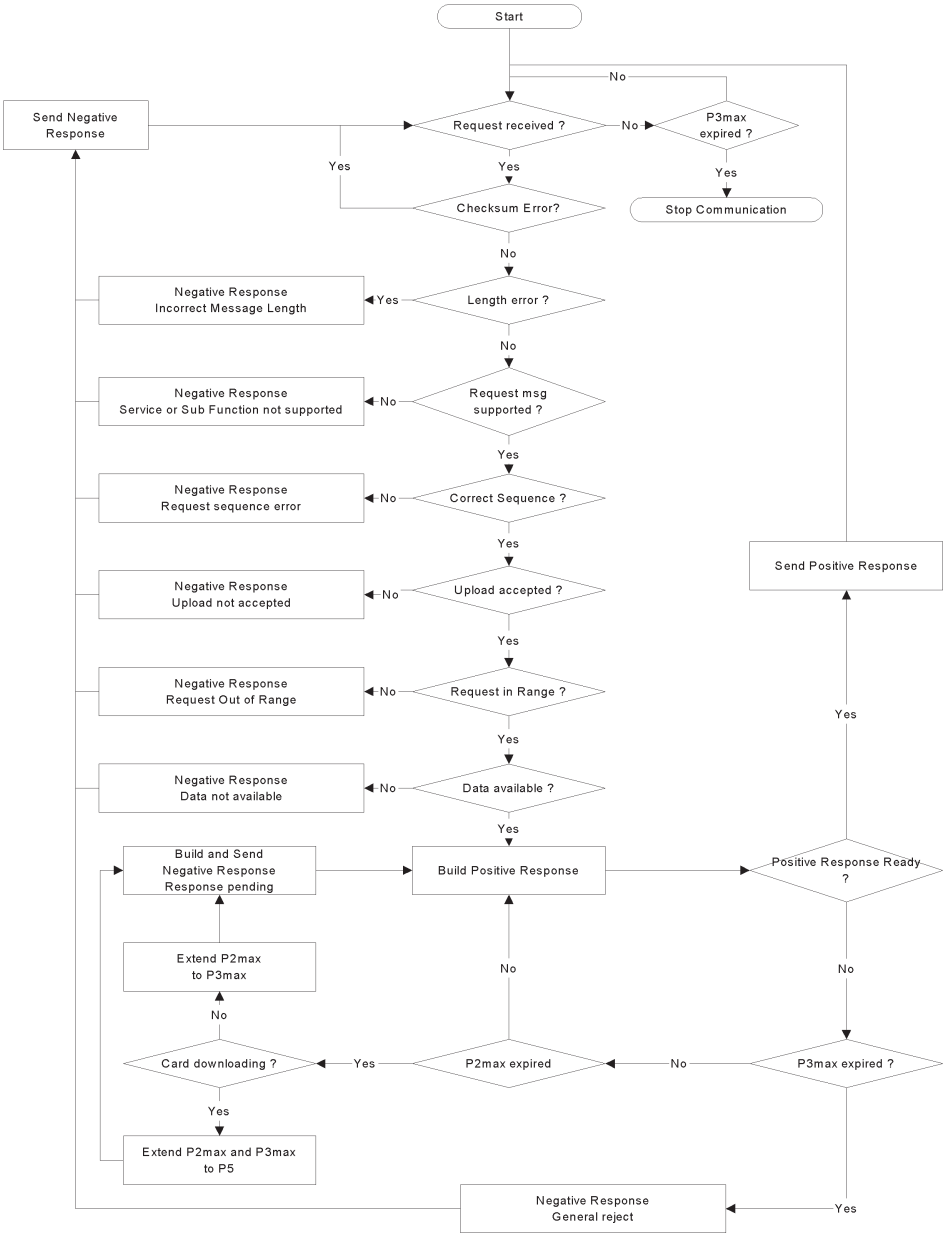
DDP_023 Če VU zazna katero od zgornjih napak, ne pošlje nobenega odziva in prezre prejeto sporočilo.

DDP_024 VU lahko zazna tudi druge napake v formatu ali vsebini prejetega sporočila (npr. sporočilo ni podprto), čeprav sporočilo izpolnjuje zahteve glede dolžine in kontrolne vsote; v takem primeru VU pošlje IDE sporočilo *Negative Response*, v katerem navede vrsto napake.

▼B

Slika 2

Obravnava napak VU



2. **IDE zazna napako prenosa VU.**

DDP_025 Za vsako prejeto sporočilo IDE zaznava napake časovnega poteka, napake v formatih bajtov (npr. kršitve pravil glede začetnih ali končnih bitov) in napake v okviru (prejeto napačno število bajtov, napaka v bajtu kontrolne vsote).

DDP_026 IDE zaznava tudi napake v zaporedju, npr. nepravilno povečevanje števca delnih sporočil v zaporedoma prejetih sporočilih.

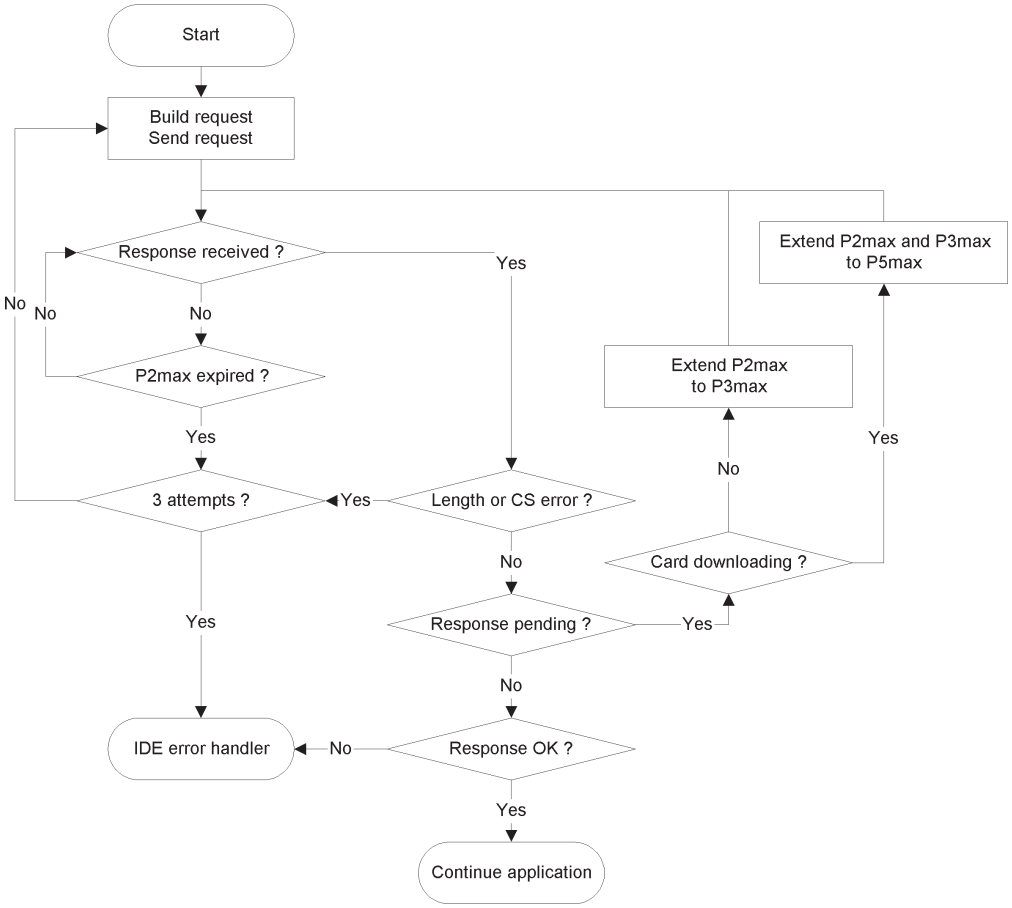
DDP_027 Če IDE zazna napako ali če ne prejme odziva iz VU v obdobju P2maks, pošlje sporočilo z zahtevkom ponovno, največ trikrat. Za namene zaznave te napake se potrditev delnega sporočila šteje kot zahtevek, poslan VU.

▼B

DDP_028 IDE pred začetkom vsakega prenosa počaka najmanj obdobje P3min; obdobje čakanja se meri od zadnjega izračunanega pojava končnega bita po tem, ko je bila napaka zaznana.

Slika 3

Obravnava napak pri IDE



2.2.6 *Vsebina sporočila odziva*

Ta odstavek določa vsebino podatkovnih polj različnih sporočil pozitivnih odzivov.

Podatkovni elementi so opredeljeni v slovarju podatkov v Dodatku 1.

Opomba: pri prenosih podatkov druge generacije je vsak podatkovni element najvišje ravni predstavljen z nizom zapisov (*record array*), četudi vsebuje le en zapis. Niz zapisa se začne z glavo; ta glava vsebuje vrsto, velikost in število zapisov. Nizi zapisov so v naslednjih tabelah poimenovani kot '… RecordArray' (z glavo).

2.2.6.1 Positive Response Transfer Data Overview

DDP_029 Podatkovno polje *Positive Response Transfer Data Overview* vsebuje naslednje podatke v naslednjem zaporedju; pri čemer je SID 76 hex, TREP 01 hex; sporočilo je ustrezno razdeljeno na delna sporočila, ki so označena z zaporednimi številkami:

▼B

Struktura podatkov prve generacije

Podatkovni element	Opomba
MemberStateCertificate VUCertificate	Varnostni certifikat VU
VehicleIdentificationNumber VehicleRegistrationIdentification	Identifikacija vozila
CurrentDateTime	Trenutni datum in čas VU
VuDownloadablePeriod	Obdobje, ki se lahko prenese
CardSlotsStatus	Vrste kartic, vstavljene v VU
VuDownloadActivityData	Prejšnji prenos podatkov z VU
VuCompanyLocksData	Vse shranjene blokade s strani podjetja. Če je razdelek prazen, se pošlje le noOfLocks = 0.
VuControlActivityData	Vsi kontrolni zapisi, shranjeni v VU. Če je razdelek prazen, se pošlje le noOfControls = 0.
Signature	Podpis RSA vseh podatkov (razen certifikatov), ki se začnejo z VehicleIdentificationNumber in končajo z zadnjim bajtom zadnjega VuControlActivityData.

Struktura podatkov druge generacije

Podatkovni element	Opomba
MemberStateCertificateRecordArray	Certifikat države članice
VUCertificateRecordArray	Certifikat VU
VehicleIdentificationNumberRecordArray	Identifikacija vozila
VehicleRegistrationNumberRecordArray	Registrska številka vozila
CurrentDateTimeRecordArray	Trenutni datum in čas VU
VuDownloadablePeriodRecordArray	Obdobje, ki se lahko prenese
CardSlotsStatusRecordArray	Vrste kartic, vstavljene v VU
VuDownloadActivityDataRecordArray	Prejšnji prenos podatkov z VU
VuCompanyLocksRecordArray	Vse shranjene blokade s strani podjetja. Če je razdelek prazen, se pošlje le glava tabele z noOfRecords = 0.
VuControlActivityRecordArray	Vsi kontrolni zapisi, shranjeni v VU. Če je razdelek prazen, se pošlje le glava tabele z noOfRecords = 0.
SignatureRecordArray	Podpis ECC vseh predhodnih podatkov razen certifikatov.

2.2.6.2 Positive Response Transfer Data Activities

DDP_030 Podatkovno polje *Positive Response Transfer Data Activities* vsebuje naslednje podatke v naslednjem zaporedju; pri čemer je SID 76 hex, TREP 02 hex; sporočilo je ustrezno razdeljeno na delna sporočila, ki so označena z zaporednimi številkami:

▼B

Struktura podatkov prve generacije

Podatkovni element	Opomba
TimeReal	Datum dne, za katerega se prenesejo podatki
OdometerValueMidnight	Števec prevožene poti na koncu prenesenega dne
VuCardIWData	Podatki o številu ciklov vstavljanja in izvleka kartice. — Če ta razdelek ne vsebuje razpoložljivih podatkov, se pošlje le noOfVuCardIWRecords = 0. — Kadar VuCardIWRecord presega 00:00 (vstavitev kartice predhodnega dne) ali 24:00 (izvlek kartice naslednji dan), se prikaže v celoti za oba zajeta dneva.
VuActivityDailyData	Stanje rež ob 00:00 in zapisane spremembe dejavnosti za dan, za katerega se prenesejo podatki.
VuPlaceDailyWorkPeriodData	Zapisani podatki o krajih za dan, za katerega se prenesejo podatki. Če je razdelek prazen, se pošlje le noOfPlaceRecords = 0.
VuSpecificConditionData	Zapisani podatki o posebnih pogojih za dan, za katerega se prenesejo podatki. Če je razdelek prazen, se pošlje le noOfSpecificConditionRecords=0.
Signature	Podpis RSA vseh podatkov, ki se začnejo s TimeReal in končajo z zadnjim bajtom zadnjega zapisa posebnih pogojev.

Struktura podatkov druge generacije:

Podatkovni element	Opomba
DateOfDayDownloadedRecordArray	Datum dne, za katerega se prenesejo podatki
OdometerValueMidnightRecordArray	Števec prevožene poti na koncu prenesenega dne
VuCardIWRecordArray	Podatki o številu ciklov vstavljanja in izvleka kartice. — Če točka ne vsebuje razpoložljivih podatkov, se pošlje le glava tabele z noOfRecords = 0. — Kadar VuCardIWRecord presega 00:00 (vstavitev kartice predhodnega dne) ali 24:00 (izvlek kartice naslednji dan), se prikaže v celoti za oba zajeta dneva.
VuActivityDailyRecordArray	Stanje rež ob 00:00 in zapisane spremembe dejavnosti za dan, za katerega se prenesejo podatki.
VuPlaceDailyWorkPeriodRecordArray	Zapisani podatki o krajih za dan, za katerega se prenesejo podatki. Če je razdelek prazen, se pošlje le glava tabele z noOfRecords = 0.
VuGNSSCDRecordArray	Položaji GNSS vozila, kadar čas neprekinjene vožnje voznika doseže večkratnik treh ur. Če je razdelek prazen, se pošlje le glava tabele z noOfRecords = 0.
VuSpecificConditionRecordArray	Zapisani podatki o posebnih pogojih za dan, za katerega se prenesejo podatki. Če je razdelek prazen, se pošlje le glava tabele z noOfRecords = 0.
SignatureRecordArray	Podpis ECC vseh predhodnih podatkov.

▼B

2.2.6.3 Positive Response Transfer Data Events and Faults

DDP_031 Podatkovno polje sporočila *Positive Response Transfer Data Events and Faults* vsebuje naslednje podatke v naslednjem zaporedju; pri čemer je SID 76 hex, TREP 03 hex; sporočilo je ustrezno razdeljeno na delna sporočila, ki so označena z zaporednimi številkami:

Struktura podatkov prve generacije

Podatkovni element	Opomba
VuFaultData	Vse shranjene ali tekoče napake v VU. Če je razdelek prazen, se pošlje le noOfVuFaults = 0.
VuEventData	Vsi shranjeni ali tekoči dogodki v VU (razen prekoračitev hitrosti). Če je razdelek prazen, se pošlje le noOfVuEvents = 0.
VuOverSpeedingControlData	Podatki v zvezi z zadnjo kontrolo prekoračitev hitrosti (privzeta vrednost, če ni podatkov).
VuOverSpeedingEventData	Vse prekoračitve hitrosti, shranjene v VU. Če je razdelek prazen, se pošlje le noOfVuOverSpeedingEvents = 0.
VuTimeAdjustmentData	Vsi dogodki nastavljanja časa, shranjeni v VU (zunaj okvira polne kalibracije). Če je razdelek prazen, se pošlje le noOfVuTimeAdjRecords = 0.
Signature	Podpis RSA vseh podatkov, ki se začnejo z noOfVuFaults in končajo z zadnjim bajtom zadnjega zapisa nastavljanja časa.

Struktura podatkov druge generacije:

Podatkovni element	Opomba
VuFaultRecordArray	Vse shranjene ali tekoče napake v VU. Če je razdelek prazen, se pošlje le glava tabele z noOfRecords = 0.
VuEventRecordArray	Vsi shranjeni ali tekoči dogodki v VU (razen prekoračitev hitrosti). Če je razdelek prazen, se pošlje le glava tabele z noOfRecords = 0.
VuOverSpeedingControlDataRecordArray	Podatki v zvezi z zadnjo kontrolo prekoračitev hitrosti (privzeta vrednost, če ni podatkov).
VuOverSpeedingEventRecordArray	Vse prekoračitve hitrosti, shranjene v VU. Če je razdelek prazen, se pošlje le glava tabele z noOfRecords = 0.
VuTimeAdjustmentRecordArray	Vsi dogodki nastavljanja časa, shranjeni v VU (zunaj okvira polne kalibracije). Če je razdelek prazen, se pošlje le glava tabele z noOfRecords = 0.
VuTimeAdjustmentGNSSRecordArray	
SignatureRecordArray	Podpis ECC vseh predhodnih podatkov.

▼B

2.2.6.4 Positive Response Transfer Data Detailed Speed

DDP_032 Podatkovno polje sporočila *Positive Response Transfer Data Detailed Speed* vsebuje naslednje podatke v naslednjem vrstnem redu; SID je 76 hex, TREP 04 hex; sporočilo je ustrezno razdeljeno na delna sporočila, označena z zaporednimi številkami:

Struktura podatkov prve generacije

Podatkovni element	Opomba
VuDetailedSpeedData	Vsi podrobni podatki o hitrosti, shranjeni v VU (en hitrostni blok na minuto, ko se je vozilo premikalo). 60 hitrostnih vrednosti na minuto (ena na sekundo).
Signature	Podpis RSA vseh podatkov, ki se začnejo z noOfSpeedBlocks in končajo z zadnjim bajtom zadnjega hitrostnega bloka.

Struktura podatkov druge generacije:

Podatkovni element	Opomba
VuDetailedSpeedBlockRecordArray	Vsi podrobni podatki o hitrosti, shranjeni v VU (en hitrostni blok na minuto, ko se je vozilo premikalo). 60 hitrostnih vrednosti na minuto (ena na sekundo).
SignatureRecordArray	Podpis ECC vseh predhodnih podatkov.

2.2.6.5 Positive Response Transfer Data Technical Data

DDP_033 Podatkovno polje sporočila *Positive Response Transfer Data Technical Data* vsebuje naslednje podatke v naslednjem zaporedju; pri čemer je SID 76 hex, TREP 05 hex; sporočilo je ustrezno razdeljeno na delna sporočila, ki so označena z zaporednimi številkami:

Struktura podatkov prve generacije

Podatkovni element	Opomba
VuIdentification	
SensorPaired	
VuCalibrationData	Vsi zapisi o kalibraciji, shranjeni v VU.
Signature	Podpis RSA vseh podatkov, ki se začnejo z vuManufacturerName in končajo z zadnjim bajtom zadnjegaVuCalibrationRecord.

▼B

Struktura podatkov druge generacije:

Podatkovni element	Opomba
VuIdentificationRecordArray	
VuSensorPairedRecordArray	Vse povezave MS, shranjene v VU.
VuSensorExternalGNSSCoupledRecordArray	Vse povezave zunanje GNSS opreme, shranjene v VU.
VuCalibrationRecordArray	Vsi zapisi o kalibraciji, shranjeni v VU.
VuCardRecordArray	Vsi podatki o vstavitvi kartice, shranjeni v VU.
VuITSConsentRecordArray	
VuPowerSupplyInterruptionRecordArray	
SignatureRecordArray	Podpis ECC vseh predhodnih podatkov.

2.3. **Hramba datoteke na zunanjem pomnilniškem mediju (ESM)**

DDP_034 Kadar je bil med sejo prenosa podatkov opravljen tudi prenos podatkov iz VU, IDE v eno samo fizično datoteko shrani vse podatke iz sporočil *Positive Response Transfer Data*, prejete iz VU v tej seji prenosa. Shranjeni podatki ne vključujejo glave sporočil, števcev delnih sporočil, praznih delnih sporočil in kontrolne vsote, vključujejo pa SID in TREP (le za prvo delno sporočilo pri več delnih sporočilih).

3. PROTOKOL ZA PRENOS PODATKOV S TAHOGRAFSKIH KARTIC

3.1. **Področje uporabe**

Ta točka opisuje neposredni prenos podatkov s tahografske kartice v IDE. IDE ni del varnega okolja, zato se med IDE in kartico ne opravi avtentikacija.

3.2. **Opredelitve pojmov**

Seja prenosa podatkov: vsakič, ko se opravi prenos podatkov ICC. Seja zajema celotni postopek od ponastavitve ICC z IFD do deaktiviranja ICC (izvlek kartice ali naslednja ponastavitev).

Podpisana podatkovna datoteka: datoteka iz ICC. Datoteka se prenese v IFD kot golo besedilo. V ICC se izračuna zgoščena vrednost, datoteka se podpiše in podpis prenese v IFD:

3.3. **Prenos podatkov s kartice**

DDP_035 Prenos podatkov s tahografske kartice zajema naslednje korake:

— prenos skupnih podatkov kartice iz EF ICCin IC. Ti podatki niso obvezni in niso zavarovani z digitalnim podpisom.

▼B

— Prenos elementarnih datotek Card_Certificate (ali CardSignCertificate) in CA_Certificate. Ti podatki niso zavarovani z digitalnim podpisom.

Te datoteke se obvezno prenesejo v vsaki seji prenosa podatkov.

— Prenos drugih aplikativnih elementarnih datotek (v okviru Tachograph DF In Tachograph_G2 DF, če je ustrezno) razen Card_Download. Ti podatki so zavarovani z digitalnim podpisom.

— V vsaki seji prenosa podatkov se obvezno preneseta vsaj elementarni datoteki Application_Identificationin ID.

— Pri prenosu podatkov z vozniške kartice je obvezen tudi prenos naslednjih elementarnih datotek:

- Events_Data,
- Faults_Data,
- Driver_Activity_Data,
- Vehicles_Used,
- Places,
- GNSS_Places (if relevant),
- Control_Activity_Data,
- Specific_Conditions.

— Pri prenosu vozniške kartice se posodobi datum LastCardDownloadv EF Card_Download.

— Pri prenosu kartice servisne delavnice se ponastavi števec kalibracij v EF Card_Download.

— Pri prenosu kartice servisne delavnice se ne prenese EF Sensor_Installation_Data.

3.3.1 *Inicializacijsko zaporedje*

DDP_036 IDE zaporedje začne na naslednji način:

Kartica	Smer	IDE/IFD	Pomen/opombe
	⇦	Ponastavitev strojne opreme	
ATR	⇨		

PPS za preklop na višjo raven baudne hitrosti se lahko neobvezno uporabi, če jo ICC podpira.

3.3.2 *Zaporedje za nepodpisane podatkovne datoteke*

DDP_037 Zaporedje za prenos EF ICC, EF IC, EF Card_Certificate (ali EF CardSignCertificate) in EF CA_Certificate je naslednje:

Kartica	Smer	IDE/IFD	Pomen/opombe
	⇦	**Select File**	Izbira glede na identifikatorje datotek
OK	⇨		

▼B

Kartica	Smer	IDE/IFD	Pomen/opombe
	⇦	**Read Binary**	Če datoteka vsebuje več podatkov, kot je zmogljivost vmesnega pomnilnika čitalnika ali kartice, je ukaz treba ponavljati, dokler se ne prebere cela datoteka.
Podatki datoteke OK	⇨	Shranitev podatkov na ESM	v skladu s **3.4** Data storage format

Opomba 1: pred izbiro EF Card_Certificate (ali CardSignCertificate) je treba izbrati tahografsko aplikacijo (izbira z AID).

Opomba 2: z uporabo ukaza Read Binary in kratkega identifikatora EF se datoteka lahko izbere in prebere istočasno.

3.3.3 *Zaporedje za podpisane podatkovne datoteke*

DDP_038 Za vsako od naslednjih datotek, ki se prenesejo s svojim podpisom, se uporabi naslednje zaporedje:

Kartica	Dir	IDE/IFD	Pomen/opombe
	⇦	**Select File**	
OK	⇨		
	⇦	**Perform Hash of File**	Izračun zgoščene vrednosti vsebine podatkov z uporabo predpisanega zgoščevalnega algoritma v skladu z Dodatkom 11. Ta ukaz ni ISO ukaz.
Izračun Hash of File in začasna shranitev zgoščene vrednosti			
OK	⇨		
	⇦	**Read Binary**	Če datoteka vsebuje več podatkov, kot je zmogljivost vmesnega pomnilnika čitalnika ali kartice, je treba ukaz ponavljati, dokler se ne prebere celotna datoteka.
Podatki datoteke OK	⇨	Shranitev sprejetih podatkov na ESM	v skladu s **3.4** Data storage format

▼B

Kartica	Dir	IDE/IFD	Pomen/opombe
	⇦	**PSO: Compute Digital Signature**	
Izvedba varnostne operacije *Compute Digital Signature* z začasno shranjeno zgoščeno vrednostjo			
Podpis OK	⇨	Dopis podatkov k predhodno shranjenim podatkom na ESM	v skladu s **3.4** Data storage format

Opomba: z uporabo ukaza *Read Binary* in kratkega identifikatora EF se datoteka lahko izbere in prebere istočasno. V tem primeru se lahko EF izbere in prebere pred uporabo ukaza *Perform Hash of File*.

3.3.4 *Zaporedje za ponastavitev števca kalibracij*

DDP_039 Zaporedje za ponastavitev števca `NoOfCalibrationsSinceDownload` v `Card_Download` na kartici servisne delavnice je naslednje:

Kartica	Dir	IDE/IFD	Pomen/opombe
	⇦	**Izbira datoteke** EFCard_Download	Izbira glede na identifikatorje datotek
OK	⇨		
	⇦	**Update Binary** NoOfCalibrationsSinceDownload = ‘00 00’	
ponastavitev števila prenosov podatkov s kartice			
OK	⇨		

Opomba: izbira in posodobitev datoteke se lahko opravi istočasno z uporabo ukaza *Update Binary* in kratkega identifikatorja EF.

3.4. **Format hrambe podatkov**

3.4.1 *Uvod*

DDP_040 Preneseni podatki se shranijo na naslednji način:

— vsi podatki se shranijo transparentno. To pomeni, da se med hrambo ohrani zaporedje bajtov in zaporedje bitov v vsakem bajtu, v kakršnem so preneseni s kartice.

— vse datoteke, prenesene med sejo prenosa podatkov, se shranijo v eni datoteki ESM.

▼B

3.4.2 *Format datoteke*

DDP_041 Format datoteke je združitev več objektov TLV.

DDP_042 Oznako EF sestavljata FID in pripona ‘00’.

DDP_043 Oznako podpisa EF sestavljata FID datoteke in pripona ‘01’.

DDP_044 Dolžina je dvobajtna vrednost, ki jo opredeljuje število bajtov v polju vrednosti. Vrednost ‘FF FF’ v polju dolžine je rezervirana za prihodnje uporabe.

DDP_045 Če se datoteka ne prenese, se ne shrani nič v zvezi s to datoteko (niti oznaka niti ničelna dolžina).

DDP_046 Podpis se shrani kot naslednji objekt TLV neposredno za objektom TLV, ki vsebuje podatke datoteke.

Opredelitev	Pomen	Dolžina
FID (2 bajta) || ‘00’	Oznaka za EF (FID)	3 bajti
FID (2 bajta) || ‘01’	Oznaka za podpis EF (FID)	3 bajti
xx xx	Dolžina polja vrednosti	2 bajta

Primer podatkov v preneseni datoteki na ESM:

Oznaka	Dolžina	Vrednost
00 02 00	00 11	Podatki v EF ICC
C1 00 00	00 C2	Podatki v EF Card_Certificate
		…
05 05 00	0A 2E	Podatki v EF Vehicles_Used
05 05 01	00 80	Podpis EF Vehicles_Used

4. PRENOS PODATKOV S TAHOGRAFSKE KARTICE PREKO ENOTE V VOZILU

DDP_047 VU omogoča prenos vsebine vstavljene vozniške kartice v priključeno IDE.

DDP_048 IDE ta način začne tako, da pošlje sporočilo *Transfer Data Request Card Download* VU (glej 2.2.2.9).

DDP_049 VU nato po datotekah prenese celotno kartico v skladu s protokolom prenosa podatkov, opredeljenim v odstavku 3, in prepošlje IDE vse podatke, ki jih prejme s kartice, v ustreznem formatu datotek TLV in enkapsulirane v sporočilu *Positive Response Transfer Data* (glej 3.4.2).

▼B

DDP_050 IDE odčita podatke iz sporočila *Positive Response Transfer Data* (pri čemer odstrani vse glave, bajte SID in TREP, števce delnih sporočil in kontrolne vsote) in jih shrani v eno samo fizično datoteko, kakor je opisano v odstavku 2.3.

DDP_051 VU nato po potrebi posodobi datoteko `Control_Activity_Data` ali `Card_Download` na vozniški kartici.

▼B

Dodatek 8

KALIBRACIJSKI PROTOKOL

KAZALO

1. UVOD

2. POJMI, OPREDELITVE POJMOV IN REFERENCE

3. PREGLED STORITEV

3.1. Razpoložljive storitve

3.2. Kode odgovorov

4. KOMUNIKACIJSKE STORITVE

4.1. Storitev StartCommunication

4.2. Storitev StopCommunication

4.2.1 Opis sporočil

4.2.2 Format sporočil

4.2.3 Opredelitev parametrov

4.3. Storitev TesterPresent

4.3.1 Opis sporočil

4.3.2 Format sporočil

5. STORITVE UPRAVLJANJA

5.1. Storitev StartDiagnosticSession

5.1.1 Opis sporočil

5.1.2 Format sporočil

5.1.3 Opredelitev parametrov

5.2. Storitev SecurityAccess

5.2.1 Opis sporočil

5.2.2 Format sporočil – SecurityAccess – requestSeed

5.2.3 Format sporočil – SecurityAccess – sendKey

6. STORITVE PRENOSA PODATKOV

6.1. Storitev ReadDataByIdentifier

6.1.1 Opis sporočil

6.1.2 Format sporočil

6.1.3 Opredelitev parametrov

6.2. Storitev WriteDataByIdentifier

6.2.1 Opis sporočil

6.2.2 Format sporočil

6.2.3 Opredelitev parametrov

▼B

7. UPRAVLJANJE PRESKUSNIH IMPULZOV – FUNKCIONALNA ENOTA ZA UPRAVLJANJE VHODOV/IZHODOV

7.1. Storitev InputOutputControlByIdentifier

7.1.1 Opis sporočil

7.1.2 Format sporočil

7.1.3 Opredelitev parametrov

8. FORMATI DATARECORDS

8.1. Območja prenesenih parametrov

8.2. Formati dataRecords

1. UVOD

Ta dodatek opisuje, kako se izmenjujejo podatki med enoto v vozilu in preskuševalnikom po liniji K, ki je del kalibracijskega vmesnika, opisanega v Dodatku 6. Opisuje tudi upravljanje linije vhodno/izhodnih signalov na priključku za kalibracijo.

Vzpostavitev komunikacij po liniji K je opisana v oddelku 4 „Komunikacijske storitve“.

V tem dodatku je pri določanju obsega upravljanja linije K v različnih pogojih uporabljen koncept diagnostičnih „sej“. Privzeta vrsta seje je „StandardDiagnosticSession“, pri kateri je mogoče iz enote v vozilu brati vse podatke, vanjo pa podatkov ni mogoče vpisovati.

Izbira diagnostične seje je opisana v oddelku 5 „Storitve upravljanja“.

V skladu z zahtevami glede interoperabilnosti iz te uredbe je ta dodatek treba upoštevati kot relevanten za obe generaciji VU in kartic servisne delavnice.

CPR_001 Vnos podatkov v enoto v vozilu omogoča seja „ECUProgrammingSession“. Poleg tega mora biti enota v vozilu za vnos kalibracijskih podatkov v KALIBRACIJSKEM načinu delovanja.

Prenos podatkov po liniji K je opisan v oddelku 6 „Storitve prenosa podatkov“. Formati prenašanih podatkov so podrobno opisani v oddelku 8 „Formati dataRecords“.

CPR_002 Seja „ECUAdjustmentSession“ omogoča izbiro V/I načina kalibracijske V/I signalne linije preko vmesnika linije K. Upravljanje kalibracijske V/I signalne linije je opisano v oddelku 7 „Upravljanje preskusnih impulzov – funkcionalna enota za upravljanje vhodov/izhodov“.

CPR_003 V tem gradivu je naslov preskuševalnika vedno označen kot „tt“. Lahko se sicer uporabijo prednostni naslovi preskuševalnika, vendar se mora VU pravilno odzvati na vsak naslov preskuševalnika. Fizični naslov VU je 0xEE.

▼B

2. POJMI, OPREDELITVE POJMOV IN REFERENCE

Protokoli, sporočila in kode napak v glavnem temeljijo na osnutku standarda ISO 14229-1 (Road vehicles – Diagnostic systems – Part 1: Diagnostic services, različica 6 z dne 22. februarja 2001).

Pri identifikatorjih storitev, zahtevkih za storitve in odgovorih ter pri standardnih parametrih se uporabljajo kodiranje bajtov in šestnajstiške vrednosti.

Izraz „preskuševalnik“ se nanaša na opremo za vnos programskih/kalibracijskih vrednosti v VU.

Izraza „odjemalec“ in „strežnik“ se nanašata na preskuševalnik oziroma VU.

Izraz ECU pomeni „elektronska krmilna enota“ in se nanaša na VU.

Vir:

ISO 14230-2: Road Vehicles – Diagnostic Systems – Keyword Protocol 2000 – Part 2: Data Link Layer.

Prva izdaja: 1999.

Vozila – diagnostika.

3. PREGLED STORITEV

3.1. **Razpoložljive storitve**

Naslednja preglednica podaja pregled storitev, ki jih omogoča tahograf in so opredeljene v tem dokumentu.

CPR_004 V preglednici so prikazane storitve, ki so na voljo v omogočeni diagnostični seji:

— v **prvem stolpcu** so naštete možne storitve,

— v **drugem stolpcu** so podane številke oddelkov v tem dodatku, v katerih so storitve podrobneje opredeljene,

— v **tretjem stolpcu** so predpisane vrednosti identifikatorja storitve za sporočila zahtevkov,

— v **četrtem stolpcu** je predpisano, katere storitve mora vsaka VU izvesti v seji **„StandardDiagnosticSession“ (SD)**,

— v **petem stolpcu** so predpisane storitve v seji **„ECUAdjustmentSession“ (ECUAS)**, ki morajo biti izvedene za upravljanje V/I signalne linije preko priključka za kalibracijo na čelni plošči VU,

— v šestem stolpcu so predpisane storitve v seji „ECUProgrammingSession“ (ECUPS), ki morajo biti vgrajene za programiranje parametrov VU.

▼B

Preglednica 1

Zbirna preglednica vrednosti identifikatorjev storitev

			Diagnostične seje		
Naziv diagnostične seje	Oddelek	Vrednost zaht. 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		■	

■ Ta simbol označuje, da je storitev v zadevni diagnostični seji obvezna.
Če tega simbola ni, to pomeni, da ta storitev v zadevni diagnostični seji ni dovoljena.

3.2. **Kode odgovorov**

Za vsako storitev so opredeljene kode odgovorov.

4. KOMUNIKACIJSKE STORITVE

Vzpostavitev in vzdrževanje komunikacije zahtevata določene storitve. Te storitve ne nastopajo na ravni aplikacije. Razpoložljive storitve so podrobno opisane v naslednji preglednici:

Preglednica 2

Komunikacijske storitve

Naziv storitve	Opis
StartCommunication	Odjemalec zahteva začetek komunikacijske seje s strežnikom(-i).
StopCommunication	Odjemalec zahteva končanje trenutne komunikacijske seje.
TesterPresent	Odjemalec strežniku naznani, da je še vedno prisoten.

CPR_005 Komunikacija se začne s storitvijo StartCommunication. Za izvedbo kakršnekoli storitve mora biti komunikacija inicializirana in komunikacijski parametri morajo ustrezati želenemu načinu.

4.1. **Storitev StartCommunication**

CPR_006 Po sprejemu primitiva StartCommunication mora VU preveriti, ali je zahtevano komunikacijsko povezavo v sedanjem stanju mogoče inicializirati. Veljavni pogoji za inicializacijo komunikacijske povezave so opisani v standardu ISO 14230-2.

▼B

CPR_007 Nato VU opravi vse potrebno za inicializacijo komunikacijske povezave in pošlje primitiv odgovora StartCommunication z izbranimi pozitivnimi parametri odgovora.

CPR_008 Če je VU ob sprejemu novega zahtevka StartCommunication Request (npr. zaradi odprave napake v preskuševalniku) že inicializirana (in je že vstopila v kakšno diagnostično sejo), mora zahtevek sprejeti in se ponovno inicializirati.

CPR_009 Če komunikacijske povezave iz kakršnegakoli razloga ni mogoče inicializirati, mora VU nadaljevati delovanje, v katerem je bila tik pred poskusom inicializacije komunikacijske povezave.

CPR_010 Sporočilo StartCommunication Request mora biti fizično naslovljeno.

CPR_011 Inicializacija VU za storitve se opravi po postopku „hitre inicializacije“.

— Pred kakršnim koli dejanjem se pusti določen čas, v katerem je vodilo v mirujočem stanju.

— Preskuševalnik nato pošlje inicializacijski vzorec.

— Odgovor VU vsebuje vse informacije, potrebne za vzpostavitev komunikacije.

CPR_012 Po zaključku inicializacije:

— so vsi komunikacijski parametri nastavljeni na vrednosti iz preglednice 4 glede na bajte ključev,

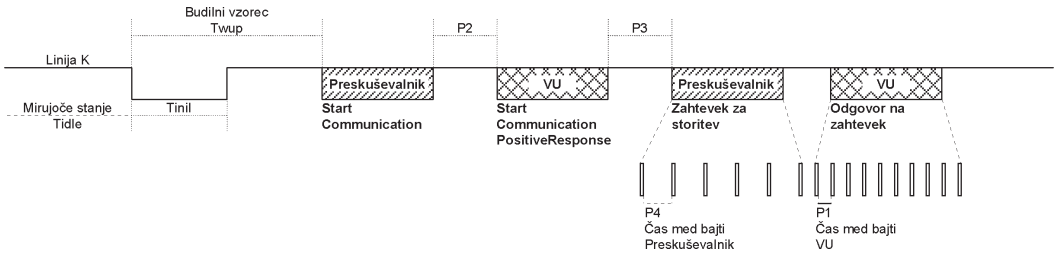
— VU čaka na prvi zahtevek iz preskuševalnika,

— je VU v privzetem diagnostičnem načinu, tj. v seji StandardDiagnosticSession,

— je kalibracijska V/I signalna linija v privzetem, tj. onemogočenem stanju.

CPR_014 Hitrost prenosa podatkov po liniji K je 10 400 Bd.

CPR_016 Preskuševalnik hitro inicializacijo sproži tako, da pošlje budilni vzorec (Wup) po liniji K. Vzorec se začne po preteku časa mirujočega stanja linije K, z nizko vrednostjo časa Tinil. Preskuševalnik pošlje prvi bit zahtevka za storitev StartCommunication po času Twup po prvem upadnem robu.



▼B

CPR_017 Časovne nastavitve za hitro inicializacijo in komunikacijo na splošno so prikazane v preglednicah v nadaljevanju. Čas mirujočega stanja ima lahko različne vrednosti:

— pri prvem prenosu po vklopu napajanja: Tidle = 300 ms;

— po zaključku storitve StopCommunication: Tidle = P3 min;

— po koncu komunikacije zaradi preteka časovne omejitve P3 max: Tidle = 0.

Preglednica 3

Časovne vrednosti za hitro inicializacijo

Parameter		Najmanjša vrednost (min)	Največja vrednost (max)
Tinil	25 ± 1 ms	24 ms	26 ms
Twup	50 ± 1 ms	49 ms	51 ms

Preglednica 4

Časovne vrednosti za komunikacijo

Časovni razpored Parameter	Opis parametra	spodnje mejne vrednosti [ms]	zgornje mejne vrednosti [ms]
		min.	max.
P1	čas med bajti odgovora VU	0	20
P2	čas med zahtevkom preskuševalnika in odgovorom VU ali med dvema odgovoroma VU	25	250
P3	čas med koncem odgovora VU in začetkom novega zahtevka preskuševalnika	55	5 000
P4	čas med bajti za zahtevek preskuševalnika	5	20

CPR_018 Format sporočil pri hitri inicializaciji je podrobno opisan v naslednjih preglednicah. (OPOMBA: Hex pomeni „šestnajstiška“)

Preglednica 5

Sporočilo StartCommunication Request

Št. bajta	Naziv parametra	Hex vrednost	Mnemonik
#1	Formatni bajt – fizično naslavljanje	81	FMT
#2	Bajt ciljnega naslova	EE	TGT
#3	Bajt izvornega naslova	tt	SRC

▼B

Št. bajta	Naziv parametra	Hex vrednost	Mnemonik
#4	**StartCommunication Request Service Id**	**81**	**SCR**
#5	Kontrolna vsota	00-FF	CS

Preglednica 6

Sporočilo StartCommunication Positive Response

Št. bajta	Naziv parametra	Hex vrednost	Mnemonik
#1	Formatni bajt – fizično naslavljanje	80	FMT
#2	Bajt ciljnega naslova	tt	TGT
#3	Bajt izvornega naslova	EE	SRC
#4	Dodatni bajt dolžine	03	LEN
#5	**StartCommunication Positive Response Service Id**	**C1**	**SCRPR**
#6	Bajt ključa 1	EA	KB1
#7	Bajt ključa 2	8F	KB2
#8	Kontrolna vsota	00-FF	CS

CPR_019 Na sporočilo zahtevka StartCommunication Request ni negativnega odgovora; če VU ne more poslati pozitivnega odgovora, se ne inicializira, ne sporoči ničesar in ostane v svojem normalnem delovanju.

4.2. **Storitev StopCommunication**

4.2.1 *Opis sporočil*

Namen te storitve na komunikacijski ravni je končati komunikacijsko sejo.

CPR_020 Po sprejemu primitiva StopCommunication VU preveri, ali je zahtevano komunikacijsko povezavo v sedanjem stanju mogoče končati. V tem primeru VU opravi vse za končanje te komunikacije.

CPR_021 Če je komunikacijo mogoče končati, VU pred koncem komunikacije pošlje primitiv odgovora StopCommunication s pozitivnimi parametri odgovora.

CPR_022 Če komunikacije iz kakršnega koli razloga ni mogoče končati, VU pošlje primitiv odgovora StopCommunication z negativnimi parametri odgovora.

CPR_023 Če VU zazna pretek časovne omejitve P3 max, konča komunikacijo, ne da bi poslala kakršenkoli primitiv odgovora.

▼B

4.2.2 *Format sporočil*

CPR_024 Formati sporočil pri primitivih StopCommunication so podrobno opisani v naslednjih preglednicah.

Preglednica 7

Sporočilo StopCommunication Request

Št. bajta	Naziv parametra	Hex vrednost	Mnemonik
#1	Formatni bajt – fizično naslavljanje	80	FMT
#2	Bajt ciljnega naslova	EE	TGT
#3	Bajt izvornega naslova	tt	SRC
#4	Dodatni bajt dolžine	01	LEN
#5	**StopCommunication Request Service Id**	**82**	**SPR**
#6	Kontrolna vsota	00-FF	CS

Preglednica 8

Sporočilo StopCommunication Positive Response

Št. bajta	Naziv parametra	Hex vrednost	Mnemonik
#1	Formatni bajt – fizično naslavljanje	80	FMT
#2	Bajt ciljnega naslova	tt	TGT
#3	Bajt izvornega naslova	EE	SRC
#4	Dodatni bajt dolžine	01	LEN
#5	**StopCommunication Positive Response Service Id**	**C2**	**SPRPR**
#6	Kontrolna vsota	00-FF	CS

Preglednica 9

Sporočilo StopCommunication Negative Response

Št. bajta	Naziv parametra	Hex vrednost	Mnemonik
#1	Formatni bajt – fizično naslavljanje	80	FMT
#2	Bajt ciljnega naslova	tt	TGT
#3	Bajt izvornega naslova	EE	SRC
#4	Dodatni bajt dolžine	03	LEN

▼B

Št. bajta	Naziv parametra	Hex vrednost	Mnemonik
#5	**negative Response Service Id**	**7F**	**NR**
#6	StopCommunication Request Service Identification	82	SPR
#7	responseCode = generalReject	10	RC_GR
#8	Kontrolna vsota	00-FF	CS

4.2.3 *Opredelitev parametrov*

Ta storitev ne zahteva nobene opredelitve parametrov.

4.3. **Storitev TesterPresent**

4.3.1 *Opis sporočil*

Storitev TesterPresent sproži preskuševalnik, z njo pa sporoči strežniku, da je še vedno prisoten, in tako prepreči, da bi se strežnik samodejno vrnil v svoje normalno delovanje in morda končal komunikacijo. Ta storitev, ki se pošilja redno, ohranja diagnostično sejo/komunikacijo, saj vsak sprejem zahtevka te storitve ponastavi časovnik P3.

4.3.2 *Format sporočil*

CPR_079 Formati sporočil pri primitivih TesterPresent so podrobno opisani v naslednjih preglednicah.

Preglednica 10

Sporočilo TesterPresent Request

Št. bajta	Naziv parametra	Hex vrednost	Mnemonik
#1	Formatni bajt – fizično naslavljanje	80	FMT
#2	Bajt ciljnega naslova	EE	TGT
#3	Bajt izvornega naslova	tt	SRC
#4	Dodatni bajt dolžine	02	LEN
#5	**StopCommunication Request Service Id**	**3E**	**TP**
#6	Sub Function = [yes responseRequired = no]	01 02	RESPREQ_Y RESPREQ_NO
#7	Kontrolna vsota	00-FF	CS

CPR_080 Če je parameter responseRequired nastavljen na „yes“, mora strežnik odgovoriti z naslednjim sporočilom pozitivnega odgovora. Če je nastavljen na „no“, strežnik ne pošlje nobenega odgovora.

▼B

Preglednica 11

Sporočilo TesterPresent Positive Response

Št. bajta	Naziv parametra	Hex vrednost	Mnemonik
#1	Formatni bajt – fizično naslavljanje	80	FMT
#2	Bajt ciljnega naslova	tt	TGT
#3	Bajt izvornega naslova	EE	SRC
#4	Dodatni bajt dolžine	01	LEN
#5	**TesterPresent Positive Response Service Id**	**7E**	**TPPR**
#6	Kontrolna vsota	00-FF	CS

CPR_081 Ta storitev podpira naslednje kode negativnih odgovorov:

Preglednica 12

Sporočilo TesterPresent Negative Response

Št. bajta	Naziv parametra	Hex vrednost	Mnemonik
#1	Formatni bajt – fizično naslavljanje	80	FMT
#2	Bajt ciljnega naslova	tt	TGT
#3	Bajt izvornega naslova	EE	SRC
#4	Dodatni bajt dolžine	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	Kontrolna vsota	00-FF	CS

▼B

5. STORITVE UPRAVLJANJA

Razpoložljive storitve so podrobno opisane v naslednji preglednici:

Preglednica 13

Storitve upravljanja

Naziv storitve	Opis
StartDiagnosticSession	Odjemalec zahteva začetek diagnostične seje z VU.
SecurityAccess	Odjemalec zahteva dostop do funkcij, do katerih lahko dostopajo le pooblaščeni uporabniki.

5.1. **Storitev StartDiagnosticSession**

5.1.1 *Opis sporočil*

CPR_025 Storitev StartDiagnosticSession se uporablja, da se v strežniku omogočijo različne diagnostične seje. Diagnostična seja omogoči določen nabor storitev v skladu s preglednico 17. Seja lahko omogoči tudi posebne storitve, ki jih določi proizvajalec vozila, vendar niso opisane v tem dokumentu. Pravila izvedbe izpolnjujejo naslednje zahteve:

— v VU mora biti ves čas aktivna natanko ena diagnostična seja;

— ob vklopu napajanja mora VU vedno začeti sejo StandardDiagnosticSession. Če ni sprožena nobena druga diagnostična seja, seja StandardDiagnosticSession teče, dokler je vključeno napajanje VU;

— če preskuševalnik zahteva začetek določene diagnostične seje, ki že teče, VU pošlje sporočilo pozitivnega odgovora;

— kadar koli preskuševalnik zahteva novo diagnostično sejo, pred aktiviranjem te nove seje v VU ta vedno pošlje sporočilo pozitivnega odgovora StartDiagnosticSession. Če VU ne more začeti zahtevane nove diagnostične seje, pošlje sporočilo negativnega odgovora StartDiagnosticSession in nadaljuje tekočo sejo.

CPR_026 Diagnostična seja se začne samo, če je med odjemalcem in VU že vzpostavljena komunikacija.

CPR_027 Po uspešni storitvi StartDiagnosticSession morajo biti časovne nastavitve iz preglednice 4 aktivne, parameter diagnosticSession pa v sporočilu zahtevka nastavljen na „StandardDiagnosticSession“, če je bila prej aktivna kakšna druga diagnostična seja.

5.1.2 *Format sporočil*

CPR_028 Formati sporočil pri primitivih StartDiagnosticSession so podrobno opisani v naslednjih preglednicah.

▼B

Preglednica 14

Sporočilo StartDiagnosticSession Request

Št. bajta	Naziv parametra	Hex vrednost	Mnemonik
#1	Formatni bajt – fizično naslavljanje	80	FMT
#2	Bajt ciljnega naslova	EE	TGT
#3	Bajt izvornega naslova	tt	SRC
#4	Dodatni bajt dolžine	02	LEN
#5	**StartDiagnosticSession Request Service Id**	**10**	**STDS**
#6	diagnosticSession = [ena od vrednosti iz preglednice 17]	xx	DS_…
#7	Kontrolna vsota	00-FF	CS

Preglednica 15

Sporočilo StartDiagnosticSession Positive Response

Št. bajta	Naziv parametra	Hex vrednost	Mnemonik
#1	Formatni bajt – fizično naslavljanje	80	FMT
#2	Bajt ciljnega naslova	tt	TGT
#3	Bajt izvornega naslova	EE	SRC
#4	Dodatni bajt dolžine	02	LEN
#5	**StartDiagnosticSession Positive Response Service Id**	**50**	**STDSPR**
#6	diagnosticSession = [enaka vrednost kot v bajtu #6 v preglednici 14]	xx	DS_…
#7	Kontrolna vsota	00-FF	CS

Preglednica 16

Sporočilo StartDiagnosticSession Negative Response

Št. bajta	Naziv parametra	Hex vrednost	Mnemonik
#1	Formatni bajt – fizično naslavljanje	80	FMT
#2	Bajt ciljnega naslova	tt	TGT
#3	Bajt izvornega naslova	EE	SRC

▼B

Št. bajta	Naziv parametra		Hex vrednost	Mnemonik
#4	Dodatni bajt dolžine		03	LEN
#5	**Negative Response Service Id**		**7F**	**NR**
#6	StartDiagnosticSession Request Service Id		10	STDS
#7	ResponseCode =	[subFunctionNot-Supported ([a])	12	RC_SFNS
		incorrectMessage-Length ([b])	13	RC_IML
		conditionsNotCor-rect ([c])	22	RC_CNC
#8	Kontrolna vsota		00-FF	CS

([a]) – vrednost, vstavljena v bajt #6 sporočila z zahtevkom, ni podprta, tj. je ni v preglednici 17,
([b]) – dolžina sporočila je napačna,
([c]) – merila za zahtevek StartDiagnosticSession niso izpolnjena.

5.1.3 *Opredelitev parametrov*

CPR_029 Storitev StartDiagnosticSession za izbiro posebnega vedenja strežnika(-ov) uporablja parameter ***diagnosticSession (DS_)***. V tem dokumentu so opredeljene naslednje diagnostične seje:

Preglednica 17

Opredelitev vrednosti diagnosticSession

Hex	Opis	Mnemonik
81	**StandardDiagnosticSession** Ta diagnostična seja omogoča vse storitve iz **4. stolpca („SD“) preglednice 1**. Te storitve omogočajo branje podatkov s strežnika (VU). Ta diagnostična seja se aktivira po uspešno zaključeni inicializaciji med odjemalcem (preskuševalnikom) in strežnikom (VU). To diagnostično sejo lahko nadomestijo druge diagnostične seje, opredeljene v tem oddelku.	**SD**
85	**ECUProgrammingSession** Ta diagnostična seja omogoča vse storitve iz **6. stolpca („ECUPS“) preglednice 1**. Te storitve podpirajo programiranje pomnilnika strežnika (VU). To diagnostično sejo lahko nadomestijo druge diagnostične seje, opredeljene v tem oddelku.	**ECUPS**

▼B

Hex	Opis	Mnemonik
87	**ECUAdjustmentSession** Ta diagnostična seja omogoča vse storitve iz **5. stolpca („ECUAS“) preglednice 1.** Te storitve podpirajo upravljanje vhodov/izhodov strežnika (VU). To diagnostično sejo lahko nadomestijo druge diagnostične seje, opredeljene v tem oddelku.	**ECUAS**

5.2. **Storitev SecurityAccess**

Če VU ni v KALIBRACIJSKEM načinu, vpisovanje kalibracijskih parametrov ni mogoče. Pred odobritvijo vstopa v KALIBRACIJSKI način je treba poleg vstavitve veljavne kartice servisne delavnice v VU tudi vnesti ustrezen PIN v VU.

Če je VU v KALIBRACIJSKEM ali NADZORNEM načinu, je omogočen tudi dostop do kalibracijske vhodno/izhodne linije.

Storitev SecurityAccess omogoča uporabniku vnesti PIN, preskuševalniku pa ugotoviti, ali je VU v KALIBRACIJSKEM načinu ali ne.

Dopustno je tudi, da se omogoči vnos PIN na kakšen drug način.

5.2.1 *Opis sporočil*

Storitev SecurityAccess obsega sporočilo SecurityAccess „requestSeed“, ki mu nato lahko sledi sporočilo SecurityAccess „sendKey“. Storitev SecurityAccess se mora izvesti po storitvi StartDiagnosticSession.

CPR_033 Preskuševalnik uporabi sporočilo SecurityAccess „requestSeed“ za to, da preveri, ali je enota v vozilu pripravljena na sprejem PIN.

CPR_034 Če je enota v vozilu že v KALIBRACIJSKEM načinu, na zahtevek odgovori tako, da pošlje „seme“ 0x0000 s storitvijo SecurityAccess Positive Response.

CPR_035 Če je enota pripravljena na sprejem PIN za verifikacijo s pomočjo kartice servisne delavnice, na zahtevek odgovori tako, da pošlje „seme“, katerega vrednost je večja od 0x0000, s storitvijo SecurityAccess Positive Response.

CPR_036 Če enota v vozilu ni pripravljena na sprejem PIN od preskuševalnika, bodisi ker vstavljena kartica servisne delavnice ni veljavna, ali ker kartica servisne delavnice ni vstavljena, ali ker enota v vozilu pričakuje vnos PIN na kakšen drug način, na zahtevek odgovori z negativnim odgovorom (Negative Response) s kodo odgovora conditionsNotCorrectOrRequestSequenceError.

CPR_037 Preskuševalnik nato morda uporabi sporočilo SecurityAccess „sendKey“ za posredovanje PIN enoti v vozilu. Da zagotovi zadosten čas za izvedbo procesa avtentikacije kartice, VU podaljša čas za odgovor z negativnim odgovorom s kodo requestCorrectlyReceived-ResponsePending. Vendar je čas za odgovor največ 5 minut. Takoj po izvršitvi

▼B

zahtevane storitve VU pošlje sporočilo pozitivnega odgovora ali sporočilo negativnega odgovora z drugačno kodo. VU lahko ponavlja negativne odgovore s kodo requestCorrectlyReceived-ResponsePending, dokler se ne izvrši zahtevana storitev, nato pa pošlje končno sporočilo odgovora.

CPR_038 Enota v vozilu odgovori na ta zahtevek s storitvijo SecurityAccess Positive Response samo, kadar je v KALIBRACIJSKEM načinu.

CPR_039 V naslednjih primerih enota v vozilu odgovori na ta zahtevek z negativnim odgovorom, pri čemer je koda odgovora:

— subFunctionNot supported: nepravilen format parametra podfunkcije (accessType),

— conditionsNotCorrectOrRequestSequenceError: enota v vozilu ni pripravljena na vnos PIN,

— invalidKey: PIN ni veljaven in število dovoljenih poskusov vnosa PIN še ni preseženo,

— exceededNumberOfAttempts: PIN ni veljaven in število dovoljenih poskusov vnosa PIN je preseženo,

— generalReject: PIN pravilen, vendar medsebojna avtentikacija s kartico servisne delavnice ni uspela.

5.2.2 *Format sporočil – SecurityAccess – requestSeed*

CPR_040 Formati sporočil pri primitivih SecurityAccess „requestSeed“ so podrobno opisani v naslednjih preglednicah.

Preglednica 18

Sporočilo SecurityAccess Request – requestSeed

Št. bajta	Naziv parametra	Hex vrednost	Mnemonik
#1	Formatni bajt – fizično naslavljanje	80	FMT
#2	Bajt ciljnega naslova	EE	TGT
#3	Bajt izvornega naslova	tt	SRC
#4	Dodatni bajt dolžine	02	LEN
#5	**SecurityAccess Request Service Id**	**27**	**SA**
#6	accessType – requestSeed	7D	AT_RSD
#7	Kontrolna vsota	00-FF	CS

▼B

Preglednica 19

Sporočilo SecurityAccess – requestSeed Positive Response

Št. bajta	Naziv parametra	Hex vrednost	Mnemonik
#1	Formatni bajt – fizično naslavljanje	80	FMT
#2	Bajt ciljnega naslova	tt	TGT
#3	Bajt izvornega naslova	EE	SRC
#4	Dodatni bajt dolžine	04	LEN
#5	**SecurityAccess Positive Response Service Id**	**67**	**SAPR**
#6	accessType – requestSeed	7D	AT_RSD
#7	Visoka vrednost semena	00-FF	SEEDH
#8	Nizka vrednost semena	00-FF	SEEDL
#9	Kontrolna vsota	00-FF	CS

Preglednica 20

Sporočilo SecurityAccess Negative Response

Št. bajta	Naziv parametra	Hex vrednost	Mnemonik
#1	Formatni bajt – fizično naslavljanje	80	FMT
#2	Bajt ciljnega naslova	tt	TGT
#3	Bajt izvornega naslova	EE	SRC
#4	Dodatni bajt dolžine	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	Kontrolna vsota	00-FF	CS

▼B

5.2.3 *Format sporočil – SecurityAccess – sendKey*

CPR_041 Formati sporočil pri primitivih SecurityAccess „sendKey“ so podrobno opisani v naslednjih preglednicah.

Preglednica 21

Sporočilo SecurityAccess Request – sendKey

Št. bajta	Naziv parametra	Hex vrednost	Mnemonik
#1	Formatni bajt – fizično naslavljanje	80	FMT
#2	Bajt ciljnega naslova	EE	TGT
#3	Bajt izvornega naslova	tt	SRC
#4	Dodatni bajt dolžine	m+2	LEN
#5	**SecurityAccess Request Service Id**	**27**	**SA**
#6	accessType – sendKey	7E	AT_SK
#7 do #m + 6	Ključ #1 (visoka vrednost) … ključ #m (nizka vrednost, najmanj 4 in največ 8)	xx … xx	KEY
#m+7	Kontrolna vsota	00-FF	CS

Preglednica 22

Sporočilo SecurityAccess – sendKey Positive Response

Št. bajta	Naziv parametra	Hex vrednost	Mnemonik
#1	Formatni bajt – fizično naslavljanje	80	FMT
#2	Bajt ciljnega naslova	tt	TGT
#3	Bajt izvornega naslova	EE	SRC
#4	Dodatni bajt dolžine	02	LEN
#5	**SecurityAccess Positive Response Service Id**	**67**	**SAPR**
#6	accessType – sendKey	7E	AT_SK
#7	Kontrolna vsota	00-FF	CS

▼B

Preglednica 23

Sporočilo SecurityAccess Negative Response

Št. bajta	Naziv parametra		Hex vrednost	Mnemonik
#1	Formatni bajt – fizično naslavljanje		80	FMT
#2	Bajt ciljnega naslova		tt	TGT
#3	Bajt izvornega naslova		EE	SRC
#4	Dodatni bajt dolžine		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	Kontrolna vsota		00-FF	CS

6. STORITVE PRENOSA PODATKOV

Razpoložljive storitve so podrobno opisane v naslednji preglednici:

Preglednica 24

Storitve prenosa podatkov

Naziv storitve	Opis
ReadDataByIdentifier	Odjemalec zahteva prenos sedanje vrednosti zapisa, do katerega dostopa recordDataIdentifier.
WriteDataByIdentifier	Odjemalec zahteva vpis zapisa, do katerega dostopa recordDataIdentifier.

▼B

6.1. **Storitev ReadDataByIdentifier**

6.1.1 *Opis sporočil*

CPR_050 Storitev ReadDataByIdentifier odjemalec uporabi za to, da od strežnika zahteva vrednosti podatkovnih zapisov. Podatke določa recordDataIdentifier. Proizvajalec VU odgovarja za to, da so med izvajanjem te storitve izpolnjeni pogoji na strežniku.

6.1.2 *Format sporočil*

CPR_051 Formati sporočil pri primitivih ReadDataByIdentifier so podrobno opisani v naslednjih preglednicah.

Preglednica 25

Sporočilo ReadDataByIdentifier Request

Št. bajta	Naziv parametra	Hex vrednost	Mnemonik
#1	Formatni bajt – fizično naslavljanje	80	FMT
#2	Bajt ciljnega naslova	EE	TGT
#3	Bajt izvornega naslova	tt	SRC
#4	Dodatni bajt dolžine	03	LEN
#5	**ReadDataByIdentifier Request Service Id**	**22**	**RDBI**
#6 do #7	recordDataIdentifier = [vrednost iz preglednice 28]	xxxx	RDI_…
#8	Kontrolna vsota	00-FF	CS

Preglednica 26

Sporočilo ReadDataByIdentifier Positive Response

Št. bajta	Naziv parametra	Hex vrednost	Mnemonik
#1	Formatni bajt – fizično naslavljanje	80	FMT
#2	Bajt ciljnega naslova	tt	TGT
#3	Bajt izvornega naslova	EE	SRC
#4	Dodatni bajt dolžine	m+3	LEN
#5	**ReadDataByIdentifier Positive Response Service Id**	**62**	**RDBIPR**
#6 in #7	recordDataIdentifier = [enaka vrednost kot v bajtih #6 in #7 v preglednici 25]	xxxx	RDI_…

▼B

Št. bajta	Naziv parametra		Hex vrednost	Mnemonik
#8 do #m + 7	dataRecord[] =	[data#1	xx	DREC_DATA1
		:	:	:
		data#m]	xx	DREC_DATAm
#m+8	Kontrolna vsota		00-FF	CS

Preglednica 27

Sporočilo ReadDataByIdentifier Negative Response

Št. bajta	Naziv parametra		Hex vrednost	Mnemonik
#1	Formatni bajt – fizično naslavljanje		80	FMT
#2	Bajt ciljnega naslova		tt	TGT
#3	Bajt izvornega naslova		EE	SRC
#4	Dodatni bajt dolžine		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	Kontrolna vsota		00-FF	CS

6.1.3 *Opredelitev parametrov*

CPR_052 Parameter ***recordDataIdentifier (RDI_)*** v sporočilu zahtevka ReadDataByIdentifier določa podatkovni zapis.

CPR_053 Vrednosti parametra recordDataIdentifier, opredeljene v tem dokumentu, so prikazane v spodnji preglednici.

Preglednica parametrov recordDataIdentifier obsega štiri stolpce in več vrstic.

— V **prvem stolpcu („Hex“)** so podane šestnajstiške vrednosti, dodeljene parametrom recordDataIdentifier, ki so določeni v tretjem stolpcu.

— **Drugi stolpec („Podatkovni element“)** prikazuje podatkovne elemente iz Dodatka 1, na katerih temelji parameter recordDataIdentifier (v nekaterih primerih je potrebno prekodiranje).

▼B

— **Tretji stolpec („Opis“)** prikazuje naziv ustreznega parametra recordDataIdentifier.

— **Četrti stolpec („Mnemonik“)** prikazuje mnemonik tega parametra.

Preglednica 28

Opredelitev vrednosti recordDataIdentifier

Hex	Podatkovni element	Naziv parametra recordDataIdentifier (gl. format v oddelku 8.2)	Mnemonik
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 Parameter ***dataRecord (DREC_)*** se pošlje s sporočilom pozitivnega odgovora ReadDataByIdentifier in odjemalcu (preskuševalniku) podaja vrednost podatkovnega zapisa, ki ga določa parameter recordDataIdentifier. Formati podatkov so določeni v oddelku 8. Lahko se izvajajo tudi drugi neobvezni parametri dataRecords, npr. vhodni, notranji in izhodni podatki, specifični za posamezno VU, vendar v tem dokumentu niso opredeljeni.

6.2. Storitev WriteDataByIdentifier

6.2.1 *Opis sporočil*

CPR_056 Storitev WriteDataByIdentifier odjemalec uporabi za to, da v strežnik zapiše vrednosti podatkovnih zapisov. Podatke določa recordDataIdentifier. Proizvajalec VU odgovarja za to, da so med izvajanjem te storitve izpolnjeni pogoji na strežniku. Za posodobitev parametrov iz preglednice 28 mora biti VU v KALIBRACIJSKEM načinu.

6.2.2 *Format sporočil*

CPR_057 Formati sporočil pri primitivih WriteDataByIdentifier so podrobno opisani v naslednjih preglednicah.

▼B

Preglednica 29

Sporočilo WriteDataByIdentifier Request

Št. bajta	Naziv parametra	Hex vrednost	Mnemonik
#1	Formatni bajt – fizično naslavljanje	80	FMT
#2	Bajt ciljnega naslova	EE	TGT
#3	Bajt izvornega naslova	tt	SRC
#4	Dodatni bajt dolžine	m + 3	LEN
#5	**WriteDataByIdentifier Request Service Id**	**2E**	**WDBI**
#6 do #7	recordDataIdentifier = [vrednost iz preglednice 28]	xxxx	RDI_…
#8 do #m + 7	dataRecord[] = [data#1 : data#m]	xx : xx	DREC_ DATA1 : DREC_ DATAm
#m+8	Kontrolna vsota	00-FF	CS

Preglednica 30

Sporočilo WriteDataByIdentifier Positive Response

Št. bajta	Naziv parametra	Hex vrednost	Mnemonik
#1	Formatni bajt – fizično naslavljanje	80	FMT
#2	Bajt ciljnega naslova	tt	TGT
#3	Bajt izvornega naslova	EE	SRC
#4	Dodatni bajt dolžine	03	LEN
#5	**WriteDataByIdentifier Positive Response Service Id**	**6E**	**WDBIPR**
#6 do #7	recordDataIdentifier = [enaka vrednost kot v bajtih #6 in #7 v preglednici 29]	xxxx	RDI_…
#8	Kontrolna vsota	00-FF	CS

▼B

Preglednica 31

Sporočilo WriteDataByIdentifier Negative Response

Št. bajta	Naziv parametra	Hex vrednost	Mnemonik
#1	Formatni bajt – fizično naslavljanje	80	FMT
#2	Bajt ciljnega naslova	tt	TGT
#3	Bajt izvornega naslova	EE	SRC
#4	Dodatni bajt dolžine	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	Kontrolna vsota	00-FF	CS

6.2.3 *Opredelitev parametrov*

Parameter ***recordDataIdentifier (RDI_)*** je opredeljen v preglednici 28.

Parameter ***dataRecord (DREC_)*** se pošlje s sporočilom z zahtevkom WriteDataByIdentifier in strežniku (VU) podaja vrednost podatkovnega zapisa, ki ga določa parameter recordDataIdentifier. Formati podatkov so določeni v oddelku 8.

7. UPRAVLJANJE PRESKUSNIH IMPULZOV – FUNKCIONALNA ENOTA ZA UPRAVLJANJE VHODOV/IZHODOV

Razpoložljive storitve so podrobno opisane v naslednji preglednici:

Preglednica 32

Funkcionalna enota za upravljanje vhodov/izhodov

Naziv storitve	Opis
InputOutputControlByIdentifier	Odjemalec strežniku pošlje zahtevo za upravljanje določenega vhoda/izhoda.

7.1. **Storitev InputOutputControlByIdentifier**

7.1.1 *Opis sporočil*

Po zvezi preko konektorja na čelni plošči je mogoče z ustreznim preskuševalnikom upravljati ali nadzirati preskusne impulze.

▼B

CPR_058 To kalibracijsko V/I signalno linijo se lahko konfigurira z ukazom za linijo K s storitvijo InputOutputControlByIdentifier; s tem se izbere želeno vhodno ali izhodno funkcijo linije. Možna stanja linije so:

— disabled (onemogočena),

— speedSignalInput, pri čemer se kalibracijska V/I signalna linija uporablja za vnos signala hitrosti (preskusnega signala), ki nadomešča signal tipala gibanja – ta funkcija ni na voljo v NADZORNEM načinu,

— realTimeSpeedSignalOutputSensor, pri čemer se kalibracijska V/I signalna linija uporablja za iznos signala hitrosti tipala gibanja,

— RTCOutput, pri čemer se kalibracijska V/I signalna linija uporablja za iznos urnega signala UTC – ta funkcija ni na voljo v NADZORNEM načinu.

CPR_059 Enota v vozilu mora biti za konfiguracijo stanja linije v nastavitveni seji in v KALIBRACIJSKEM ali NADZORNEM načinu. Kadar je VU v KALIBRACIJSKEM načinu, se lahko izbere katero koli od štirih stanj linije (disabled, speedSignalInput, realTimeSpeedSignalOutputSensor, RTCOutput). Kadar je VU v NADZORNEM načinu, se lahko izbere le eno od dveh stanj linije (disabled, realTimeSpeedSignalOutputSensor). Ob izstopu iz nastavitvene seje ali iz KALIBRACIJSKEGA načina mora enota v vozilu zagotoviti vrnitev kalibracijske V/I signalne linije v „onemogočeno“ (privzeto) stanje.

CPR_060 Če VU prejme impulze hitrosti po normalni vhodni signalni liniji, pri tem ko je kalibracijska V/I signalna linija nastavljena na stanje vhoda, mora kalibracijsko V/I signalno linijo nastaviti v stanje izhoda ali vrniti v onemogočeno stanje.

CPR_061 Zaporedje je naslednje:

— vzpostavitev komunikacij s storitvijo StartCommunication;

— vstop v nastavitveno sejo s storitvijo StartDiagnosticSession in vstop v KALIBRACIJSKI ali NADZORNI način delovanja (zaporedje teh dveh vstopov ni pomembno);

— sprememba stanja izhoda s storitvijo InputOutputControlByIdentifier.

7.1.2 *Format sporočil*

CPR_062 Formati sporočil pri primitivih InputOutputControlByIdentifier so podrobno opisani v naslednjih preglednicah.

▼B

Preglednica 33

Sporočilo InputOutputControlByIdentifier Request

Št. bajta	Naziv parametra	Hex vrednost	Mnemonik
#1	Formatni bajt – fizično naslavljanje	80	FMT
#2	Bajt ciljnega naslova	EE	TGT
#3	Bajt izvornega naslova	tt	SRC
#4	Dodatni bajt dolžine	xx	LEN
#5	**InputOutputControlByIdentifier Request Sid**	**2F**	**IOCBI**
#6 in #7	InputOutputIdentifier = [CalibrationInputOutput]	F960	IOI_CIO
#8 ali #8 do #9	ControlOptionRecord = [		COR_…
	inputOutputControlParameter – ena od vrednosti iz preglednice 36	xx	IOCP_…
	controlState – ena od vrednosti iz preglednice 37 (gl. spodnjo opombo)]	xx	CS_…
#9 ali #10	Kontrolna vsota	00-FF	CS

Opomba: Parameter controlState je prisoten le v nekaterih primerih (glej oddelek 7.1.3).

Preglednica 34

Sporočilo InputOutputControlByIdentifier Positive Response

Št. bajta	Naziv parametra	Hex vrednost	Mnemonik
#1	Formatni bajt – fizično naslavljanje	80	FMT
#2	Bajt ciljnega naslova	tt	TGT
#3	Bajt izvornega naslova	EE	SRC
#4	Dodatni bajt dolžine	xx	LEN
#5	**inputOutputControlByIdentifier Positive Response SId**	**6F**	**IOCBIPR**
#6 in #7	inputOutputIdentifier = [CalibrationInputOutput]	F960	IOI_CIO
#8 ali #8 do #9	controlStatusRecord = [		CSR_
	inputOutputControlParameter (enaka vrednost kot v bajtu #8 v preglednici 33)	xx	IOCP_…
	controlState (enaka vrednost kot v bajtu #9 v preglednici 33)] (če je ustrezno)	xx	CS_…
#9 ali #10	Kontrolna vsota	00-FF	CS

▼B

Preglednica 35

Sporočilo InputOutputControlByIdentifier Negative Response

Št. bajta	Naziv parametra	Hex vrednost	Mnemonik
#1	Formatni bajt – fizično naslavljanje	80	FMT
#2	Bajt ciljnega naslova	tt	TGT
#3	Bajt izvornega naslova	EE	SRC
#4	Dodatni bajt dolžine	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	Kontrolna vsota	00-FF	CS

7.1.3 *Opredelitev parametrov*

CPR_064 Parameter ***inputOutputControlParameter (IOCP_)*** je opredeljen v preglednici spodaj.

Preglednica 36

Opredelitev vrednosti inputOutputControlParameter

Hex	Opis	Mnemonik
00	**ReturnControlToECU** Ta vrednost kaže strežniku (VU), da preskuševalnik ne upravlja več kalibracijske V/I signalne linije.	RCTECU
01	**ResetToDefault** Ta vrednost sporoča strežniku (VU), naj ponastavi kalibracijsko V/I signalno linijo v njeno privzeto stanje.	RTD

▼B

Hex	Opis	Mnemonik
03	**ShortTermAdjustment** Ta vrednost sporoča strežniku (VU), naj nastavi kalibracijsko V/I signalno linijo na vrednost, ki jo vsebuje parameter controlState.	STA

CPR_065 Parameter ***controlState*** je prisoten le, kadar je inputOutputControlParameter nastavljen na ShortTermAdjustment, opredeljen pa je v naslednji preglednici:

Preglednica 37

Opredelitev vrednosti controlState

Način	Hex vrednost	Opis
Onemogoči	00	V/I linija je onemogočena (privzeto stanje)
Omogoči	01	Omogoči kalibracijo V/I linije kot speedSignalInput
Omogoči	02	Omogoči kalibracijo V/I linije kot realTimeSpeedSignalOutputSensor
Omogoči	03	Omogoči kalibracijo V/I linije kot RTCOutput

8. FORMATI DATARECORDS

Ta oddelek opisuje:

— splošna pravila glede območij parametrov, ki jih enota v vozilu pošilja preskuševalniku,

— formate, ki se uporabljajo za podatke, ki se prenesejo s storitvami prenosa podatkov, opisanimi v oddelku 6.

CPR_067 VU mora podpirati vse naštete parametre.

CPR_068 Podatki, ki jih VU pošlje preskuševalniku kot odgovor na sporočilo zahtevka, morajo biti merjeni podatki (tj. trenutna vrednost zahtevanega parametra, kot jo je izmerila ali zaznala VU).

8.1. **Območja prenesenih parametrov**

CPR_069 Preglednica 38 opredeljuje območja, ki se uporabljajo za ugotavljanje veljavnosti prenesenih parametrov.

CPR_070 Vrednosti v območju „znak napake“ služijo VU za takojšnje sporočanje, da zaradi kakšne napake na tahografu veljavne vrednosti parametrov trenutno niso na voljo.

CPR_071 Vrednosti v območju „ni na voljo“ služijo VU za pošiljanje sporočila, ki vsebuje parameter, ki ni na voljo ali v trenutnem modulu ni podprt. Vrednosti v območju „ni zahtevano“ služijo napravi za pošiljanje ukaznega sporočila in določitev tistih parametrov, za katere od sprejemne naprave ne pričakuje odgovora.

▼B

CPR_072 Če napaka določenega sestavnega dela onemogoča prenos veljavne vrednosti kakšnega parametra, se namesto podatkov tega parametra uporabi znak napake, opisan v preglednici 38. Če pa meritev ali izračun da vrednost, ki je veljavna, vendar leži zunaj opredeljenega območja parametra, se znak napake ne uporabi. Tak podatek se prenese z uporabo ustrezne najmanjše ali največje vrednosti parametra.

Preglednica 38

Območja dataRecords

Naziv območja	1 bajt (Hex vrednost)	2 bajta (Hex vrednost)	4 bajti (Hex vrednost)	ASCII
Veljaven signal	00 do FA	0000 do FAFF	00000000 do FAFFFFFF	1 do 254
Specifični kazalnik parametra	FB	FB00 do FBFF	FB000000 do FBFFFFFF	ga ni
Rezervirano območje za prihodnje označevalne bite	FC do FD	FC00 do FDFF	FC000000 do FDFFFFFF	ga ni
Znak napake	FE	FE00 do FEFF	FE000000 do FEFFFFFF	0
Ni na voljo ali ni zahtevano	FF	FF00 do FFFF	FF000000 do FFFFFFFF	FF

CPR_073 Pri ASCII-kodiranih parametrih je ASCII znak „*“ rezerviran za ločevalec.

8.2. **Formati dataRecords**

Formati, ki se uporabljajo pri storitvah ReadDataByIdentifier in WriteDataByIdentifier, so podrobno opisani v preglednicah 39 do 42 spodaj.

CPR_074 Preglednica 39 podaja dolžino, ločljivost in delovno območje vseh parametrov, ki jih določajo identifikatorji recordDataIdentifier:

Preglednica 39

Format dataRecords

Naziv parametra	Dolžina podatkov (v bajtih)	Ločljivost	Delovno območje
TimeDate	8	podrobneje v preglednici 40	
HighResolutionTotalVehicleDistance	4	ojačitev 5 m/bit, zamik 0 m	0 do + 21 055 406 km
Kfactor	2	ojačitev 0,001 impulza/m/bit, zamik 0	0 do 64,255 impulza/m
LfactorTyreCircumference	2	ojačitev 0,125 10^{-3} m/bit, zamik 0	0 do 8,031 m
WvehicleCharacteristicFactor	2	ojačitev 0,001 impulza/m/bit, zamik 0	0 do 64,255 impulza/m
TyreSize	15	ASCII	ASCII
NextCalibrationDate	3	podrobneje v preglednici 41	
SpeedAuthorised	2	ojačitev 1/256 km/h/bit, zamik 0	0 do 250,996 km/h

▼B

Naziv parametra	Dolžina podatkov (v bajtih)	Ločljivost	Delovno območje
RegisteringMemberState	3	ASCII	ASCII
VehicleRegistrationNumber	14	podrobneje v preglednici 42	
VIN	17	ASCII	ASCII

CPR_075 V preglednici 40 so podrobno opisani formati različnih bajtov parametra TimeDate:

Preglednica 40

Podrobni format parametra TimeDate (vrednost recordDataIdentifier # F90B)

Bajt	Opredelitev parametra	Ločljivost	Delovno območje
1	Sekunde	ojačitev 0,25 s/bit, zamik 0 s	0 do 59,75s
2	Minute	ojačitev 1 min/bit, zamik 0 m	0 do 59 min
3	Ure	ojačitev 1 h/bit, zamik 0 h	0 do 23 h
4	Mesec	ojačitev 1 mesec/bit, zamik 0 mesecev	1 do 12 mesecev
5	Dan	ojačitev 0,25 dneva/bit, zamik 0 dni (glej OPOMBO pod preglednico 41)	0,25 do 31,75 dneva
6	Leto	ojačitev 1 leto/bit, zamik + 1985 let (glej OPOMBO pod preglednico 41)	1985 do 2235 let
7	Lokalna minutna izravnava	ojačitev 1 min/bit, zamik – 125 min	– 59 do + 59 min
8	Lokalna urna izravnava	ojačitev 1 h/bit, zamik – 125 h	– 23 do + 23 h

CPR_076 V preglednici 41 so podrobno opisani formati različnih bajtov parametra NextCalibrationDate.

Preglednica 41

Podrobni format parametra NextCalibrationDate (vrednost recordDataIdentifier # F922)

Bajt	Opredelitev parametra	Ločljivost	Delovno območje
1	Mesec	ojačitev 1 mesec/bit, zamik 0 mesecev	1 do 12 mesecev
2	Dan	ojačitev 0,25 dneva/bit, zamik 0 dni (glej OPOMBO spodaj)	0,25 do 31,75 dneva
3	Leto	ojačitev 1 leto/bit, zamik + 1985 let (glej OPOMBO spodaj)	1985 do 2235 let

▼B

OPOMBA glede uporabe parametra „Dan“:

1) Vrednost datuma 0 je neveljavna vrednost. Vrednosti 1, 2, 3 in 4 pomenijo prvi dan v mesecu, vrednosti 5, 6, 7 in 8 pomenijo drugi dan v mesecu itd.

2) Ta parameter ne vpliva na parameter ur in ga ne spreminja.

OPOMBA glede uporabe bajta za parameter „Leto“:

Vrednost parametra „Leto“ 0 pomeni leto 1985, vrednost 1 pomeni leto 1986 itd.

CPR_078 V preglednici 42 so podrobno opisani formati različnih bajtov parametra VehicleRegistrationNumber:

Preglednica 42

Podrobni format parametra VehicleRegistrationNumber (vrednost recordDataIdentifier # F97E)

Bajt	Opredelitev parametra	Ločljivost	Delovno območje
1	Kodna stran (kot je opredeljena v Dodatku 1)	ASCII	01 do 0A
2–14	Registrska številka vozila (kot je opredeljena v Dodatku 1)	ASCII	ASCII

▼B

Dodatek 9

HOMOLOGACIJA SEZNAM MINIMALNIH ZAHTEVANIH PRESKUSOV

KAZALO

1. UVOD

2. PRESKUSI FUNKCIONALNOSTI ENOTE V VOZILU

3. PRESKUSI FUNKCIONALNOSTI TIPALA GIBANJA

4. PRESKUSI FUNKCIONALNOSTI TAHOGRAFSKE KARTICE

5. PRESKUSI ZUNANJE GNSS OPREME

6. PRESKUSI NAPRAVE ZA KOMUNIKACIJO NA DALJAVO

7. PRESKUSI FUNKCIONALNOSTI PAPIRJA

8. PRESKUSI INTEROPERABILNOSTI

1. UVOD

1.1. **Homologacija**

ES-homologacija zapisovalne naprave (ali njenega sestavnega dela) ali tahografske kartice temelji na:

— **certificiranju zaščite** na podlagi specifikacij skupnih meril, da se ugotovi, ali so cilji zaščite v celoti izpolnjeni v skladu z Dodatkom 10 k tej prilogi (se dopolni/spremeni),

— **certificiranju funkcionalnosti**, s katerim organ države članice potrdi, da preskušana oprema izpolnjuje zahteve te priloge glede izvajanja funkcij, točnosti meritev in okoljskih lastnosti,

— **certificiranju interoperabilnosti**, s katerim pristojni organ potrdi, da je zapisovalna naprava (ali tahografska kartica) v celoti interoperabilna z zahtevanimi modeli tahografskih kartic (ali zapisovalne naprave) (glej poglavje 8 te priloge).

Ta dodatek predpisuje, katere preskuse mora (najmanj) opraviti organ države članice v okviru preskušanja funkcionalnosti in katere preskuse mora (najmanj) opraviti pristojni organ v okviru preskušanja interoperabilnosti. Postopki izvedbe preskusov in vrsta preskusov niso podrobneje predpisani.

Ta dodatek ne obravnava vidikov certificiranja zaščite. Če so bili nekateri preskusi, predpisani za homologacijo, opravljeni že v procesu ocene in certificiranja zaščite, teh preskusov ni potrebno opraviti še enkrat. V takem primeru se lahko pregleda zgolj rezultate teh preskusov. Opomba: zahteve, ki naj bi se preskušale (ali so tesno povezane s preskusi, katerih izvedba se pričakuje) v okviru certificiranja zaščite, so v tem dodatku označene z „*“.

Naštete zahteve se nanašajo na glavni del priloge, druge zahteve pa na druge dodatke (npr. PIC_001 se nanaša na zahtevo PIC_001 Dodatka 3 o piktogramih).

Ta dodatek ločeno obravnava homologacijo tipala gibanja, enote v vozilu in zunanje GNSS opreme kot sestavnih delov zapisovalne naprave. Vsak

▼B

sestavni del bo dobil svoje potrdilo o homologaciji, v katerem bodo navedeni drugi združljivi sestavni deli. Preskus funkcionalnosti tipala gibanja (ali zunanje GNSS opreme) se opravi skupaj z enoto v vozilu in obratno.

Interoperabilnost med vsakim modelom tipala gibanja (ali zunanje GNSS opreme) in vsakim modelom enote v vozilu se ne zahteva. V tem primeru se lahko homologacija tipala gibanja (ali zunanje GNSS opreme) podeli samo v kombinaciji s homologacijo zadevne enote v vozilu in obratno.

1.2. **Viri**

V tem dodatku so uporabljeni naslednji viri:

IEC 60068-2-1: Okoljski preskusi – 2-1. del: Preskusi – Preskusi A: Mraz

IEC 60068-2-2: Basic environmental testing procedures; part 2: tests; tests B: dry heat (sinusoidal)

IEC 60068-2-6: Environmental testing – Part 2: Tests – Test Fc: Vibration

IEC 60068-2-14: Environmental testing; Part 2-14: Tests; Test N: Change of temperature

IEC 60068-2-27: Okoljsko preskušanje. 2. del: Preskusi – Preskus Ea in vodilo: Udarec

IEC 60068-2-30: Okoljski preskusi – 2-30. del: Preskusi – Preskus Db: Vlažna toplota, ciklična (12 + 12-urni cikel)

IEC 60068-2-64: Okoljski preskusi – 2-64. del: Preskusi – Preskus Fh: Vibracije, naključne širokopasovne, in vodilo

IEC 60068-2-78 Okoljski preskusi – 2-78. del: Preskusi – Preskuševalna omarica: Vlažna vročina, ustaljeno stanje

ISO 16750-3 – Mechanical loads (2012-12)

ISO 16750-4 – Climatic loads(2010-04).

ISO 20653: Road vehicles – Degree of protection (IP code) – Protection of electrical equipment against foreign objects, water and access

ISO 10605:2008 + Technical Corrigendum:2010 + AMD1:2014 Road vehicles – Test methods for electrical disturbances from electrostatic discharge

ISO 7637-1:2002 + AMD1: 2008 Road vehicles – Electrical disturbances from conduction and coupling – Part 1: Definitions and general considerations.

ISO 7637-2 Road vehicles – Electrical disturbances from conduction and coupling – Part 2: Electrical transient conduction along supply lines only.

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.

ISO/IEC 7816-1 Identification cards – Integrated circuit(s) cards with contacts – Part 1: Physical characteristics..

ISO/IEC 7816-2 Information technology – Identification cards – Integrated circuit(s) cards with contacts – Part 2: Dimensions and location of the contacts.

ISO/IEC 7816-3 Information technology – Identification cards – Integrated circuit(s) cards with contacts – Part 3: Electronic signals and transmission protocol.

ISO/IEC 10373-1:2006 + AMD1:2012 Identification cards – Test methods – Part 1: General characteristics

ISO/IEC 10373-3:2010 + Technical Corrigendum:2013 Identification cards – Test methods – Part 3: Integrated circuit cards with contacts and related interface devices

▼B

ISO 16844-3:2004, Cor 1:2006 Road vehicles – Tachograph systems – Part 3: Motion sensor interface (with vehicle units).

ISO 16844-4 Road vehicles – Tachograph systems – Part 4: CAN interface

ISO 16844-6 Road vehicles – Tachograph systems – Part 6: Diagnostics

ISO 16844-7 Road vehicles – Tachograph systems – Part 7: Parameters

ISO 534 Papir, karton in lepenka – Ugotavljanje debeline, gostote in specifičnega volumna

UN ECE R10 Enotne določbe za homologacijo vozil glede na elektromagnetno združljivost (Ekonomska komisija Združenih narodov za Evropo).

2. PRESKUSI FUNKCIONALNOSTI ENOTE V VOZILU

Št.	Preskus	Opis	Povezane zahteve
1.	**Administrativni pregled**		
1.1	Dokumentacija	Pravilnost dokumentacije	
1.2	Rezultati preskusa proizvajalca	Rezultati preskusa proizvajalca, opravljenega med vgradnjo Papirna dokazila	88, 89, 91
2.	**Vizualni pregled**		
2.1	Skladnost z dokumentacijo		
2.2	Identifikacija/oznake		224 do 226
2.3	Materiali		219 do 223
2.4	Zapečatenje		398, 401 do 405
2.5	Zunanji vmesniki		
3.	**Preskusi funkcionalnosti**		
3.1	Možne funkcije		03, 04, 05, 07, 382
3.2	Načini delovanja		09 do 11*, 132, 133
3.3	Pravice dostopa do funkcij in podatkov		12* 13*, 382, 383, 386 do 389
3.4	Spremljanje vstavljanja in izvlečenja kartic		15, 16, 17, 18, 19*, 20*, 132
3.5	Merjenje hitrosti in razdalje		21 do 31

▼B

Št.	Preskus	Opis	Povezane zahteve
3.6	Merjenje časa (preskus se opravlja pri 20 °C)		38 do 43
3.7	Spremljanje voznikovih dejavnosti		44 do 53, 132
3.8	Spremljanje statusa vožnje		54, 55, 132
3.9	Ročni vnosi		56 do 62
3.10	Upravljanje blokad s strani podjetja		63 do 68
3.11	Spremljanje nadzornih dejavnosti		69, 70
3.12	Zaznavanje dogodkov in/ali napak		71 do 88, 132
3.13	Identifikacijski podatki naprave		93*, 94*, 97, 100
3.14	Podatki o vstavljanju in izvlečenju vozniške kartice		102* do 104*
3.15	Podatki o voznikovih dejavnostih		105* do 107*
3.16	Podatki o krajih in položajih		108* do 112*
3.17	Podatki kilometrskega števca		113* do 115*
3.18	Podrobni podatki o hitrosti		116*
3.19	Podatki o dogodkih		117*
3.20	Podatki o napakah		118*
3.21	Kalibracijski podatki		119* do 121*
3.22	Podatki o prilagajanju časa		124*, 125*
3.23	Podatki o nadzornih dejavnostih		126*, 127*
3.24	Podatki o blokadah s strani podjetja		128*
3.25	Podatki o prenosih podatkov		129*
3.26	Podatki o posebnih stanjih		130*, 131*
3.27	Zapisovanje in shranjevanje podatkov na tahografske kartice		134, 135, 136*, 137*, 139*, 140, 141 142, 143, 144*, 145*, 146*, 147, 148
3.28	Prikazovanje		90, 132, 149 do 166 PIC_001, DIS_001
3.29	Tiskanje		90, 132, 167 do 179, PIC_001, PRT_001 to PRT_014
3.30	Opozarjanje		132, 180 do 189 PIC_001
3.31	Prenos podatkov na zunanje medije		90, 132, 190 do 194
3.32	Komunikacija na daljavo za namen ciljnih cestnih preverjanj		195 do 197
3.33	Iznos podatkov na dodatne zunanje naprave		198, 199

▼B

Št.	Preskus	Opis	Povezane zahteve
3.34	Kalibracija		202 do 206*, 383, 384, 386 do 391
3.35	Cestno preverjanje kalibracije		207 do 209
3.36	Prilagajanje časa		210 do 212*
3.37	Brez interference s strani dodatnih funkcij		06, 425
3.38	Vmesnik tipala gibanja		02, 122
3.39	Zunanja GNSS oprema		03, 123
3.40	Preverjanje, ali VU odkrije, zapiše in shrani dogodke in/ali napake, ki jih opredeli proizvajalec VU, ko se povezano tipalo gibanja odzove na magnetna polja, ki motijo odkrivanje gibanja vozila.		217
3.41	Nabor algoritmov in standardizirani parametri domen		CSM_48, CSM_50
4.	**Okoljski preskusi**		
4.1	Temperatura	Preverjanje funkcionalnosti z naslednjimi preskusi: preskus v skladu z ISO 16750-4, poglavje 5.1.1.2: Low temperature operation test (72 h pri – 20 °C) Ta preskus se nanaša na IEC 60068-2-1: Environmental testing – Part 2-1: Tests – Test A: Cold Preskus v skladu z ISO 16750-4, poglavje 5.1.2.2: High temperature operation test (72 h pri 70 °C) Ta preskus se nanaša na IEC 60068-2-2: Basic environmental testing procedures; part 2: tests; tests B: dry heat Preskus v skladu z ISO 16750-4, poglavje 5.3.2: Rapid change of temperature with specified transition duration (– 20 °C/70 °C, 20 ciklov, čas mirovanja 2 h pri vsaki temperaturi) Skrčen nabor preskusov (izbranih med preskusi, predpisanimi v oddelku 3 te preglednice) se lahko opravi pri nižji temperaturi, pri višji temperaturi ali med temperaturnimi cikli	213
4.2	Vlažnost	Preverjanje, ali lahko enota v vozilu prenese cikle vlage (preskus s ciklično vlažno vročino) s preskusom Db po IEC 60068-2-30, šest 24-urnih ciklov, pri vsakem spreminjanje temperature od + 25 °C do + 55 °C, relativna vlažnost 97 % pri + 25 °C in 93 % pri + 55 °C	214

▼B

Št.	Preskus	Opis	Povezane zahteve
4.3	Mehanski	1. Sinusoidne vibracije preverjanje, ali lahko enota v vozilu prenese sinusoidne vibracije naslednjih lastnosti: konstantni premiki med 5 in 11 Hz: konica 10 mm konstantni pospeški med 11 in 300 Hz: 5g To zahtevo se preverja s preskusom Fc po IEC 60068-2-6, z najmanjšim trajanjem preskusa 3 × 12 ur (12 ur na vsako os) ISO 16750-3 za naprave, nameščene v ločeno kabina vozila, ne zahteva preskusa s sinusoidnimi vibracijami. 2. Naključne vibracije: Preskus v skladu z ISO 16750-3, poglavje 4.1.2.8: Test VIII: Commercial vehicle, decoupled vehicle cab Preskus z naključnimi vibracijami, 10–2 000 Hz, RMS navpično 21,3 m/s^2, RMS vodoravno 11,8 m/s^2, RMS bočno 13,1 m/s^2, 3 osi, 32 h na os, vključno s temperaturnim ciklom – 20–70 °C. Ta preskus se nanaša na IEC 60068-2-64: Environmental testing – Part 2-64: Tests – Test Fh: Vibration, broadband random and guidance 3. Udarci: mehanski udarec s 3 g, pol sinusni v skladu z ISO 16750. Zgoraj opisani preskusi se opravijo na različnih vzorcih preskušane opreme.	219
4.4	Zaščita pred vodo in tujki	Preskus v skladu z ISO 20653: Road vehicles – Degree of protection (IP code) – Protection of electrical equipment against foreign objects, water and access (brez sprememb parametrov); najnižja vrednost IP 40	220, 221
4.5	Prenapetostna zaščita	Preverjanje, ali enota v vozilu prenese naslednje napajanje: izvedbe 24 V: 34 V pri + 40 °C 1 uro; izvedbe 12 V: 17 V pri + 40 °C 1 uro; (ISO 16750-2)	216

▼B

Št.	Preskus	Opis	Povezane zahteve
4.6	Zaščita pred zamenjavo polarnosti	Preverjanje, ali enota v vozilu prenese zamenjavo polaritete svoje napajalne napetosti. (ISO 16750-2)	216
4.7	Kratkostična zaščita	Preverjanje, ali so izhodni signali zaščiteni pred kratkimi stiki z napajalno napetostjo in ozemljitvijo (ISO 16750-2)	216
5.	**Preskusi elektromagnetne združljivosti (EMC)**		
5.1	Lastna sevanja in dovzetnost	Skladnost s Pravilnikom ECE R10	218
5.2	Elektrostatična razelektritev	Skladnost z ISO 10605:2008 + Technical Corrigendum:2010 + AMD1:2014: +/– 4 kV za kontakt in +/– 8 kV za odvod zraka	218
5.3	Prehodna dovzetnost za prevodne motnje	Pri izvedbah 24 V: skladnost z ISO 7637-2 + Pravilnikom ECE št. 10 Rev. 3: impulz 1a: Vs = – 450 V Ri =50 ohmov impulz 2a: Vs = + 37 V Ri = 2 ohma impulz 2b: Vs = + 20 V Ri = 0,05 ohma impulz 3a: Vs = – 150 V Ri = 50 ohmov impulz 3b: Vs = + 150 V Ri = 50 ohmov impulz 4: Vs = – 16 V Va = – 12 V t6 = 100 ms impulz 5: Vs = + 120 V Ri = 2,2 ohma td = 250 ms Pri izvedbah 12 V: skladnost z ISO 7637-1 + Pravilnikom ECE št. 10 Rev. 3: impulz 1: Vs = – 75 V Ri = 10 ohmov impulz 2a: Vs = + 37 V Ri = 2 ohma impulz 2b: Vs = + 10 V Ri = 0,05 ohma impulz 3a: Vs = – 112 V Ri = 50 ohmov impulz 3b: Vs = + 75 V Ri = 50 ohmov impulz 4: Vs = – 6 V Va = – 5 V t6 = 15 ms impulz 5: Vs = + 65 V Ri = 3 ohme td = 100 ms impulz 5 se preskuša le za enote v vozilu, namenjene za vgradnjo v vozila brez vgrajene zunanje skupne zaščite pred razbremenitvami Za predlog razbremenitve glej ISO 16750-2, 4. izdaja, poglavje 4.6.4.	218

▼B

3. PRESKUSI FUNKCIONALNOSTI TIPALA GIBANJA

Št.	Preskus	Opis	Povezane zahteve
1.	**Administrativni pregled**		
1.1	Dokumentacija	Pravilnost dokumentacije	
2.	**Vizualni pregled**		
2.1	Skladnost z dokumentacijo		
2.2	Identifikacija/oznake		225, 226
2.3	Materiali		219 do 223
2.4	Zapečatenje		398, 401 do 405
3.	**Preskusi funkcionalnosti**		
3.1	Identifikacijski podatki tipala		95 do 97*
3.2	Povezava tipala gibanja in enote v vozilu		122*, 204
3.3	Zaznavanje gibanja Točnost merjenja gibanja		30 do 35
3.4	Vmesnik enote v vozilu		02
3.5	Preverjanje, ali je tipalo gibanja odporno na stalno magnetno polje. Druga možnost je preverjanje, ali se tipalo gibanja odziva na stalna magnetna polja, ki motijo zaznavanje gibanja vozila, da lahko povezana VU zazna, zabeleži in shrani napake tipala		217
4.	**Okoljski preskusi**		
4.1	Delovna temperatura	Preverjanje funkcionalnosti (opredeljene pri preskusu št. 3.3) v temperaturnem območju [– 40 °C; + 135 °C] s preskusom: IEC 60068-2-1, preskus Ad, trajanje preskusa 96 ur pri najnižji temperaturi To_{min} IEC 60068-2-2, preskus Bd, trajanje preskusa 96 ur pri najvišji temperaturi To_{max} Preskus v skladu z ISO 16750-4, poglavje 5.1.1.2: Low temperature operation test (24 h @ – 40 °C) Ta preskus se nanaša na IEC 60068-2-1: Environmental testing – Part 2-1: Tests – Test A: Cold IEC 68-2-2, preskus Bd, trajanje preskusa 96 ur pri najnižji temperaturi – 40 °C. Preskus v skladu z ISO 16750-4, poglavje 5.1.2.2: High temperature operation test (96 h @ 135 °C) Ta preskus se nanaša na IEC 60068-2-2: Basic environmental testing procedures; part 2: tests; tests B: dry heat	213

▼B

Št.	Preskus	Opis	Povezane zahteve
4.2	Temperaturni cikli	Preskus v skladu z ISO 16750-4, poglavje 5.3.2: Rapid change of temperature with specified transition duration (– 40°C/135 °C, 20 ciklov, čas mirovanja 30 pri vsaki temperaturi) IEC 60068-2-14: Environmental testing; Part 2-14: Tests; Test N: Change of temperature	213
4.3	Cikli vlažnosti	Preverjanje funkcionalnosti (opredeljene pri preskusu št. 3.3) s preskusom Db po IEC 60068-2-30, šest 24-urnih ciklov, pri vsakem spreminjanje temperature od + 25 °C do + 55 °C, relativna vlažnost 97 % pri + 25 °C in 93 % pri + 55 °C	214
4.4	Vibracije	ISO 16750-3, poglavje 4.1.2.6: Test VI: Commercial vehicle, engine, gearbox Mešani preskusi vibracij, vključno s a) preskusom sinusoidnih vibracij, 20–520 Hz, 11,4– 120 m/s^2, <= 0,5 oct/min b) preskusom naključnih vibracij, 10–2 000 Hz, RMS 177 m/s^2 94 h na os, vključno s temperaturnim ciklom – 20–70 °C) Ta preskus se nanaša na IEC 60068-2-80: Environmental testing – Part 2-80: Tests – Test Fi: Vibration – Mixed mode	219
4.5	Mehanski udarci	ISO 16750-3, poglavje 4.2.3: Test VI: Test for devices in or on the gearbox polsinusni udarec, pospešek po dogovoru v območju 3 000–15 000 m/s^2, trajanje impulza po dogovoru, vendar < 1 ms, število udarcev: po dogovoru Ta preskus se nanaša na IEC 60068-2-27: Environmental testing. Part 2: Tests. Test Ea and guidance: Shock	219
4.6	Zaščita pred vodo in tujki	Preskus v skladu z ISO 20653: Road vehicles – Degree of protection (IP code) – Protection of electrical equipment against foreign objects, water and access (ciljna vrednost IP 64)	220, 221
4.7	Zaščita pred zamenjavo polarnosti	Preverjanje, ali tipalo gibanja prenese zamenjavo polarnosti svojega napajanja.	216
4.8	Kratkostična zaščita	Preverjanje, ali so izhodni signali zaščiteni pred kratkimi stiki z napajalno napetostjo in ozemljitvijo	216

▼B

Št.	Preskus	Opis	Povezane zahteve
5.	**EMC**		
5.1	Sevane emisije in dovzetnost	Preverjanje skladnosti s Pravilnikom ECE R10	218
5.2	Elektrostatična razelektritev	Skladnost z ISO 10605:2008 + Technical Corrigendum:2010 + AMD1:2014: +/– 4 kV za kontakt in +/– 8 kV za odvod zraka	218
5.3	Prehodna dovzetnost podatkovnih linij	Pri izvedbah 24 V: skladnost z ISO 7637-2 + Pravilnikom ECE št. 10 Rev. 3: impulz 1a: Vs = – 450 V Ri = 50 ohmov impulz 2a: Vs = + 37 V Ri = 2 ohma impulz 2b: Vs = + 20 V Ri = 0,05 ohma impulz 3a: Vs = – 150 V Ri = 50 ohmov impulz 3b: Vs = + 150 V Ri = 50 ohmov impulz 4: Vs = – 16 V Va = – 12 V t6 = 100 ms impulz 5: Vs = +120 V Ri = 2,2 ohma td = 250 ms Pri izvedbah 12 V: skladnost z ISO 7637-1 + Pravilnikom ECE št. 10 Rev. 3: impulz 1: Vs = – 75 V Ri = 10 ohmov impulz 2a: Vs = + 37 V Ri = 2 ohma impulz 2b: Vs = + 10 V Ri = 0,05 ohma impulz 3a: Vs = – 112 V Ri = 50 ohmov impulz 3b: Vs = + 75 V Ri = 50 ohmov impulz 4: Vs = – 6 V Va = – 5 V t6 = 15 ms impulz 5: Vs = + 65 V Ri = 3 ohme td = 100 ms impulz 5 se preskuša le za enote v vozilu, namenjene za vgradnjo v vozila brez vgrajene zunanje skupne zaščite pred razbremenitvami Za predlog razbremenitve glej ISO 16750-2, 4. izdaja, poglavje 4.6.4.	218

4. PRESKUSI FUNKCIONALNOSTI TAHOGRAFSKE KARTICE

Preskuse v skladu z oddelkom 4,

št. 5 „Preskusi protokolov“,

št. 6 „Struktura kartice“ in

št. 7 „Preskusi funkcionalnosti“,

lahko opravi ocenjevalec ali izdajatelj certifikata med postopkom certificiranja na podlagi skupnih meril za modul čipa.

Preskusa številka 2.3 in 4.2 sta enaka. To sta mehanska preskusa kombinacije kartice in modula čipa. Ta poskusa je treba opraviti, če se kateri od teh sestavnih delov (kartica, modul čipa) spremeni.

▼B

Št.	Preskus	Opis	Povezane zahteve
1.	**Administrativni pregled**		
1.1	Dokumentacija	Pravilnost dokumentacije	
2.	**Kartica**		
2.1	Oblika natisnjenih podatkov	Preverjanje, ali so vse varnostne značilnosti in vidni podatki natisnjeni na kartici pravilno in v skladu z zahtevami [Označitev] Priloga 1C, poglavje 4.1 „Vidni podatki“, 227) Prednja stran mora vsebovati: glede na vrsto kartice besede „vozniška kartica“ ali „nadzorna kartica“ ali „kartica servisne delavnice“ ali „kartica podjetja“, natisnjeni z velikimi tiskanimi črkami v uradnem jeziku države izdajateljice kartice. [Ime države članice] Priloga 1C, poglavje 4.1 „Vidni podatki“, 228) Prednja stran mora vsebovati: ime države izdajateljice (neobvezno). [Podpis] Priloga 1C, poglavje 4.1 „Vidni podatki“, 229) Prednja stran mora vsebovati: oznako države članice, ki izda kartico, natisnjeno v negativu v modrem pravokotniku in obkroženo z 12 rumenimi zvezdami. [Oštevilčenje] Priloga 1C, poglavje 4.1 „Vidni podatki“, 232) Zadnja stran mora vsebovati: razlago oštevilčenih postavk, ki so na prednji strani kartice. [Barva] Priloga 1C, poglavje 4.1 „Vidni podatki“, 234) Tahografske kartice morajo biti natisnjene na ozadju naslednjih prevladujočih barv: — vozniška kartica: bela, — kartica servisne delavnice: rdeča, — nadzorna kartica: modra, — kartica podjetja: rumena.	227 do 229, 232, 234 do 236

▼B

Št.	Preskus	Opis	Povezane zahteve
		[Zaščita] Priloga 1C, poglavje 4.1 „Vidni podatki“, 235) Tahografska kartica mora biti zaščitena pred ponarejanjem in nepooblaščenimi posegi vsaj z naslednjimi zaščitami: — varnostni vzorec ozadja s finimi vzorci giljoše in mavričnim tiskom, — vsaj ena dvobarvna črta v mikrotisku.	
		[Oznake] Priloga 1C, poglavje 4.1 „Vidni podatki“, 236) Države članice lahko uporabijo dodatne barve ali oznake, npr. nacionalne simbole in zaščitne elemente.	
		[Homologacijska oznaka] Tahografske kartice morajo vsebovati homologacijsko oznako. Homologacijska oznaka je sestavljena iz: — pravokotnika, znotraj katerega je črka „e“, ki ji sledi oznaka države (številka ali črka), ki je izdala homologacijo, — homologacijske številke, ki ustreza številki potrdila o homologaciji za tahografsko kartico, ki naj bo v neposredni bližini tega pravokotnika.	
2.2	Mehanski preskusi	[Velikost kartice] Tahografske kartice morajo ustrezati standardu ISO/IEC 7810, Identification cards – Physical characteristics, [5] Dimension of card, [5.1] Card size, [5.1.1] Card dimensions and tolererances, card type ID-1 Unused card	240, 243 ISO/IEC 7810
		[Robovi kartice] Tahografske kartice morajo ustrezati standardu ISO/IEC 7810, Identification cards – Physical characteristics, [5] Dimension of card, [5.1] Card size, [5.1.2] Card edges	

▼B

Št.	Preskus	Opis	Povezane zahteve
		[Konstrukcija kartice] Tahografske kartice morajo ustrezati standardu ISO/IEC 7810, Identification cards – Physical characteristics, [6] Card construction	
		[Materiali kartice] Tahografske kartice morajo ustrezati standardu ISO/IEC 7810, Identification cards – Physical characteristics, [7] Card materials	
		[Upogibna trdnost] Tahografske kartice morajo ustrezati standardu ISO/IEC 7810, Identification cards – Physical characteristics, [8] Card characteristics, [8.1] Bending stiffness	
		[Toksičnost] Tahografske kartice morajo ustrezati standardu ISO/IEC 7810, Identification cards – Physical characteristics, [8] Card characteristics, [8.3] Toxicity	
		[Odpornost proti kemikalijam] Tahografske kartice morajo ustrezati standardu ISO/IEC 7810, Identification cards – Physical characteristics, [8] Card characteristics, [8.4] Resistance to chemicals	
		[Stabilnost kartice] Tahografske kartice morajo ustrezati standardu ISO/IEC 7810, Identification cards – Physical characteristics, [8] Card characteristics, [8.5] Card dimensional stability and warpage with temperature and humidity	

▼B

Št.	Preskus	Opis	Povezane zahteve
		[Svetloba] Tahografske kartice morajo ustrezati standardu ISO/IEC 7810, Identification cards – Physical characteristics, [8] Card characteristics, [8.6] Light	
		[Obstojnost] Priloga 1C, poglavje 4.4 „Okoljske in električne tehnične zahteve“, 241) Tahografske kartice morajo ob uporabi v predpisanih okoljskih in električnih pogojih delovati pravilno pet let.	
		[Luščilna trdnost] Tahografske kartice morajo ustrezati standardu ISO/IEC 7810, Identification cards – Physical characteristics, [8] Card characteristics, [8.8] Peel strength	
		[Oprijem ali blokiranje] Tahografske kartice morajo ustrezati standardu ISO/IEC 7810, Identification cards – Physical characteristics, [8] Card characteristics, [8.9] Adhesion or blocking	
		[Skrivljenje] Tahografske kartice morajo ustrezati standardu ISO/IEC 7810, Identification cards – Physical characteristics, [8] Card characteristics, [8.11] Overall card warpage	
		[Odpornost proti toploti] Tahografske kartice morajo ustrezati standardu ISO/IEC 7810, Identification cards – Physical characteristics, [8] Card characteristics, [8.12] Resistance to heat	

▼B

Št.	Preskus	Opis	Povezane zahteve
		[Deformacija površine] Tahografske kartice morajo ustrezati standardu ISO/IEC 7810, Identification cards – Physical characteristics, [8] Card characteristics, [8.13] Surface distortions	
		[Kontaminacija] Tahografske kartice morajo ustrezati standardu ISO/IEC 7810, Identification cards – Physical characteristics, [8] Card characteristics, [8.14] Contamination and interaction of card components	
2.3	Mehanski preskusi z vgrajenim modulom čipa	[Upogibanje] Tahografske kartice morajo ustrezati standardu ISO/IEC 7810:2003/Amd. 1:2009, Identification cards – Physical characteristics, Amendment 1: Criteria for cards containing integrated circuits [9.2] Dynamic bending stress Skupno število ciklov upogibanja: 4 000.	ISO/IEC 7810
		[Torzija] Tahografske kartice morajo ustrezati standardu ISO/IEC 7810:2003/Amd. 1:2009, Identification cards – Physical characteristics, Amendment 1: Criteria for cards containing integrated circuits [9.3] Dynamic torsional stress Skupno število torzijskih ciklov: 4 000.	
3.	**Modul**		
3.1	Modul	Modul sestoji iz inkapsulacije čipa in stične plošče [Profil površine] Tahografske kartice morajo ustrezati standardu ISO/IEC 7816-1:2011, Identification cards – Integrated circuit cards – Part 1: Cards with contacts – Physical characteristics [4.2] Surface profile of contacts	ISO/IEC 7816

▼B

Št.	Preskus	Opis	Povezane zahteve
		[Mehanska trdnost] Tahografske kartice morajo ustrezati standardu ISO/IEC 7816-1:2011, Identification cards – Integrated circuit cards – Part 1: Cards with contacts – Physical characteristics [4.3] Mechanical strength (of a card and contacts)	
		[Električna upornost] Tahografske kartice morajo ustrezati standardu ISO/IEC 7816-1:2011, Identification cards – Integrated circuit cards – Part 1: Cards with contacts – Physical characteristics [4.4] Electrical resistance (of contacts)	
		[Mere] Tahografske kartice morajo ustrezati standardu ISO/IEC 7816-2:2007, Identification cards – Integrated circuit cards – Part 2: Cards with contacts – Dimension and location of the contacts [3] Dimension of the contacts	
		[Postavitev] Tahografske kartice morajo ustrezati standardu ISO/IEC 7816-2:2007, Identification cards – Integrated circuit cards – Part 2: Cards with contacts – Dimension and location of the contacts [4] Number and location of the contacts V primeru modulov s šestimi kontakti za kontakta ‘C4’ in ‘C8’ ta preskusna zahteva ne velja.	
4.	**Čip**		
4.1	Čip	[Delovna temperatura] Čip tahografske kartice čip deluje v temperaturi okolice od – 25 °C do + 85 °C.	241 do 244 ECE R10 ISO/IEC 7810 ISO/IEC 10373

▼B

Št.	Preskus	Opis	Povezane zahteve
		[Temperatura in vlažnost] Priloga 1C, poglavje 4.4 „Okoljske in električne tehnične zahteve“, 241) Tahografske kartice morajo delovati pravilno v vseh podnebnih pogojih, ki jih normalno lahko srečamo na območju Skupnosti, in najmanj v območju temperatur od – 25 °C do + 70 °C z občasnimi temperaturnimi konicami do + 85 °C, pri čemer „občasno“ pomeni ne več kot 4 ure naenkrat in skupaj ne več kakor 100-krat v dobi uporabe kartice. Tahografske kartice so za določen čas zaporedoma izpostavljene naslednjim temperaturam in vlažnostim. Po vsakem koraku se preskusi električna funkcionalnost tahografskih kartic. 1. Temperatura – 20 °C za 2 h. 2. Temperatura +/– 0 °C za 2 h. 3. Temperatura + 20 °C, 50 % RV, za 2 h. 4. Temperatura + 50 °C, 50 % RV, za 2 h. 5. Temperatura + 70 °C, 50 % RV, za 2 h. Temperatura se v presledkih poveča na + 85 °C, 50 % RV, za 60 min. 6. Temperatura 70 °C, 85 % RV, za 2 h. Temperatura se v presledkih poveča na + 85 °C, 85 % RV, za 30 min.	
		[Vlažnost] Priloga 1C, poglavje 4.4 „Okoljske in električne tehnične zahteve“, 242) Tahografske kartice morajo delovati pravilno v območju vlažnosti od 10 % do 90 %.	
		[Elektromagnetna združljivost – EMC] Priloga 1C, poglavje 4.4 „Okoljske in električne tehnične zahteve“, 244) Med delovanjem morajo tahografske kartice izpolnjevati zahteve Pravilnika ECE R10 o elektromagnetni združljivosti.	

▼B

Št.	Preskus	Opis	Povezane zahteve
		[Statična elektrika] Priloga 1C, poglavje 4.4 „Okoljske in električne tehnične zahteve“, 244) Med delovanjem morajo biti tahografske kartice zaščitene pred elektrostatičnimi razelektritvami. Tahografske kartice morajo ustrezati standardu ISO/IEC 7810:2003/Amd. 1:2009, Identification cards – Physical characteristics, Amendment 1: Criteria for cards containing integrated circuits [9.4] Static electricity [9.4.1] Contact IC cards Preskusna napetost: 4 000 V.	
		[Rentgenski žarki] Tahografske kartice morajo ustrezati standardu ISO/IEC 7810:2003/Amd. 1:2009, Identification cards – Physical characteristics, Amendment 1: Criteria for cards containing integrated circuits [9.1] X-rays	
		[Ultravijolična svetloba] ISO/IEC 10373-1:2006, Identification cards – Test methods – Part 1: General characteristics [5.11] Ultraviolet light	
		[Preskus s tremi kolesi] Tahografske kartice morajo ustrezati standardu ISO/IEC 10373-1:2006/Amd. 1:2012, Identification cards – Test methods – Part 1: General characteristics, Amendment 1 [5.22] ICC – Mechanical strength: 3 wheel test for ICCs with contacts	
		[Ovoj] Tahografske kartice morajo ustrezati standardu MasterCard CQM V2.03:2013 [11.1.3] R-L3-14-8: Wrapping Test Robustness [13.2.1.32] TM-422: Mechanical Reliability: Wrapping Test	

▼B

Št.	Preskus	Opis	Povezane zahteve
4.2	Mehanski preskusi modula čipa, vgrajenega v telo kartice-> enako kot 2.3	[Upogibanje] Tahografske kartice morajo ustrezati standardu ISO/IEC 7810:2003/Amd. 1:2009, Identification cards – Physical characteristics, Amendment 1: Criteria for cards containing integrated circuits [9.2] Dynamic bending stress Skupno število ciklov upogibanja: 4 000. [Torzija] Tahografske kartice morajo ustrezati standardu ISO/IEC 7810:2003/Amd. 1:2009, Identification cards – Physical characteristics, Amendment 1: Criteria for cards containing integrated circuits [9.3] Dynamic torsional stress Skupno število torzijskih ciklov: 4 000.	ISO/IEC 7810
5.	**Preskusi protokolov**		
5.1	ATR	Preverjanje skladnosti ATR	ISO/IEC 7816-3 TCS_14, TCS_17, TCS_18
5.2	T=0	Preverjanje skladnosti protokola T=0	ISO/IEC 7816-3 TCS_11, TCS_12, TCS_13, TCS_15
5.3	PTS	Preverjanje skladnosti ukaza PTS s preklopom s T=0 na T=1	ISO/IEC 7816-3 TCS_12, TCS_19, TCS_20, TCS_21
5.4	T=1	Preverjanje skladnosti protokola T=1	ISO/IEC 7816-3 TCS_11, TCS_13, TCS_16
6.	**Struktura kartice**		
6.1		Preskus skladnosti datotečne strukture kartice s preverjanjem prisotnosti obveznih datotek na kartici in pogojev za dostop do njih	TCS_22 to TCS_28 TCS_140 to TCS_179
7.	**Preskusi funkcionalnosti**		
7.1	Normalna obdelava	Vsaj en preskus vsake dovoljene uporabe vsakega ukaza (npr.: preverjanje ukaza UPDATE BINARY s CLA = ‘00’, CLA = ‘0C’ in z različnimi parametri P1, P2 in Lc) Preverjanje, ali so bile operacije na kartici dejansko izvedene (npr.: z branjem datoteke, na kateri je bila operacija izvedena)	TCS_29 do TCS_139

▼B

Št.	Preskus	Opis	Povezane zahteve
7.2	Sporočila napak	Vsaj en preskus vsakega sporočila o napaki (kot so opredeljena v Dodatku 2) pri vsakem ukazu Vsaj en preskus vsake generične napake (razen napak celovitosti '**6400**', ki se jih preverja v okviru varnostnega certificiranja)	
7.3	Nabor algoritmov in standardizirani parametri domen		CSM_48, CSM_50
8.	**Personalizacija**		
8.1	Optična personalizacija	Priloga 1C, poglavje 4.1 „Vidni podatki“, 230) Prednja stran mora vsebovati: informacije, značilne za izdano kartico.	230, 231, 235
		Priloga 1C, poglavje 4.1 „Vidni podatki“, 231) Prednja stran mora vsebovati: datume, ki se pišejo v obliki „dd/mm/llll“ ali „dd.mm.llll“ (dan, mesec, leto);	
		Priloga 1C, poglavje 4.1 „Vidni podatki“, 235) Tahografska kartica mora biti zaščitena pred ponarejanjem in nepooblaščenimi posegi vsaj z naslednjimi zaščitami: — v območju fotografije se morata varnostni vzorec ozadja in fotografija prekrivati.	

5. PRESKUSI ZUNANJE GNSS OPREME

Št.	Preskus	Opis	Povezane zahteve
1.	**Administrativni pregled**		
1.1	Dokumentacija	Pravilnost dokumentacije	
2.	**Vizualni pregled zunanje GNSS opreme**		
2.1	Skladnost z dokumentacijo		
2.2	Identifikacija/oznake		224 do 226
2.3	Materiali		219 do 223
3.	**Preskusi funkcionalnosti**		
3.1	Identifikacijski podatki tipala		98, 99
3.2	Povezava med zunanjim GNSS modulom in enoto v vozilu		123, 205

▼B

Št.	Preskus	Opis	Povezane zahteve
3.3	Položaj GNSS		36, 37
3.4	Vmesnik enote v vozilu, če je sprejemnik GNSS nameščen zunaj enote v vozilu		03
3.5	Nabor algoritmov in standardizirani parametri domen		CSM_48, CSM_50
4.	**Okoljski preskusi**		
4.1	Temperatura	Preverjanje funkcionalnosti z naslednjimi preskusi: preskus v skladu z ISO 16750-4, poglavje 5.1.1.2: Low temperature operation test (72 h @ – 20 °C) Ta preskus se nanaša na IEC 60068-2-1: Environmental testing – Part 2-1: Tests – Test A: Cold Preskus v skladu z ISO 16750-4, poglavje 5.1.2.2: High temperature operation test (72 h pri 70 °C) Ta preskus se nanaša na IEC 60068-2-2: Basic environmental testing procedures; part 2: tests; tests B: dry heat Preskus v skladu z ISO 16750-4, poglavje 5.3.2: Rapid change of temperature with specified transition duration (– 20 °C/70 °C, 20 ciklov, čas mirovanja 1 h pri vsaki temperaturi) Skrčen nabor preskusov (izbranih med preskusi, predpisanimi v oddelku 3 te preglednice) se lahko opravi pri nižji temperaturi, pri višji temperaturi ali med temperaturnimi cikli	213
4.2	Vlažnost	Preverjanje, ali lahko enota v vozilu prenese cikle vlage (preskus s ciklično vlažno vročino) s preskusom Db po IEC 60068-2-30, šest 24-urnih ciklov, pri vsakem spreminjanje temperature od + 25 °C do + 55 °C, relativna vlažnost 97 % pri + 25 °C in 93 % pri + 55 °C	214
4.3	Mehanski	1. Sinusoidne vibracije preverjanje, ali lahko enota v vozilu prenese sinusoidne vibracije naslednjih lastnosti: konstantni premiki med 5 in 11 Hz: konica 10 mm konstantni pospeški med 11 in 300 Hz: 5g To zahtevo se preverja s preskusom Fc po IEC 60068-2-6, z najmanjšim trajanjem preskusa 3 × 12 ur (12 ur na vsako os) ISO 16750-3 za naprave, nameščene v ločeno kabina vozila, ne zahteva preskusa s sinusoidnimi vibracijami.	219

▼B

Št.	Preskus	Opis	Povezane zahteve
		2. Naključne vibracije: Preskus v skladu z ISO 16750-3, poglavje 4.1.2.8: Test VIII: Commercial vehicle, decoupled vehicle cab Preskus z naključnimi vibracijami, 10–2 000 Hz, RMS navpično 21,3 m/s^2, RMS vodoravno 11,8 m/s^2, RMS bočno 13,1 m/s^2, 3 osi, 32 h na os, vključno s temperaturnim ciklom – 20–70 °C. Ta preskus se nanaša na IEC 60068-2-64: Environmental testing – Part 2-64: Tests – Test Fh: Vibration, broadband random and guidance 3. Udarci: mehanski udarec s 3 g, polsinusni v skladu z ISO 16750. Zgoraj opisani preskusi se opravijo na različnih vzorcih preskušane opreme.	
4.4	Zaščita pred vodo in tujki	Preskus v skladu z ISO 20653: Road vehicles – Degree of protection (IP code) – Protection of electrical equipment against foreign objects, water and access (brez sprememb parametrov)	220, 221
4.5	Prenapetostna zaščita	Preverjanje, ali enota v vozilu prenese naslednje napajanje: izvedbe 24 V: 34 V pri + 40 °C 1 uro; izvedbe 12 V: 17 V pri + 40 °C 1 uro; (ISO 16750-2, poglavje 4.3)	216
4.6	Zaščita pred zamenjavo polarnosti	Preverjanje, ali enota v vozilu prenese zamenjavo polarnosti svojega napajanja. (ISO 16750-2, poglavje 4.7)	216
4.7	Kratkostična zaščita	Preverjanje, ali so izhodni signali zaščiteni pred kratkimi stiki z napajalno napetostjo in ozemljitvijo (ISO 16750-2, poglavje 4.10)	216
5.	**Preskusi elektromagnetne združljivosti (EMC)**		
5.1	Lastna sevanja in dovzetnost	Skladnost s Pravilnikom ECE R10	218

▼B

Št.	Preskus	Opis	Povezane zahteve
5.2	Elektrostatična razelektritev	Skladnost z ISO 10605:2008 + Technical Corrigendum:2010 + AMD1:2014: +/- 4 kV za kontakt in +/– 8 kV za odvod zraka	218
5.3	Prehodna dovzetnost za prevodne motnje	Pri izvedbah 24 V: skladnost z ISO 7637-2 + Pravilnikom ECE št. 10 Rev. 3: impulz 1a: Vs = – 450 V Ri = 50 ohmov impulz 2a: Vs = + 37 V Ri = 2 ohma impulz 2b: Vs = + 20 V Ri = 0,05 ohma impulz 3a: Vs = – 150 V Ri = 50 ohmov impulz 3b: Vs = + 150 V Ri = 50 ohmov impulz 4: Vs = – 16 V Va = – 12 V t6 = 100 ms impulz 5: Vs = + 120 V Ri = 2,2 ohma td = 250 ms Pri izvedbah 12 V: skladnost z ISO 7637-1 + Pravilnikom ECE št. 10 Rev. 3: impulz 1: Vs = – 75 V Ri = 10 ohmov impulz 2a: Vs = + 37 V Ri = 2 ohma impulz 2b: Vs = + 10 V Ri = 0,05 ohma impulz 3a: Vs = – 112 V Ri = 50 ohmov impulz 3b: Vs = + 75 V Ri = 50 ohmov impulz 4: Vs = – 6 V Va = – 5 V t6 = 15 ms impulz 5: Vs = + 65 V Ri = 3 ohme td = 100 ms impulz 5 se preskuša le za enote v vozilu, namenjene za vgradnjo v vozila brez vgrajene zunanje skupne zaščite pred razbremenitvami Za predlog razbremenitve glej ISO 16750-2, 4. izdaja, poglavje 4.6.4.	218

6. PRESKUSI NAPRAVE ZA KOMUNIKACIJO NA DALJAVO

Št.	Preskus	Opis	Povezane zahteve
1.	**Administrativni pregled**		
1.1	Dokumentacija	Pravilnost dokumentacije	
2.	**Vizualni pregled**		
2.1	Skladnost z dokumentacijo		
2.2	Identifikacija/oznake		225, 226
2.3	Materiali		219 do 223
4.	**Okoljski preskusi**		
4.1	Temperatura	Preverjanje funkcionalnosti z naslednjimi preskusi: preskus v skladu z ISO 16750-4, poglavje 5.1.1.2: Low temperature operation test (72 h @ – 20 °C) Ta preskus se nanaša na IEC 60068-2-1: Environmental testing – Part 2-1: Tests – Test A: Cold	213

▼B

Št.	Preskus	Opis	Povezane zahteve
		Preskus v skladu z ISO 16750-4, poglavje 5.1.2.2: High temperature operation test (72 h pri 70 °C) Ta preskus se nanaša na IEC 60068-2-2: Basic environmental testing procedures; part 2: tests; tests B: dry heat Preskus v skladu z ISO 16750-4, poglavje 5.3.2: Rapid change of temperature with specified transition duration (– 20 °C/70 °C, 20 ciklov, čas mirovanja 1 h (?) pri vsaki temperaturi) Skrčen nabor preskusov (izbranih med preskusi, predpisanimi v oddelku 3 te preglednice) se lahko opravi pri nižji temperaturi, pri višji temperaturi ali med temperaturnimi cikli	
4.4	Zaščita pred vodo in tujki	Preskus v skladu z ISO 20653: Road vehicles – Degree of protection (IP code) – Protection of electrical equipment against foreign objects, water and access (ciljna vrednost IP40)	220, 221
5.	**Preskusi elektromagnetne združljivosti (EMC)**		
5.1	Lastna sevanja in dovzetnost	Skladnost s Pravilnikom ECE R10	218
5.2	Elektrostatična razelektritev	Skladnost z ISO 10605:2008 + Technical Corrigendum:2010 + AMD1:2014: +/– 4 kV za kontakt in +/– 8 kV za odvod zraka	218
5.3	Prehodna dovzetnost za prevodne motnje	Pri izvedbah 24 V: skladnost z ISO 7637-2 + Pravilnikom ECE št. 10 Rev. 3: impulz 1a: Vs = – 450 V Ri = 50 ohmov impulz 2a: Vs = + 37 V Ri = 2 ohma impulz 2b: Vs = + 20 V Ri = 0,05 ohma impulz 3a: Vs = – 150 V Ri = 50 ohmov impulz 3b: Vs = + 150 V Ri = 50 ohmov impulz 4: Vs = – 16 V Va = – 12 V t6 = 100 ms impulz 5: Vs = + 120 V Ri = 2,2 ohma td = 250 ms Pri izvedbah 12 V: skladnost z ISO 7637-1 + Pravilnikom ECE št. 10 Rev. 3: impulz 1: Vs = – 75 V Ri = 10 ohmov impulz 2a: Vs = + 37 V Ri = 2 ohma impulz 2b: Vs = + 10 V Ri = 0,05 ohma impulz 3a: Vs = – 112 V Ri = 50 ohmov impulz 3b: Vs = + 75 V Ri = 50 ohmov impulz 4: Vs = – 6 V Va = – 5 V t6 = 15 ms impulz 5: Vs = + 65 V Ri = 3 ohme td = 100 ms impulz 5 se preskuša le za enote v vozilu, namenjene za vgradnjo v vozila brez vgrajene zunanje skupne zaščite pred razbremenitvami Za predlog razbremenitve glej ISO 16750-2, 4. izdaja, poglavje 4.6.4.	218

▼B

7. PRESKUSI FUNKCIONALNOSTI PAPIRJA

Št.	Preskus	Opis	Povezane zahteve
1.	**Administrativni pregled**		
1.1	Dokumentacija	Pravilnost dokumentacije	
2.	**Splošni preskusi**		
2.1	Število znakov v vrstici	Vizualni pregled izpisov	172
2.2	Minimalna velikost znakov	Vizualni pregled izpisov in pregled znakov	173
2.3	Podprti nabori znakov	Tiskalnik podpira znake, določene v poglavju 4 „Nabori znakov“ Dodatka 1.	174
2.4	Ločljivost izpisov	Preverjanje homologacije tahografa in vizualni pregled izpisov	174
2.5	Čitljivost in identifikacija izpisov	Pregled izpisov Dokazovanje s poročili in zapisniki o preskusih s strani proizvajalca. Vse homologacijske številke tahografov, s katerimi se lahko uporablja papir za tiskalnik, so odtisnjene na papirju.	175, 177, 178
2.6	Dodajanje ročno napisanih opomb	Vizualni pregled: Na voljo je polje za podpis voznika. Na voljo so polja za dodatne ročno napisane vnose.	180
2.7	Dodatne podrobnosti na sprednji strani papirja.	Na sprednji in zadnji strani papirja so lahko dodatne podrobnosti in informacije. Te dodatne podrobnosti in informacije ne smejo ovirati čitljivosti izpisov. Vizualni pregled	177, 178
3.	**Preskusi glede shranjevanja**		
3.1	Suha vročina	Predkondicioniranje: 16 ur pri temperaturi + 23 C ± 2 °C/relativni vlažnosti 55 % ± 3 % Preskusno okolje: 72 ur pri temperaturi + 70 °C ± 2 °C Vzpostavitev prvotnih pogojev: 16 ur pri temperaturi + 23 C ± 2 °C/relativni vlažnosti 55 % ± 3 %	176, 178 IEC 60068-2-2-Bb
2.2	Vlažna vročina	Predkondicioniranje: 16 ur pri temperaturi + 23 C ± 2 °C/relativni vlažnosti 55 % ± 3 % Preskusno okolje: 144 ur pri temperaturi + 55 C ± 2 °C/ relativni vlažnosti 93 % ± 3 % Vzpostavitev prvotnih pogojev: 16 ur pri temperaturi + 23 C ± 2 °C/relativni vlažnosti 55 % ± 3 %	176, 178 IEC 60068-2-78-Cab

▼B

Št.	Preskus	Opis	Povezane zahteve
4.	**Preskusi papirja med delovanjem**		
4.1	Ozadje, odporno proti vlagi (nepotiskan papir)	Predkondicioniranje: 16 ur pri temperaturi + 23 C ± 2 °C/relativni vlažnosti 55 % ± 3 % Preskusno okolje: 144 ur pri temperaturi + 55 C ± 2 °C/ relativni vlažnosti 93 % ± 3 % Vzpostavitev prvotnih pogojev: 16 ur pri temperaturi + 23 C ± 2 °C/relativni vlažnosti 55 % ± 3 %	176, 178 IEC 60068-2-78-Cab
4.2	Natisljivost	Predkondicioniranje: 24 ur pri temperaturi + 40 C ± 2 °C/relativni vlažnosti 93 % ± 3 % Preskusno okolje: izpis pri + 23°C ± 2°C Vzpostavitev prvotnih pogojev: 16 ur pri temperaturi + 23 C ± 2 °C/relativni vlažnosti 55 % ± 3 %	176, 178
4.3	Odpornost proti vročini	Predkondicioniranje: 16 ur pri temperaturi + 23 C ± 2 °C/relativni vlažnosti 55 % ± 3 % Preskusno okolje: 2 uri pri temperaturi + 70 °C ± 2 °C, suha vročina Vzpostavitev prvotnih pogojev: 16 ur pri temperaturi + 23 C ± 2 °C/relativni vlažnosti 55 % ± 3 %	176, 178 IEC 60068-2-2-Bb
4.4	Odpornost proti nizki temperaturi	Predkondicioniranje: 16 ur pri temperaturi + 23 C ± 2 °C/relativni vlažnosti 55 % ± 3 % Preskusno okolje: 24 ur pri – 20 °C ± 3°C, suh mraz Vzpostavitev prvotnih pogojev: 16 ur pri temperaturi + 23 C ± 2 °C/relativni vlažnosti 55 % ± 3 %	176, 178 ISO 60068-2-1-Ab
4.5	Odpornost proti svetlobi	Predkondicioniranje: 16 ur pri temperaturi + 23 C ± 2 °C/relativni vlažnosti 55 % ± 3 % Preskusno okolje: 100 ur pri osvetljenosti 5 000 luksov in temperaturi +23 C ± 2 °C/relativni vlažnosti 55 % ± 3 % Vzpostavitev prvotnih pogojev: 16 ur pri temperaturi + 23 C ± 2 °C/relativni vlažnosti 55 % ± 3 %	176, 178

Merila čitljivosti za preskusa 3.x in 4.x:

Čitljivost izpisov je zagotovljena, če je optična gostota v skladu z naslednjimi mejnimi vrednostmi:

Natisnjeni znaki: najmanj 1,0

Ozadje (nepotiskan papir): največ 0,2

Optične gostote tako narejenih izpisov se merijo glede na DIN EN ISO 534.

Pri izpisih morajo mere ostati nespremenjene, ostati morajo jasno čitljivi.

8. PRESKUSI INTEROPERABILNOSTI

Št.	Preskus	Opis
9.1 Preskusi interoperabilnosti med enotami v vozilu in tahografskimi karticami		
1.	Medsebojna avtentikacija	Preverjanje normalnega poteka medsebojne avtentikacije enote v vozilu in tahografske kartice

▼B

Št.	Preskus	Opis
2.	Preskusi pisanja/branja	Izvedba značilnega scenarija uporabe enote v vozilu. Scenarij mora biti prilagojen vrsti preskušane kartice in mora obsegati vpise v kar največ elementarnih datotek na kartici. Preverjanje, ali so bili vsi zapisi pravilno opravljeni, s prenosom podatkov z enote v vozilu Preverjanje, ali so bili vsi zapisi pravilno opravljeni, s prenosom podatkov s kartice Preverjanje, ali je mogoče vse zapise pravilno prebrati, z dnevnimi izpisi
	9.2 Preskusi interoperabilnosti med enotami v vozilu in tipali gibanja	
1.	Povezovanje	Preverjanje normalnega poteka povezave med enotami v vozilu in tipali gibanja
2.	Preskusi delovanja	Izvedba značilnega scenarija uporabe tipala gibanja. Scenarij vključuje običajno delovanje in ustvarjanje čim več dogodkov in napak. Preverjanje, ali so bili vsi zapisi pravilno opravljeni, s prenosom podatkov z enote v vozilu Preverjanje, ali so bili vsi zapisi pravilno opravljeni, s prenosom podatkov s kartice Preverjanje, ali je mogoče vse zapise pravilno prebrati, z dnevnim izpisom
	9.3 Preskusi interoperabilnosti med enotami v vozilu in zunanjo GNSS opremo (če je primerno)	
1.	Medsebojna avtentikacija	Preverjanje normalnega poteka medsebojne avtentikacije (povezave) med enoto v vozilu in zunanjim GNSS modulom
2.	Preskusi delovanja	Izvedba značilnega scenarija uporabe zunanje GNSS opreme. Scenarij vključuje običajno delovanje in ustvarjanje toliko dogodkov in napak, kot je mogoče. Preverjanje, ali so bili vsi zapisi pravilno opravljeni, s prenosom podatkov z enote v vozilu Preverjanje, ali so bili vsi zapisi pravilno opravljeni, s prenosom podatkov s kartice Preverjanje, ali je mogoče vse zapise pravilno prebrati, z dnevnim izpisom

▼B

Dodatek 10

VARNOSTNE ZAHTEVE

Ta dodatek določa varnostne zahteve IT za sestavne dele sistema pametnih tahografov (tahografi druge generacije).

SEC_001 Naslednji sestavni deli sistema pametnih tahografov morajo biti varnostno certificirani v skladu s skupnimi merili:

— enota v vozilu,

— tahografska kartica,

— tipalo gibanja,

— zunanja GNSS oprema.

SEC_002 Minimalne varnostne zahteve IT, ki jih mora izpolnjevati vsak sestavni del, ki ga je treba varnostno certificirati, so določene v profilih zaščite sestavnih delov v skladu s skupnimi merili.

SEC_003 Evropska komisija zagotovi, da se v skladu s to prilogo financira, razvija, odobri s strani vladnih certifikacijskih organov za varnost IT, ki so združeni v delovni skupini za skupno razlaganje (JIWG), ki podpira vzajemno priznavanje certifikatov v okviru evropskega SOGIS-MRA (Soglasja o vzajemnem priznavanju potrdil o varnosti informacijskih tehnologij), in evidentira naslednje štiri profile zaščite:

— profil zaščite za enoto v vozilu,

— profil zaščite za tahografsko kartico,

— profil zaščite za tipalo gibanja,

— profil zaščite za zunanjo GNSS opremo.

Profil zaščite za enoto v vozilu velja za primere, ko je VU zasnovana za uporabo z ali brez zunanje GNSS opreme. V prvem primeru se varnostne zahteve za zunanjo GNSS opremo navedejo v namenskem profilu zaščite.

SEC_004 Pri oblikovanju varnostnih ciljev, s katerimi bodo utemeljevali svoje zahteve po varnostnem certificiranju sestavnih delov, morajo proizvajalci sestavnih delov po potrebi dopolniti in izpopolniti ustrezni profil zaščite sestavnega dela, pri tem pa ne smejo spremeniti ali izbrisati obstoječih nevarnosti, ciljev, postopkov ali specifikacij funkcij za zagotavljanje varnosti.

SEC_005 Med postopkom ocenjevanja mora biti ugotovljena dosledna skladnost takšnih posebnih varnostnih ciljev z ustreznim profilom zaščite.

SEC_006 Raven varnosti za vsak profil zaščite mora biti EAL4, povišana z varnostnima komponentama ATE_DPT.2 in AVA_VAN.5.

▼B

Dodatek 11

SKUPNI VARNOSTNI MEHANIZMI

KAZALO

PREAMBULA

DEL A SISTEM TAHOGRAFOV PRVE GENERACIJE

1. UVOD

1.1. Viri

1.2. Zapisi in kratice

2. KRIPTOGRAFSKI SISTEMI IN ALGORITMI

2.1. Kriptografski sistemi

2.2. Kriptografski algoritmi

2.2.1 Algoritem RSA

2.2.2 Zgoščevalni algoritem

2.2.3 Algoritem šifriranja podatkov

3. KLJUČI IN CERTIFIKATI

3.1. Ustvarjanje in distribucija ključev

3.1.1 Ustvarjanje in distribucija ključev RSA

3.1.2 Preskusni ključi RSA

3.1.3 Ključi tipala gibanja

3.1.4 Ustvarjanje in distribucija ključev sej T-DES

3.2. Ključi

3.3. Certifikati

3.3.1 Vsebina certifikatov

3.3.2 Izdani certifikati

3.3.3 Preverjanje in razvijanje certifikatov

4. MEHANIZEM MEDSEBOJNE AVTENTIKACIJE

5. MEHANIZMI ZAUPNOSTI, CELOVITOSTI IN AVTENTIKACIJE PRENOSA PODATKOV MED VU IN KARTICO

5.1. Varno sporočanje

5.2. Obravnava napak pri varnem sporočanju

5.3. Algoritmi izračuna kriptografskih kontrolnih vsot

5.4. Algoritmi izračuna kriptogramov za DO, povezanih z zaupnostjo

6. MEHANIZMI DIGITALNEGA PODPISA ZA PRENOS PODATKOV

6.1. Ustvarjanje podpisa

▼B

6.2.	Preverjanje podpisa
DEL B	SISTEM TAHOGRAFOV DRUGE GENERACIJE
7.	UVOD
7.1.	Viri
7.2.	Zapisi in kratice
7.3.	Opredelitve pojmov
8.	KRIPTOGRAFSKI SISTEMI IN ALGORITMI
8.1.	Kriptografski sistemi
8.2.	Kriptografski algoritmi
8.2.1	Simetrični algoritmi
8.2.2	Asimetrični algoritmi in standardizirani parametri domen
8.2.3	Zgoščevalni algoritmi
8.2.4	Nabor algoritmov
9.	KLJUČI IN CERTIFIKATI
9.1.	Asimetrični pari ključev in certifikati javnega ključa
9.1.1	Splošno
9.1.2	Evropska raven
9.1.3	Raven držav članic
9.1.4	Raven opreme: enote v vozilu
9.1.5	Raven opreme: tahografske kartice
9.1.6	Raven opreme: zunanja GNSS oprema
9.1.7	Pregled: nadomestitev certifikata
9.2.	Simetrični ključi
9.2.1	Ključi za zavarovanje komunikacije med enoto v vozilu in tipalom gibanja
9.2.2	Ključi za zavarovanje komunikacije DSRC
9.3.	Certifikati
9.3.1	Splošno
9.3.2	Vsebina certifikatov
9.3.3	Zahtevek za certifikate
10.	MEDSEBOJNA AVTENTIKACIJA IN VARNO SPOROČANJE MED VU IN KARTICO
10.1.	Splošno
10.2.	Medsebojno preverjanje verige certifikatov
10.2.1	Preverjanje verige certifikatov kartice s strani VU

▼B

10.2.2	Preverjanje verige certifikatov VU s strani kartice
10.3.	Avtentikacija VU
10.4.	Avtentikacija čipa in uskladitev ključa seje
10.5.	Varno sporočanje
10.5.1	Splošno
10.5.2	Struktura varnega sporočila
10.5.3	Prekinitev seje varnega sporočanja
11.	POVEZAVA MED VU IN ZUNANJO GNSS OPREMO, MEDSEBOJNA AVTENTIKACIJA IN VARNO SPOROČANJE
11.1.	Splošno
11.2.	Povezava med VU in zunanjo GNSS opremo
11.3.	Medsebojno preverjanje verige certifikatov
11.3.1	Splošno
11.3.2	Med povezovanjem VU in EGF
11.3.3	Med običajnim delovanjem
11.4.	Avtentikacija VU, avtentikacija čipa in uskladitev ključa seje
11.5.	Varno sporočanje
12.	POVEZAVA IN KOMUNIKACIJA MED VU IN TIPALOM GIBANJA
12.1.	Splošno
12.2.	Povezava med VU in tipalom gibanja z uporabo različnih generacij ključev
12.3.	Povezava in komunikacija med VU in tipalom gibanja z uporabo AES
12.4.	Povezava med VU in tipalom gibanja za različne generacije opreme
13.	VARNOST KOMUNIKACIJE NA DALJAVO Z DSRC
13.1.	Splošno
13.2.	Šifriranje koristnih podatkov tahografa in ustvarjanje MAC
13.3.	Preverjanje in dešifriranje koristnih podatkov tahografa
14.	PODPIS PRENOSOV PODATKOV IN PREVERJANJE PODPISOV
14.1.	Splošno
14.2.	Ustvarjanje podpisa
14.3.	Preverjanje podpisa

▼B

PREAMBULA

Ta dodatek predpisuje varnostne mehanizme za zagotavljanje:

— medsebojne avtentikacije med različnimi sestavnimi deli sistema tahografov,

— zaupnosti, celovitosti, avtentičnosti, in/ali nezatajljivosti podatkov, ki se prenašajo med različnimi sestavnimi deli sistema tahografov ali so preneseni na zunanje pomnilniške medije.

Ta dodatek je sestavljen iz dveh delov. Del A opredeljuje varnostne mehanizme za sistem tahografov prve generacije (digitalni tahograf). Del B opredeljuje varnostne mehanizme za sistem tahografov druge generacije (pametni tahograf).

Mehanizmi iz dela A tega dodatka se uporabljajo, če je vsaj eden od sestavnih delov sistema tahografov, vključen v postopek medsebojne avtentikacije in/ali prenosa podatkov, sestavni del prve generacije.

Mehanizmi iz dela B tega dodatka se uporabljajo, če sta oba sestavna dela sistema tahografov, vključena v postopek medsebojne avtentikacije in/ali prenosa podatkov, sestavna dela druge generacije.

Dodatek 15 vsebuje več informacij o uporabi sestavnih delov prve generacije v kombinaciji s sestavnimi deli druge generacije.

DEL A

SISTEM TAHOGRAFOV PRVE GENERACIJE

1. UVOD

1.1. **Viri**

V tem dodatku so uporabljeni naslednji viri:

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*. Verzija 2.0. Oktober 1998
TDES	National Institute of Standards and Technology (NIST). *FIPS Publication 46-3: Data Encryption Standard*. Osnutek 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. Prva izdaja: 1995 + Sprememba 1: 1997.
ISO/IEC 7816-6	Information Technology – Identification cards – Integrated circuit(s) cards with contacts – Part 6: Interindustry data elements. Prva izdaja: 1996 + Popr. 1: 1998.
ISO/IEC 7816-8	Information Technology – Identification cards – Integrated circuit(s) cards with contacts – Part 8: Security related interindustry commands. Prva izdaja: 1999.
ISO/IEC 9796-2	Information Technology – Security techniques – Digital signature schemes giving message recovery – Part 2: Mechanisms using a hash function. Prva izdaja: 1997.

▼B

ISO/IEC 9798-3	Information Technology – Security techniques – Entity authentication mechanisms – Part 3: Entity authentication using a public key algorithm. Druga izdaja: 1998
ISO 16844-3	Road vehicles – Tachograph systems – Part 3: Motion sensor interface.

1.2. **Zapisi in kratice**

V tem dodatku so uporabljeni naslednji zapisi in kratice:

(K_a, K_b, K_c)	šop ključev za algoritem trojnega šifriranja podatkov
CA	certifikacijski organ
CAR	referenca certifikacijskega organa
CC	kriptografska kontrolna vsota
CG	kriptogram
CH	glava ukaza
CHA	pooblastilo imetnika certifikata
CHR	referenca imetnika certifikata
D()	dešifriranje z DES
DE	podatkovni element
DO	podatkovni objekt
d	zasebni ključ RSA, zasebni eksponent
e	javni ključ RSA, javni eksponent
E()	šifriranje z DES
EQT	oprema
Hash()	zgoščena vrednost, rezultat zgoščevalne funkcije
Hash	zgoščevalna funkcija
KID	identifikator ključa
Km	ključ TDES, glavni ključ po opredelitvi iz ISO 16844-3
Km_{VU}	ključ TDES, vstavljen v enote v vozilu
Km_{WC}	ključ TDES, vstavljen v kartice servisne delavnice
m	predstavnik sporočila, cela vrednost med 0 in $n - 1$
n	ključi RSA, modul
PB	zapolnitveni bajti
PI	označevalni zapolnitveni bajt (za kriptograme DO, povezanih z zaupnostjo)
PV	nešifrirana vrednost
s	predstavnik podpisa, cela vrednost med 0 in $n - 1$
SSC	števec pošiljanj zaporedja
SM	varno sporočanje
TCBC	način delovanja z veriženjem šifrirnih blokov TDEA

▼B

TDEA	algoritem trojnega šifriranja podatkov
TLV	vrednost dolžine oznake
VU	enota v vozilu
X.C	certifikat uporabnika X, ki ga je izdal certifikacijski organ
X.CA	certifikacijski organ uporabnika X
X.CA.PK $_{o}$ X.C	operacija razvitja certifikata za ekstrakcijo javnega ključa; to je medponski operator, katerega levi operand je javni ključ certifikacijkega organa, desni operand pa certifikat, ki ga je izdal ta certifikacijski organ; rezultat je javni ključ uporabnika X, katerega certifikat je desni operand
X.PK	javni ključ RSA uporabnika X
X.PK[I]	informacija I, šifrirana po RSA ob uporabi javnega ključa uporabnika X
X.SK	zasebni ključ RSA uporabnika X
X.SK[I]	informacija I, šifrirana po RSA ob uporabi zasebnega ključa uporabnika X
‘xx’	šestnajstiška vrednost
||	operator združevanja

2. KRIPTOGRAFSKI SISTEMI IN ALGORITMI

2.1. **Kriptografski sistemi**

CSM_001 Enote v vozilu in tahografske kartice uporabljajo klasični kriptografski sistem RSA z javnim ključem za zagotavljanje naslednjih varnostnih mehanizmov:

— avtentikacija med enotami v vozilu in karticami,

— prenos ključev sej TDES med enotami v vozilu in tahografskimi karticami,

— digitalno podpisovanje podatkov, ki se prenašajo iz enot v vozilu ali tahografskih kartic na zunanje pomnilniške medije.

CSM_002 Enote v vozilu in tahografske kartice za zagotavljanje mehanizma celovitosti podatkov pri izmenjavi uporabniških podatkov med enotami v vozilu in tahografskimi karticami ter po potrebi za zagotavljanje zaupnosti izmenjave podatkov med enotami v vozilu in tahografskimi karticami uporabljajo simetrični kriptografski sistem TDES.

2.2. **Kriptografski algoritmi**

2.2.1 *Algoritem RSA*

CSM_003 Algoritem RSA v celoti opredeljujeta naslednji relaciji:

▼B

$$X.SK[m] = s = m^d \bmod n$$

$$X.PK[s] = m = s^e \bmod n$$

Podrobnejši opis funkcije RSA je na voljo v viru [PKCS1]. Javni eksponent e za izračune RSA je celo število med 3 in n-1, pri čemer je gcd(e, lcm(p-1, q-1))=1.

2.2.2 *Zgoščevalni algoritem*

CSM_004 Mehanizmi digitalnega podpisa uporabljajo zgoščevalni algoritem SHA-1, opredeljen v viru [SHA-1].

2.2.3 *Algoritem šifriranja podatkov*

CSM_005 V načinu delovanja z veriženjem šifrirnih blokov se uporabljajo algoritmi na podlagi DES.

3. KLJUČI IN CERTIFIKATI

3.1. **Ustvarjanje in distribucija ključev**

3.1.1 *Ustvarjanje in distribucija ključev RSA*

CSM_006 Ključi RSA se ustvarijo na treh funkcionalnih hierarhičnih ravneh:

— evropski ravni,

— ravni države članice,

— ravni opreme.

CSM_007 Na evropski ravni se ustvari en sam evropski par ključev (EUR.SK in EUR.PK). Evropski zasebni ključ se uporablja za certificiranje javnih ključev držav članic. Vodi se evidenca vseh certificiranih ključev. Te naloge opravlja evropski certifikacijski organ v pristojnosti in odgovornosti Evropske komisije.

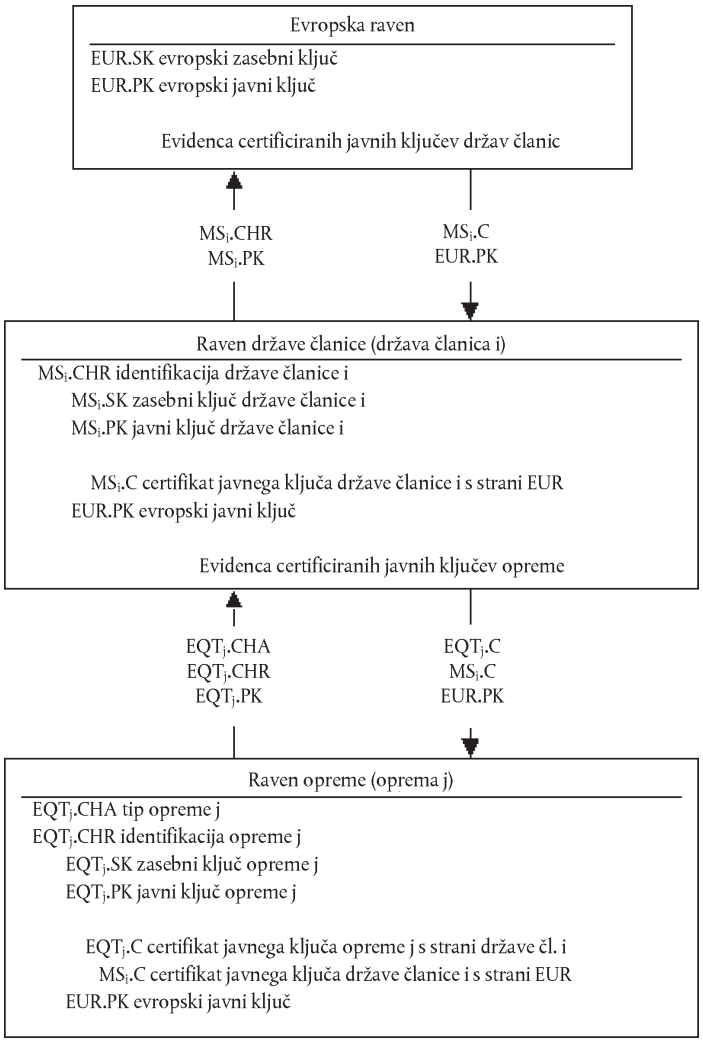
CSM_008 Na ravni držav članic se ustvari par ključev države članice (MS.SK in MS.PK). Javne ključe držav članic certificira evropski certifikacijski organ. Zasebni ključ države članice se uporablja za certificiranje javnih ključev, ki se vstavljajo v opremo (enote v vozilu in tahografske kartice). Vodi se evidenca certificiranih javnih ključev z identifikacijo opreme, za katero so namenjeni. Te naloge opravljajo certifikacijski organi držav članic. Država članica lahko redno spreminja svoj par ključev.

CSM_009 Na ravni opreme se ustvari en sam par ključev (EQT.SK in EQT.PK) in se vstavi v vsak kos opreme. Javne ključe opreme certificira certifikacijski organ države članice. Te naloge lahko opravljajo proizvajalci opreme, personalizatorji opreme ali organi držav članic. Ta par ključev se uporablja za storitve avtentikacije, digitalnega podpisovanja in šifriranja.

CSM_010 Med ustvarjanjem, prenosom (če pride do njega) in hranjenjem je treba vzdrževati zaupnost zasebnih ključev.

▼B

Naslednja slika povzema tok podatkov v tem procesu:



3.1.2 *Preskusni ključi RSA*

CSM_011 Za preskušanje opreme (vključno s preskušanjem interoperabilnosti) evropski certifikacijski organ ustvari en drugačen evropski par preskusnih ključev in vsaj dva preskusna para ključev države članice, katerih javna ključa se certificirata z evropskim zasebnim preskusnim ključem. Proizvajalci v opremo, ki jo predložijo v homologacijsko preskušanje, vstavijo preskusne ključe, certificirane z enim od teh preskusnih ključev države članice.

3.1.3 *Ključi tipala gibanja*

Med ustvarjanjem, prenosom (če pride do njega) in hranjenjem je treba vzdrževati zaupnost treh spodaj opisanih ključev TDES.

Za zagotavljanje skladnosti sestavnih delov tahografa z ISO 16844 evropski certifikacijski organ in certifikacijski organi držav članic poleg tega zagotovijo še naslednje:

CSM_036 Evropski certifikacijski organ ustvari KmVU in KmWC, dva neodvisna in edinstvena ključa TDES, ter Km, pri čemer velja: $Km = Km_{VU}$ XOR Km_{WC}. Evropski certifikacijski organ te ključe na zahtevo z ustrezno zavarovanimi postopki posreduje certifikacijskim organom držav članic.

▼B

CSM_037 Certifikacijski organi držav članic:

— uporabljajo Km za šifriranje podatkov tipal gibanja za potrebe proizvajalcev tipal gibanja (podatki, ki se šifrirajo s Km, so opredeljeni v ISO 16844-3),

— z ustrezno zavarovanimi postopki posredujejo Km_{VU} proizvajalcem enot v vozilu za vstavitev v enote v vozilu,

— zagotovijo, da se med personalizacijo kartic Km_{WC} vstavi v vse kartice servisne delavnice (`SensorInstallationSecData`v elementarni datoteki `Sensor_Installation_Data`).

3.1.4 *Ustvarjanje in distribucija ključev sej T-DES*

CSM_012 Enote v vozilu in tahografske kartice v okviru procesa medsebojne avtentikacije ustvarijo in si izmenjajo podatke, potrebne za izdelavo skupnega ključa seje TDES. Zaupnost te izmenjave podatkov je zaščitena z mehanizmom šifriranja RSA.

CSM_013 Ta ključ se uporablja za vse naslednje kriptografske operacije, ki uporabljajo varno sporočanje. Veljavnost ključa se izteče ob koncu seje (izvlek kartice ali ponastavitev kartice) in/ali po 240 uporabah (ena uporaba ključa = en ukaz, ki uporablja varno sporočanje, poslan kartici, in odziv na ta ukaz).

3.2. **Ključi**

CSM_014 Ključi RSA (na vseh ravneh) imajo naslednje dolžine: modul *n* 1 024 bitov, javni eksponent *e* največ 64 bitov, zasebni eksponent *d* 1 024 bitov.

CSM_015 Ključi TDES imajo obliko (K_a, K_b, K_a), pri čemer sta K_a in K_b neodvisna ključa dolžine 64 bitov. Nastavljen ni noben bit za ugotavljanje parnostnih napak.

3.3. **Certifikati**

CSM_016 Certifikati javnih ključev RSA so „ne-samoopisni“, „s kartico preverljivi“ certifikati (vir: ISO/IEC 7816-8).

3.3.1 *Vsebina certifikatov*

CSM_017 Certifikate javnih ključev RSA se tvori iz naslednjih podatkov v naslednjem vrstnem redu:

Podatki	Format	Bajti	Opomba
CPI	INTEGER	1	Identifikator profila certifikata (za to različico ‘01’)
CAR	OCTET STRING	8	Referenca certifikacijskega organa
CHA	OCTET STRING	7	Pooblastilo imetnika certifikata

▼B

Podatki	Format	Bajti	Opomba
EOV	TimeReal	4	Konec veljavnosti certifikata; neobvezno, če se ne uporablja, se vnese ‘FF’
CHR	OCTET STRING	8	Referenca imetnika certifikata
n	OCTET STRING	128	Javni ključ (modul)
e	OCTET STRING	8	Javni ključ (javni eksponent)
		164	

Opombe:

1. „Identifikator profila certifikata“ (CPI) določa natančno strukturo certifikata za avtentikacijo. Lahko se uporablja v opremi kot interni identifikator ustreznega seznama, ki opisuje združevanje podatkovnih elementov v certifikatu.

Seznam, povezan s to vsebino certifikata, je naslednji:

‘4D’	‘16’	‘5F 29’	‘01’	‘42’	‘08’	‘5F 4B’	‘07’	‘5F 24’	‘04’	‘5F 20’	‘08’	‘7F 49’	‘05’	‘81’	‘81 80’	‘82’	‘08’
Oznaka razširjenega seznama	Dolžina seznama	Oznaka CPI	Dolžina CPI	Oznaka CAR	Dolžina CAR	Oznaka CHA	Dolžina CHA	Oznaka EOV	Dolžina EOV	Oznaka CHR	Dolžina CHR	Oznaka javnega ključa (sestavljena)	Dolžina poznejših DO	Oznaka modula	Dolžina modula	Oznaka javnega eksponenta	Dolžina javnega eksponenta

2. „Referenca certifikacijskega organa“ (CAR) služi za identifikacijo CA, ki je izdajatelj certifikat, tako, da se podatkovni element lahko hkrati uporabi tudi kot identifikator ključa organa za referenciranje javnega ključa certifikacijskega organa (za kodiranje glej točko Identifikator ključa v nadaljevanju).

3. „Pooblastilo imetnika certifikata“ (CHA) se uporablja za identifikacijo pravic imetnika certifikata. Sestavljata ga ID tahografske aplikacije in vrsta opreme, za katero je certifikat namenjen (v skladu s podatkovnim elementom `EquipmentType`, ‘00’ za državo članico).

▼B

4. „Referenca imetnika certifikata“ (CHR) služi za nedvoumno identifikacijo imetnika certifikata, tako, da se podatkovni element lahko hkrati uporabi tudi kot identifikator ključa subjekta za referenciranje javnega ključa imetnika certifikata.

5. Identifikatorji ključev nedvoumno identificirajo imetnika certifikata ali certifikacijski organ. Kodirani so na naslednji način:

5.1 Oprema (VU ali kartica):

Podatki	Serijska številka opreme	Datum	Vrsta	Proizvajalec
Dolžina	4 bajti	2 bajta	1 bajt	1 bajt
Vrednost	Celo število	BCD-kodirana mesec (mm) in leto (ll)	Določi proizvajalec	Koda proizvajalca

Pri VU lahko proizvajalec takrat, ko zahteva certifikate, pozna ali ne pozna identifikacije opreme, v katero bodo vstavljeni ključi.

Če jo pozna, identifikacijo opreme skupaj z javnim ključem pošlje certifikacijskemu organu države članice. Certifikat bo v tem primeru vseboval identifikacijo opreme, proizvajalec pa mora zagotoviti, da bodo ključi in certifikat vstavljeni v opremo, za katero so namenjeni. Identifikator ključa ima obliko, prikazano zgoraj.

Če proizvajalec identifikacije opreme ne pozna, mora nedvoumno identificirati vsak zahtevek za certifikat in to identifikacijo skupaj z javnim ključem poslati certifikacijskemu organu države članice. Certifikat bo vseboval identifikacijo zahtevka. Proizvajalec mora po namestitvi ključa v opremo certifikacijski organ svoje države članice obvestiti o dodelitvi ključa opremi (tj. sporočiti identifikacijo zahtevka in identifikacijo opreme). Identifikator ključa ima naslednjo obliko:

Podatki	Serijska številka zahtevka za certifikat	Datum	Vrsta	Proizvajalec
Dolžina	4 bajti	2 bajta	1 bajt	1 bajt
Vrednost	Celo število	BCD-kodirana mesec (mm) in leto (ll)	‘FF’	Koda proizvajalca

▼B

5.2 Certifikacijski organ:

Podatki	Identifikacija organa	Serijska številka ključa	Dodatne informacije	Identifikator
Dolžina	4 bajti	1 bajt	2 bajta	1 bajt
Vrednost	1 bajt numerične kode države 3 bajti alfanumerične kode države	Celo število	Dodatne kode (določi CA) ‘FF FF’, če se ne uporabljajo	‘01’

Serijska številka ključa se uporablja za ločevanje med različnimi ključi države članice v primeru sprememb teh ključev.

6. Osebe, ki preverjajo certifikat, implicitno vedo, da je certificirani javni ključ RSA ključ za avtentikacijo, preverjanje digitalnega podpisa in šifriranje pri zaupnih storitvah (certifikat ne vsebuje nikakršnega identifikatorja objekta, ki bi to sporočal).

3.3.2 *Izdani certifikati*

CSM_018 Izdani certifikat je digitalni podpis z delno obnovitvijo vsebine certifikata v skladu z ISO/IEC 9796-2 (razen Priloge A4), s priloženo „referenco certifikacijskega organa“.

$$X.C = X.CA.SK[‘6A’ \parallel C_r \parallel \mathit{Hash}(Cc) \parallel ‘BC’] \parallel C_n \parallel X.CAR$$

pri čemer je vsebina certifikata = Cc =	C_r	$\parallel$	C_n
	106 bajtov		58 bajtov

Opombe:

1. Ta certifikat ima dolžino 194 bajtov.

2. CAR, skrit s podpisom, je prav tako priložen podpisu, tako da je mogoče pri preverjanju certifikata izbrati javni ključ certifikacijskega organa.

3. Oseba, ki preverja certifikat, implicitno pozna algoritem, ki ga je certifikacijski organ uporabil za podpis certifikata.

4. Seznam, povezan s to vsebino izdanega certifikata, je naslednji:

‘7F 21’	‘09’	‘5F 37’	‘81 80’	‘5F 38’	‘3A’	‘42’	‘08’
Oznaka certifikata CV (sestavljena)	Dolžina poznejših DO	Oznaka podpisa	Dolžina podpisa	Oznaka ostanka	Dolžina ostanka	Oznaka CAR	Dolžina CAR

▼B

3.3.3 *Preverjanje in razvijanje certifikatov*

Preverjanje in razvijanje certifikatov obsega preverjanje podpisa po ISO/IEC 9796-2, pridobitev vsebine certifikata in javnega ključa iz njega: X.PK = X.CA.PK o X.C ter preverjanje veljavnosti certifikata.

CSM_019 To obsega naslednje korake:

Preverjanje podpisa in pridobitev vsebine:

— Pridobitev Sign, C_n' in CAR' iz X.C:

X.C =	Sign	||	C_n'	||	CAR'
	128 bajtov		58 bajtov		8 bajtov

— Izbira ustreznega javnega ključa certifikacijskega organa iz CAR' (če ni to že storjeno na kak drug način)

— Odpiranje Sign z javnim ključem CA: Sr'= X.CA.PK [Sign],

— Preverjanje, ali se Sr' začne s ‘6A’ in konča z ‘BC’

— Izračun Cr' in H' iz: Sr' =

‘6A’	||	C_r'	||	H'	||	‘BC’
		106 bajtov		20 bajtov		

— Obnovitev vsebine certifikata C' = C_r' || C_n',

— Preverjanje, ali je Hash(C') = H'

Če so preverjanja uspešna, je certifikat pravi in njegova vsebina je C'.

Preverjanje veljavnosti. Iz C':

— Po potrebi preverjanje datuma izteka veljavnosti.

Pridobitev in shranitev javnega ključa, identifikatorja ključa, pooblastila imetnika certifikata in konca veljavnosti iz C':

— X.PK = n || e

— X.KID = CHR

— X.CHA = CHA

— X.EOV = EOV

4. MEHANIZEM MEDSEBOJNE AVTENTIKACIJE

Medsebojna avtentikacija med karticami in VU temelji na naslednjem načelu:

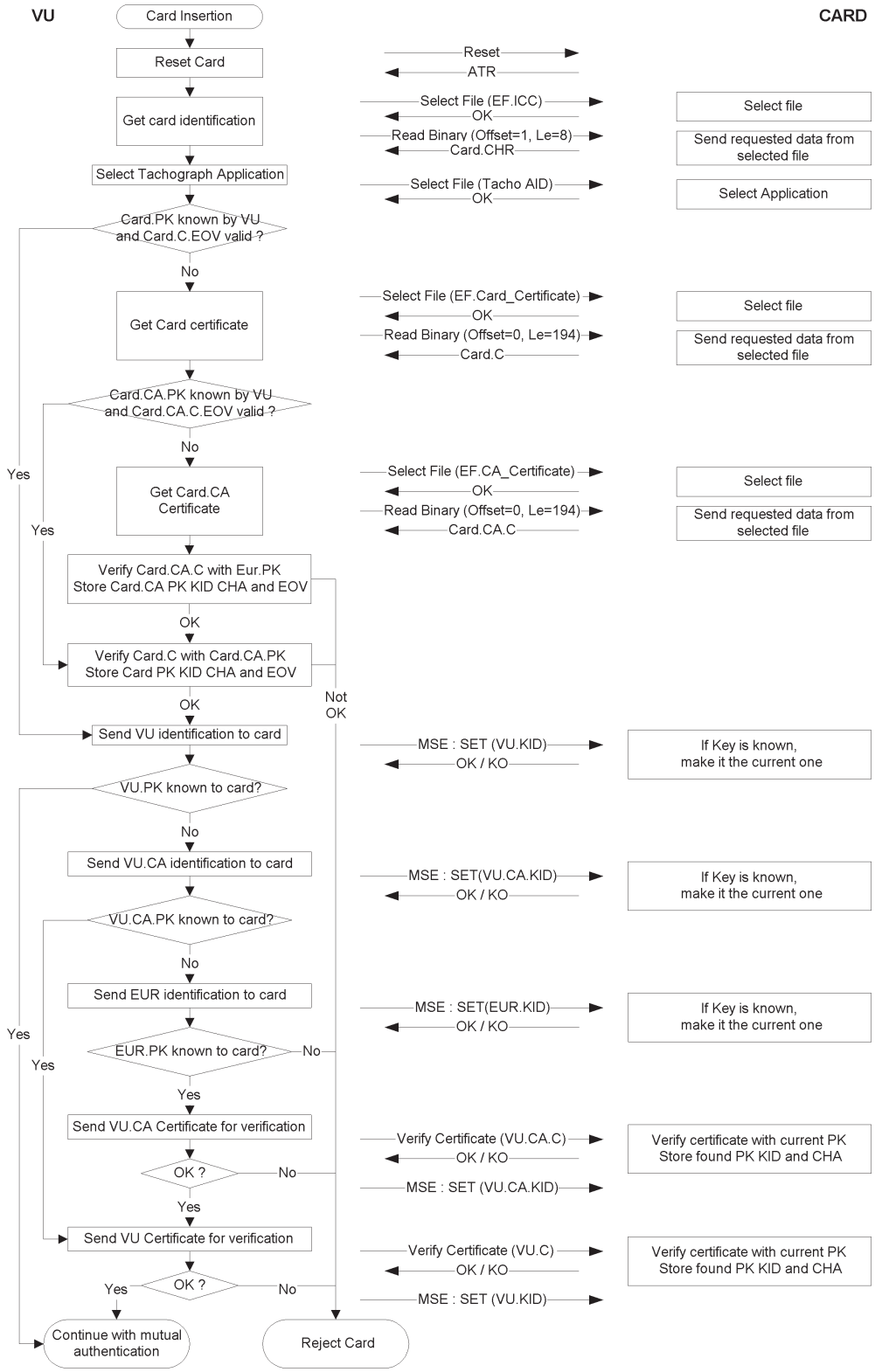
Vsaka stran drugi strani dokaže, da ima veljaven par ključev, v katerem je javni ključ certificiral certifikacijski organ države članice, ki jo je certificiral evropski certifikacijski organ.

Dokazovanje se opravi tako, da se z zasebnim ključem podpiše naključno število, ki ga je poslala druga stran; ta pa mora za preverjanje tega podpisa spet obnoviti to naključno število.

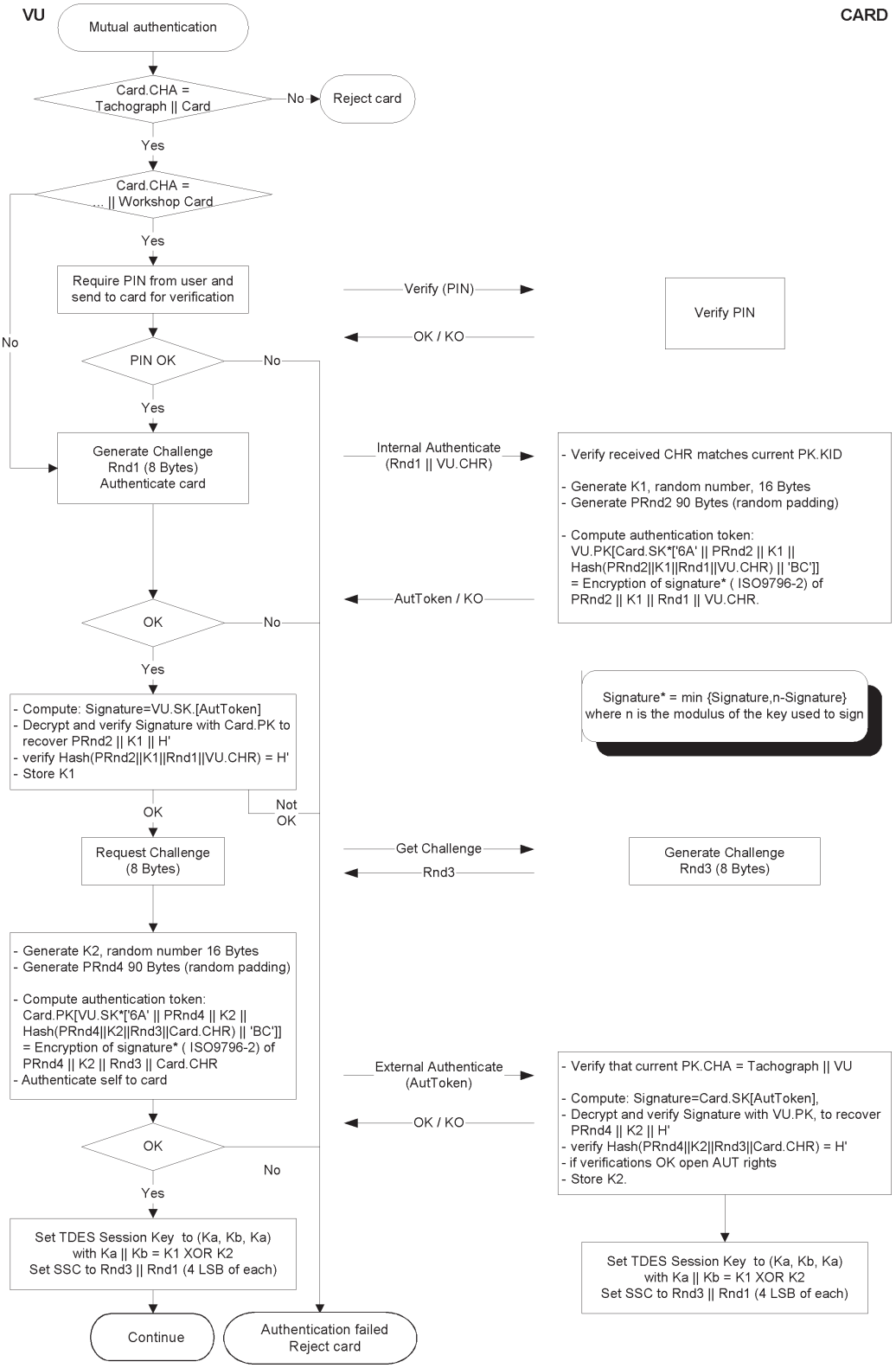
Mehanizem sproži VU ob vstavitvi kartice. Začne se z izmenjavo certifikatov in razvitjem javnih ključev, konča pa z določitvijo ključa seje.

▼B

CSM_020 Uporablja se naslednji protokol (puščice označujejo izmenjavo ukazov in podatkov (glej Dodatek 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
Not OK
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. MEHANIZMI ZAUPNOSTI, CELOVITOSTI IN AVTENTIKACIJE PRENOSA PODATKOV MED VU IN KARTICO

5.1. **Varno sporočanje**

CSM_021 Celovitost prenosov podatkov med VU in kartico mora biti zaščitena z varnim sporočanjem v skladu z viroma [ISO/IEC 7816-4] in [ISO/IEC 7816-8].

CSM_022 Kadar je treba podatke med prenosom zaščititi, se podatkom, poslanim v okviru ukaza ali odgovora, priloži podatkovni objekt kriptografske kontrolne vsote. Prejemnik preveri kriptografsko kontrolno vsoto.

CSM_023 Kriptografska kontrolna vsota v okviru ukaza poslanih podatkov združuje glavo ukaza in vse poslane podatkovne objekte (=>CLA = ‘0C’, vsi podatkovni objekti pa so opremljeni z oznakami, pri katerih velja b1=1).

CSM_024 Kadar odziv ne vsebuje nobenega podatkovnega polja, so s kriptografsko kontrolno vsoto zaščiteni bajti statusa odziva.

CSM_025 Kriptografska kontrolna vsota je dolga 4 bajte.

Pri uporabi varnega sporočanja je torej struktura ukazov in odzivov naslednja:

Uporabljeni DO so podmnožica DO varnega sporočanja, opisanih v ISO/IEC 7816-4:

Oznaka	Mnemonik	Pomen
‘81’	T_{PV}	Nešifrirana vrednost podatkov, nekodirana z BER-TLV (zaščititi s CC)
‘97’	$\mathbf{T_{LE}}$	Vrednost Le nezaščitenega ukaza (zaščititi s CC)
‘99’	T_{SW}	Statusne informacije (zaščititi s CC)
‘8E’	T_{CC}	Kriptografska kontrolna vsota
‘87’	$T_{PI\ CG}$	Označevalni zapolnitveni bajt || kriptogram (nešifrirana vrednost, nekodirana z BER-TLV)

▼B

Ob podanem nezaščitenem paru ukaz-odziv:

Glava ukaza				Telo ukaza		
CLA	INS	P1	P2	[polje L_c]	[podatkovno polje]	[polje L_e]
4 bajti				bajti L, označeni kot B_1 do B_L		

Telo odziva	Rep odziva	
[podatkovno polje]	SW1	SW2
podatkovni bajti L_r	dva bajta	

Ustrezni zaščiteni par ukaz-odziv je:

Zaščiteni ukaz:

Glava ukaza (CH)				Telo ukaza										
CLA	INS	P1	P2	[novo polje L_c]	[novo podatkovno polje]									[novo polje L_e]
‘OC’				Dolžina novega podatkovnega polja	T_{PV}	L_{PV}	PV	T_{LE}	L_{LE}	L_e	T_{CC}	L_{CC}	CC	‘00’
					‘81’	L_c	Podatkovno polje	‘97’	‘01’	L_e	‘8E’	‘04’	CC	

Podatki, ki se jih združi v kontrolno vsoto = CH || PB || T_{PV} || L_{PV} || PV || T_{LE} || L_{LE} || L_e || PB.

PB = zapolnitveni bajti (80 .. 00) v skladu z ISO-IEC 7816-4 in metodo 2 po ISO 9797.

Podatkovna objekta PV in LE nastopata le, kadar je v nezaščitenem ukazu kaj ustreznih podatkov.

Zaščiteni odziv:

1. Če podatkovno polje odziva ni prazno in ni treba zaščititi njegove zaupnosti:

Telo odziva						Rep odziva
[novo podatkovno polje]						Nova SW1 SW2
T_{PV}	L_{PV}	PV	T_{CC}	L_{CC}	CC	
‘81’	L_r	Podatkovno polje	‘8E’	‘04’	CC	

Podatki, ki se jih združi v kontrolno vsoto = T_{PV} || L_{PV} || PV || PB.

2. Če podatkovno polje odziva ni prazno in je treba zaščititi njegovo zaupnost:

▼B

Telo odziva						Rep odziva
[novo podatkovno polje]						Nova SW1 SW2
$T_{PI\ CG}$	$L_{PI\ CG}$	PI CG	T_{CC}	L_{CC}	CC	
'87'		PI ‖ CG	'8E'	'04'	CC	

Podatki, ki jih prenaša CG: podatki, nekodirani z BER-TLV, in zapolnitveni bajti.

Podatki, ki se jih združi v kontrolno vsoto = $T_{PI\ CG}$ ‖ $L_{PI\ CG}$ ‖ PI CG ‖ PB.

3. Če je podatkovno polje odziva prazno:

Telo odziva						Rep odziva
[novo podatkovno polje]						Nova SW1 SW2
T_{SW}	L_{SW}	SW	T_{CC}	L_{CC}	CC	
'99'	'02'	Nova SW1 SW2	'8E'	'04'	CC	

Podatki, ki se jih združi v kontrolno vsoto = T_{SW} ‖ L_{SW} ‖ SW ‖ PB.

5.2. **Obravnava napak pri varnem sporočanju**

CSM_026 Če tahografska kartica pri interpretiranju ukaza ugotovi napako pri SM, mora vrniti statusna bajta brez uporabe SM. Po ISO/IEC 7816-4 so za označevanje napak pri SM opredeljeni naslednji statusni bajti:

'66 88': neuspešno preverjanje kriptografske kontrolne vsote,

'69 87': manjkajo pričakovani podatkovni objekti SM,

'69 88': nepravilni podatkovni objekti SM.

CSM_027 Ko tahografska kartica vrne statusna bajta brez DO SM ali z napačnimi DO SM, mora VU prekiniti sejo.

5.3. **Algoritmi izračuna kriptografskih kontrolnih vsot**

CSM_028 Kriptografske kontrolne vsote se tvori z DES z retail MAC po ANSI X9.19:

— Začetna faza: začetni preskusni blok y0 je E(Ka, SSC).

— Naslednje zaporedne faze: preskusni bloki y1, .., yn se računajo s Ka.

— Končna faza: kriptografska kontrolna vsota se izračuna iz zadnjega preskusnega bloka yn, kot sledi: E(Ka, D(Kb, yn)),

pri čemer E() pomeni šifriranje z DES, D() pa dešifriranje z DES.

Prenesejo se štirje najpomembnejši bajti kriptografske kontrolne vsote.

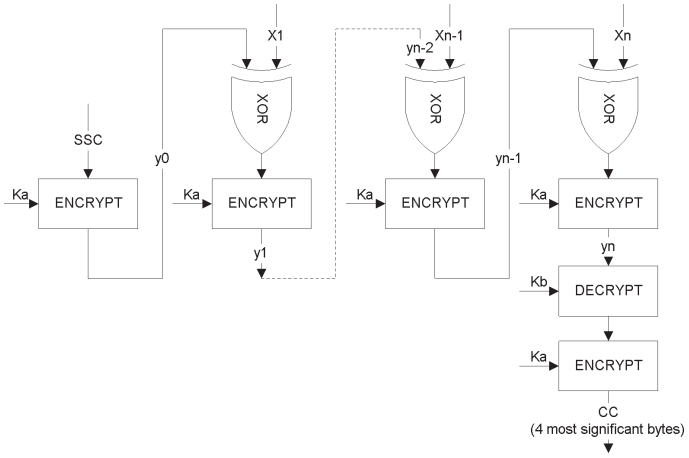
▼B

CSM_029 Med postopkom usklajevanja ključa se števec pošiljanj zaporedja (SCC) nastavi na:

začetni SCC: Rnd3 (4 bajti z najmanjšo težo) || Rnd1 (4 bajti z najmanjšo težo).

CSM_030 Števec pošiljanj zaporedja se poveča za 1 pred vsakim izračunom MAC (SCC za prvi ukaz je začetni SCC + 1, SCC za prvi odziv je začetni SCC + 2).

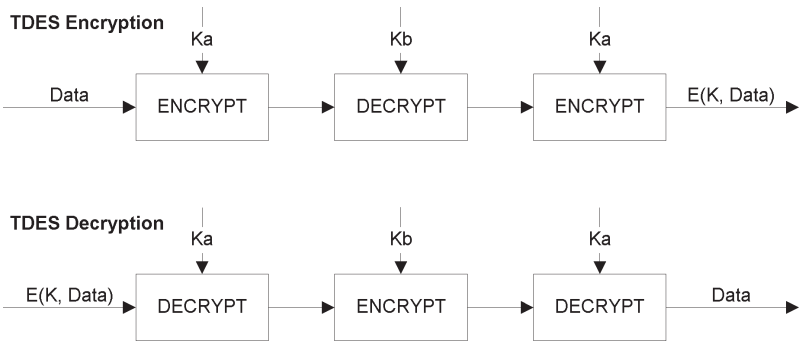
Naslednja slika prikazuje izračun retail MAC:



5.4. **Algoritmi izračuna kriptogramov za DO, povezanih z zaupnostjo**

CSM_031 Kriptograme se izračuna s TDEA v načinu delovanja TCBC v skladu z viroma [TDES] in [TDES-OP] in z ničelnim vektorjem kot blokom začetne vrednosti.

Naslednja slika prikazuje uporabo ključev v TDES:



▼B

6. MEHANIZMI DIGITALNEGA PODPISA ZA PRENOS PODATKOV

CSM_032 Inteligentna namenska oprema (IDE) podatke, prejete iz opreme (VU ali kartice) v eni seji prenosa podatkov, shrani v eni fizični podatkovni datoteki. Ta datoteka mora vsebovati certifikata MS_i.C in EQT.C. Datoteka vsebuje digitalne podpise podatkovnih blokov, kakor je predpisano v Dodatku 7 „Protokoli za prenos podatkov“.

CSM_033 Digitalni podpisi prenesenih podatkov morajo biti izdelani po shemi digitalnega podpisovanja s takim dodatkom, da je mogoče prenesene podatke po želji brati tudi brez kakršnega koli dešifriranja.

6.1. **Ustvarjanje podpisa**

CSM_034 Oprema mora ustvariti podpis podatkov po shemi podpisovanja z dodatkom, opredeljenim v viru (PKCS1), z zgoščevalno funkcijo SHA-1:

Podpis = EQT.SK[‘00’ || ‘01’ || *PS* || ‘00’ || DER(SHA-1(Data))]

PS = oktetni niz za zapolnitev z vrednostjo ‘FF’, tako da je dolžina 128.

DER(SHA-1(*M*)) pomeni šifriranje ID algoritma zgoščevalne funkcije in zgoščene vrednosti v vrednost ASN.1 tipa DigestInfo (posebna pravila kodiranja).

‘30’||‘21’||‘30’||‘09’||‘06’||‘05’||‘2B’||‘0E’||‘03’||‘02’||‘1A’||‘05’||‘00’||‘04’||‘14’||Hash Value.

6.2. **Preverjanje podpisa**

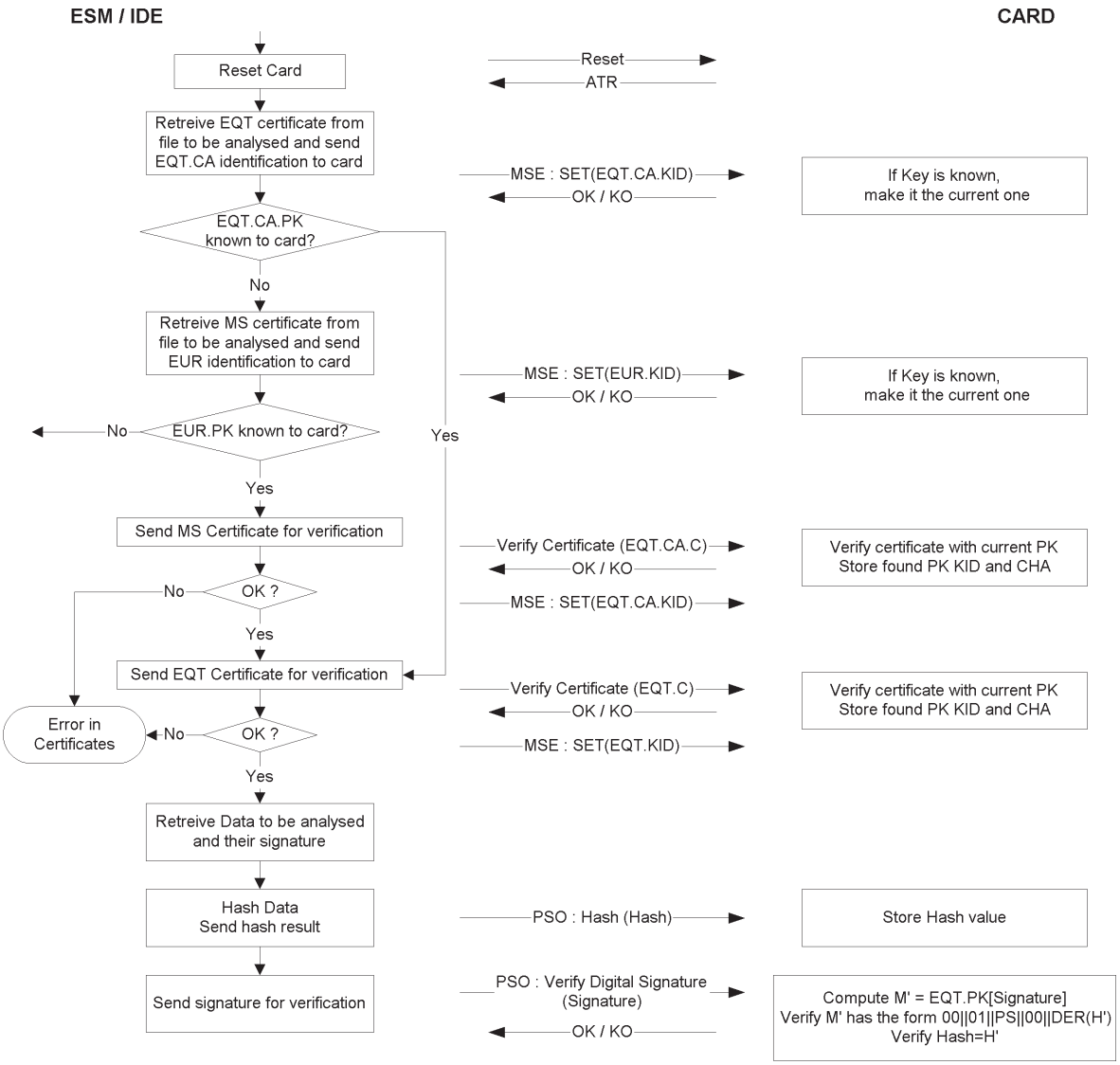
CSM_035 Preverjanje podpisa prenesenih podatkov poteka po shemi podpisovanja z dodatkom, opredeljenim v viru [PKCS1], z zgoščevalno funkcijo SHA-1.

Oseba, ki opravlja preverjanje, mora neodvisno poznati evropski javni ključ EUR.PK (in mu mora biti ključ zaupan).

Naslednja preglednica prikazuje protokol, ki ga lahko uporablja IDE z nadzorno kartico za preverjanje celovitosti podatkov, prenesenih in shranjenih na ESM (zunanji pomnilniški medij). Za dešifriranje digitalnih podpisov se uporablja nadzorna kartica. V takem primeru ni treba, da je ta funkcija vgrajena v IDE.

Oprema, s katero so bili preneseni podatki in ki je podpisala podatke, ki se jih analizira, je označena kot EQT.

▼B



DEL B

SISTEM TAHOGRAFOV DRUGE GENERACIJE

7. UVOD

7.1. **Viri**

V tem delu tega dodatka so uporabljeni naslednji viri:

AES	National Institute of Standards and Technology (NIST), FIPS PUB 197: Advanced Encryption Standard (AES), 26. november, 2001.
DSS	National Institute of Standards and Technology (NIST), FIPS PUB 186-4: Digital Signature Standard (DSS), julij 2013.
ISO 7816-4	ISO/IEC 7816-4 Identifikacijski dokumenti – Kartice z integriranim vezjem – 4. del: Organizacija, varovanje in ukazi za izmenjavo. Tretja izdaja, 15. 4. 2013.
ISO 7816-8	ISO/IEC 7816-8, Identification cards – Integrated circuit cards – Part 8: Commands for security operations. Druga izdaja 1. 6. 2004.

▼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). Četrta izdaja, 15. 12. 2008.
ISO 9797-1	ISO/IEC 9797-1, Information technology – Security techniques – Message Authentication Codes (MACs) – Part 1: Mechanisms using a block cipher. Druga izdaja, 1. 3. 2011.
ISO 10116	ISO/IEC 10116, Information technology – Security techniques – Modes of operation of an *n*-bit block cipher. Tretja izdaja, 1. 2. 2006.
ISO 16844-3	ISO/IEC 16844-3, Road vehicles – Tachograph systems – Part 3: Motion sensor interface. Prva izdaja 2004, vključno s tehničnim popravkom 1 2006.
RFC 5480	Elliptic Curve Cryptography Subject Public Key Information, marec 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, marec 2012.
SP 800-38B	National Institute of Standards and Technology (NIST), posebna izdaja 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, vezrija 2.00, 2012-06-28.

7.2. **Zapisi in kratice**

V tem dodatku so uporabljeni naslednji zapisi in kratice:

AES	napredni standard šifriranja
CA	certifikacijski organ
CAR	referenca certifikacijskega organa
CBC	veriženje šifrirnih blokov (način delovanja)
CH	glava ukaza
CHA	pooblastilo imetnika certifikata
CHR	referenca imetnika certifikata
CV	konstantni vektor
DER	posebna pravila kodiranja
DO	podatkovni objekt
DSRC	namenska komunikacija kratkega dosega
ECC	kriptografija eliptične krivulje
ECDSA	algoritem digitalnega podpisa na podlagi eliptične krivulje
ECDH	izmenjava ključev Diffie Hellman na podlagi eliptične krivulje (algoritem za uskladitev ključev)
EGF	zunanja GNSS oprema
EQT	oprema

▼B

IDE	inteligentna namenska oprema
K_M	glavni ključ tipala gibanja, ki omogoča povezavo enote v vozilu s tipalom gibanja
$K_{M\text{-}VU}$	ključ, vstavljen v enote v vozilu, ki enoti v vozilu omogoči pridobiti glavni ključ tipala gibanja, če je v enoto v vozilu vstavljena kartica servisne delavnice
$K_{M\text{-}WC}$	ključ, vstavljen v kartice servisne delavnice, ki enoti v vozilu omogoči pridobiti glavni ključ tipala gibanja, če je v enoto v vozilu vstavljena kartica servisne delavnice
MAC	koda za ugotavljanje avtentičnosti sporočila
MoS	tipalo gibanja
MSB	bit z največjo težo
PKI	infrastruktura javnega ključa
RCF	oprema za komunikacijo na daljavo
SSC	števec pošiljanj zaporedja
SM	varno sporočanje
TDES	standard trojnega šifriranja podatkov
TLV	vrednost dolžine oznake
VU	enota v vozilu
X.C	certifikat javnega ključa uporabnika X
X.CA	certifikacijski organ, ki je izdal certifikat uporabnika X
X.CAR	referenca certifikacijskega organa iz certifikata uporabnika X
X.CHR	referenca imetnika certifikata iz certifikata uporabnika X
X.PK	javni ključ uporabnika X
X.SK	zasebni ključ uporabnika X
$X.PK_{eph}$	kratkotrajni javni ključ uporabnika X
$X.SK_{eph}$	kratkotrajni zasebni ključ uporabnika X
‘xx’	šestnajstiška vrednost
||	operator združevanja

7.3. **Opredelitve pojmov**

Opredelitve pojmov, ki se uporabljajo v tem dodatku, so vključene v oddelek I Priloge 1C.

8. KRIPTOGRAFSKI SISTEMI IN ALGORITMI

8.1. **Kriptografski sistemi**

CSM_38 Enote v vozilu in tahografske kartice morajo uporabljati kriptografski sistem z javnim ključem na podlagi eliptične krivulje, da zagotovijo naslednje varnostne storitve:

— medsebojno avtentikacijo med enoto v vozilu in kartico,

— uskladitev ključev sej AES med enoto v vozilu in kartico,

▼B

— zagotavljanje avtentičnosti, celovitosti in/ali nezatajljivosti podatkov, ki se prenašajo iz enot v vozilu ali tahografskih kartic na zunanje pomnilniške medije.

CSM_39 Enote v vozilu in zunanja GNSS oprema morajo uporabljati kriptografski sistem z javnim ključem na podlagi eliptične krivulje, da zagotovijo naslednje varnostne storitve:

— povezavo enote v vozilu in zunanje GNSS opreme,

— medsebojno avtentikacijo med enoto v vozilu in zunanjo GNSS opremo,

— uskladitev ključev seje AES med enoto v vozilu in zunanjo GNSS opremo.

CSM_40 Enote v vozilu in tahografske kartice morajo uporabljati simetrični kriptografski sistem na podlagi AES, da zagotovijo naslednji varnostni storitvi:

— zagotavljanje avtentičnosti in celovitosti podatkov, izmenjanih med enoto v vozilu in tahografsko kartico,

— zagotavljanje zaupnosti podatkov, izmenjanih med enoto v vozilu in tahografsko kartico, če je primerno.

CSM_41 Enote v vozilu in zunanja GNSS oprema morajo uporabljati simetrični kriptografski sistem na podlagi AES, da zagotovijo naslednje varnostne storitve:

— zagotavljanje avtentičnosti in celovitosti podatkov, izmenjanih med enoto v vozilu in zunanjo GNSS opremo.

CSM_42 Enote v vozilu in tipala gibanja morajo uporabljati simetrični kriptografski sistem na podlagi AES, da zagotovijo naslednje varnostne storitve:

— povezavo enote v vozilu in tipala gibanja,

— medsebojno avtentikacijo med enoto v vozilu in tipalom gibanja,

— zagotavljanje zaupnosti podatkov, izmenjanih med enoto v vozilu in tipalom gibanja.

CSM_43 Enote v vozilu in nadzorne kartice morajo uporabljati simetrični kriptografski sistem na podlagi AES, da zagotovijo naslednjo varnostno storitev na vmesniku za komuniciranje na daljavo:

— zagotavljanje zaupnosti, avtentičnosti in celovitosti podatkov, izmenjanih med enoto v vozilu in nadzorno kartico.

Opombi:

— Podatki se pod nadzorom inšpektorja z opremo za komunikacijo na daljavo, ki je lahko znotraj ali zunaj enote v vozilu, prenesejo iz enote v vozilu v daljinski

▼B

poizvedovalnik (glej Dodatek 14). Daljinski poizvedovalnik prejete podatke pošlje nadzorni kartici, ki jih dešifrira in potrdi njihovo avtentičnost. Z vidika varnosti sta oprema za komunikacijo na daljavo in daljinski poizvedovalnik povsem pregledna.

— Kartica servisne delavnice ponuja enake varnostne storitve za vmesnik DSRC kot nadzorna kartica. To servisni delavnici omogoča, da potrdi pravilno delovanje vmesnika za komunikacijo na daljavo enote v vozilu, vključno z njegovo zaščito. Več informacij je na voljo v oddelku 9.2.2.

8.2. **Kriptografski algoritmi**

8.2.1 *Simetrični algoritmi*

CSM_44 Enote v vozilu, tahografske kartice, tipala gibanja in zunanja GNSS oprema morajo podpirati algoritem AES, kot je opredeljen v [AES], z dolžinami ključev 128, 192 in 256 bitov.

8.2.2 *Asimetrični algoritmi in standardizirani parametri domen*

CSM_45 Enote v vozilu, tahografske kartice in zunanja GNSS oprema morajo podpirati kriptografijo na podlagi eliptične krivulje z dolžinami ključev 256, 384 in 512/521 bitov.

CSM_46 Enote v vozilu, tahografske kartice in zunanja GNSS oprema morajo podpirati algoritem podpisa ECDSA, kot je določeno v [DSS].

CSM_47 Enote v vozilu, tahografske kartice in zunanja GNSS oprema morajo podpirati algoritem za uskladitev ključev ECKA-EG, kot je določeno v [TR 03111].

CSM_48 Enote v vozilu, tahografske kartice in zunanja GNSS oprema morajo podpirati standardizirane parametre domen, določene v Table 1, za kriptografijo na podlagi eliptične krivulje.

Preglednica 1

Standardizirani parametri domen

Ime	Velikost (biti)	Referenca	Identifikator objekta
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

Opomba: identifikatorji objekta iz zadnjega stolpca Table 1 so za krivulje Brainpool določeni v [RFC 5639], za krivulje NIST pa v [RFC 5480].

Primer 1: identifikator objekta krivulje BrainpoolP256r1 je `{iso(1) identified-organization(3) teletrust(36) algorithm(3) signaturealgorithm(3) ecSign(2) ecStdCurvesAndGeneration (8) ellipticCurve(1) versionOne(1) 7}`.

ali v zapisu s pikami: `1.3.36.3.3.2.8.1.1.7`.

Primer 2: identifikator objekta krivulje NIST P-384 je

`{iso(1) identified-organization(3) certicom(132) curve(0) 34}`.

ali v zapisu s pikami: `1.3.132.0.34`.

8.2.3 *Zgoščevalni algoritmi*

CSM_49 Enote v vozilu in tahografske kartice morajo podpirati algoritme SHA-256, SHA-384 in SHA-512, določene v [SHS].

8.2.4 *Nabor algoritmov*

CSM_50 Če se simetrični algoritem, asimetrični algoritem in/ali zgoščevalni algoritem uporabljajo skupaj in oblikujejo varnostni protokol, morajo biti njihove dolžine ključev in velikost zgoščene vrednosti (približno) enako močne. Table 2 prikazuje dovoljene nabore algoritmov:

Preglednica 2

Dovoljeni nabori algoritmov

ID nabora algoritmov	Velikost ključa ECC (bitov)	Velikost ključa AES (bitov)	Zgoščevalni algoritem	Dolžina MAC (bajtov)
CS#1	256	128	SHA-256	8
CS#2	384	192	SHA-384	12
CS#3	512/521	256	SHA-512	16

Opomba: ključi ECC velikosti 512 bitov in 521 bitov veljajo za enako močne za vse namene v tem dodatku.

9. KLJUČI IN CERTIFIKATI

9.1. **Asimetrični pari ključev in certifikati javnega ključa**

9.1.1 *Splošno*

Opomba: ključi, opisani v tem oddelku, se uporabljajo za medsebojno avtentikacijo in varno sporočanje med enotami v vozilu in tahografskimi karticami ter med enotami v vozilu in zunanjo GNSS opremo. Ti postopki so podrobno opisani v poglavjih 10 in 11 tega dodatka.

CSM_51 V okviru evropskega sistema pametnih tahografov se pari ključev ECC in pripadajoči certifikati ustvarijo in upravljajo na treh funkcionalnih hierarhičnih ravneh:

— evropski ravni,

— ravni države članice,

— ravni opreme.

▼B

CSM_52 V okviru celotnega evropskega sistema pametnih tahografov se javni in zasebni ključi ter certifikati ustvarijo, upravljajo in sporočajo z uporabo standardiziranih in varnih metod.

9.1.2 *Evropska raven*

CSM_53 Na evropski ravni se ustvari en sam edinstven par ključev ECC (EUR). Sestavljen je iz zasebnega (EUR.SK) in javnega ključa (EUR.PK). Ta par ključev je korenski par ključev celotne evropske PKI za pametne tahografe. To nalogo opravlja evropskega organa za korenske certifikate (European Root Certificate Authority – ERCA) pod vodstvom in odgovornostjo Evropske komisije.

CSM_54 ERCA za podpis korenskega certifikata (s samodejnim podpisom) evropskega javnega ključa uporabi evropski zasebni ključ in ta korenski certifikat sporoči vsem državam članicam.

CSM_55 ERCA za podpis certifikatov javnih ključev držav članic na zahtevo uporabi evropski zasebni ključ. ERCA vodi evidenco vseh podpisanih certifikatov javnih ključev držav članic.

CSM_56 Kot je prikazano na sliki 1 v oddelku 9.1.7, ERCA nov evropski korenski par ključev ustvari vsakih 17 let. Kadar koli ERCA ustvari nov evropski korenski par ključev, mora ustvariti nov korenski certifikat s samodejnim podpisom za nov evropski javni ključ. Veljavnost evropskega korenskega certifikata je 34 let in 3 mesece.

Opomba: uvedba novega korenskega para ključev pomeni tudi, da bo ERCA ustvarila nov glavni ključ za tipalo gibanja in nov glavni ključ za DSRC, glej oddelka 9.2.1.2 in 9.2.2.2.

CSM_57 Preden ERCA ustvari nov evropski korenski par ključev, mora opraviti analizo kriptografske moči, potrebne za nov par ključev, saj mora ta ostati varen naslednjih 34 let. Če je potrebno, ERCA preklopi na nabor algoritmov, ki je močnejši od trenutnega, kot je navedeno v CSM_50.

CSM_58 Kadar koli ERCA ustvari nov evropski korenski par ključev, mora pripraviti vezni certifikat za nov evropski javni ključ in ga podpisati s predhodnim evropskim zasebnim ključem. Veljavnost veznega certifikata je 17 let. To je prikazano tudi na sliki 1 v oddelku 9.1.7.

Opomba: Ker vezni certifikat vsebuje javni ključ ERCA generacije *X* in je podpisan z zasebnim ključem ERCA generacije *X-1*, vezni certifikat opremi, izdani v okviru generacije *X-1*, zagotavlja možnost, da zaupa opremi, izdani v okviru generacije *X*.

CSM_59 Po tem, ko nov korenski certifikat ključa začne veljati, ERCA v nobenem primeru ne sme uporabiti zasebnega ključa korenskega para ključev.

▼B

CSM_60 ERCA ima vedno na voljo naslednje kriptografske ključe in certifikate:

— trenutni par ključev EUR in pripadajoči certifikat,

— vse predhodne certifikate EUR, ki se jih uporablja za preverjanje certifikatov MSCA, ki so še v veljavi,

— vezne certifikate za vse generacije certifikatov EUR, razen prve.

9.1.3 *Raven držav članic*

CSM_61 Vse države članice, od katerih se zahteva podpis certifikatov tahografskih kartic, morajo ustvariti enega ali več edinstvenih parov ključev ECC, označenih kot MSCA_Card. Vse države članice, od katerih se zahteva podpis certifikatov za enote v vozilu ali zunanjo GNSS opremo, morajo poleg tega ustvariti enega ali več edinstvenih parov ključev ECC, označenih kot MSCA_VU-EGF.

CSM_62 Nalogo ustvarjanja parov ključev države članice prevzame certifikacijski organ države članice (MSCA). Kadar koli MSCA ustvari nov par ključev države članice, mora javni ključ poslati ERCA, da pridobi pripadajoč certifikat države članice, ki ga podpiše ERCA.

CSM_63 MSCA izbere moč para ključev države članice, ki je enaka moči evropskega korenskega para ključev, ki se uporablja za podpis pripadajočih certifikatov države članice.

CSM_64 Če par ključev MSCA_VU-EGF obstaja, je sestavljen iz zasebnega ključa MSCA_VU-EGF.SK in javnega ključa MSCA_VU-EGF.PK. MSCA zasebni ključ MSCA_VU-EGF.SK uporablja izključno za podpis certifikatov javnih ključev za enote v vozilu in zunanjo GNSS opremo.

CSM_65 Par ključev MSCA_Card je sestavljen iz zasebnega ključa MSCA_Card.SK in javnega ključa MSCA_Card.PK. MSCA zasebni ključ MSCA_Card.SK uporablja izključno za podpis certifikatov ključev za tahografske kartice.

CSM_66 MSCA vodi evidenco vseh podpisanih certifikatov za enote v vozilu, zunanjo GNSS opremo in kartice, prav tako pa evidentira identifikacijo opreme, za katero je vsak certifikat namenjen.

CSM_67 Veljavnost certifikata MSCA_VU-EGF je 17 let in 3 mesece. Veljavnost certifikata MSCA_Card je 7 let in 1 mesec.

CSM_68 Kot je prikazano na sliki 1 v oddelku 9.1.7, je obdobje uporabe zasebnega ključa para ključev MSCA_VU-EGF in zasebnega ključa para ključev MSCA_Card dve leti.

▼B

CSM_69 Po tem, ko obdobje uporabe zasebnega ključa para ključev MSCA_VU-EGF poteče, ga MSCA v nobenem primeru ne sme uporabiti. Prav tako MSCA v nobenem primeru ne sme uporabiti zasebnega ključa para ključev MSCA_Card po tem, ko poteče njegovo obdobje uporabe.

CSM_70 MSCA ima vedno na voljo naslednje kriptografske ključe in certifikate:

— trenutni par ključev MSCA_Card in pripadajoči certifikat,

— vse predhodne certifikate MSCA_Card, ki se jih uporablja za preverjanje certifikatov tahografskih kartic, ki so še v veljavi,

— trenutni certifikat EUR, potreben za preverjanje trenutnih certifikatov MSCA,

— vse predhodne certifikate EUR, potrebne za preverjanje vseh certifikatov MSCA, ki so še v veljavi.

CSM_71 Če se od MSCA zahteva podpis certifikatov za enote v vozilu ali zunanjo GNSS opremo, ima poleg tega še naslednje ključe in certifikate:

— trenutni par ključev MSCA_VU-EGF in pripadajoči certifikat,

— vse predhodne javne ključe MSCA_VU-EGF, ki se jih uporablja za preverjanje certifikatov za enote v vozilu ali zunanjo GNSS opremo, ki so še v veljavi.

9.1.4 *Raven opreme: enote v vozilu*

CSM_72 Za vsako enoto v vozilu se ustvarita dva edinstvena para ključev ECC, označena kot VU_MA in VU_Sign. To nalogo prevzamejo proizvajalci enote v vozilu. Kadar koli se ustvari par ključev VU, mora stran, ki ga ustvari, javni ključ poslati MSCA države, kjer ima sedež, da pridobi pripadajoči certifikat za enoto v vozilu, podpisan s strani MSCA. Zasebni ključ uporablja samo enota v vozilu.

CSM_73 Certifikata VU_MA in VU_Sign enote v vozilu imata enak datum začetka veljavnosti.

CSM_74 Proizvajalec enote v vozilu izbere moč para ključev VU, ki je enaka moči para ključev MSCA, ki se uporablja za podpis pripadajočega certifikata VU.

CSM_75 Enota v vozilu svoj par ključev VU_MA, ki je sestavljen iz zasebnega ključa VU_MA.SK in javnega ključa VU_MA.PK, uporablja izključno za avtentikacijo enote v vozilu glede na tahografske kartice in zunanjo GNSS opremo, kot je določeno v oddelkih 10.3 in 11.4 tega dodatka.

CSM_76 Enota v vozilu mora biti sposobna ustvariti kratkotrajen par ključev ECC, ki ga uporablja izključno za uskladitev ključa seje s tahografsko kartico ali zunanjo GNSS opremo, kot je določeno v oddelkih 10.4 in 11.4 tega dodatka.

▼B

CSM_77 Enota v vozilu zasebni ključ VU_Sign.SK svojega para ključev VU_Sign uporablja izključno za podpis prenesenih podatkovnih datotek, kot je določeno v poglavju 14 tega dodatka. Pripadajoči javni ključ VU_Sign.PK se uporablja izključno za preverjanje podpisov, ki jih ustvari enota v vozilu.

CSM_78 Kot je prikazano na sliki 1 v oddelku 9.1.7, je veljavnost certifikata VU_MA 15 let in 3 mesece. Veljavnost certifikata VU_Sign je prav tako 15 let in 3 mesece.

Opombi:

— Podaljšana veljavnost certifikata VU_Sign enoti v vozilu omogoča, da v prvih treh mesecih po poteku veljavnosti ustvarja veljavne podpise za prenesene podatke, kot je zahtevano v Uredbi (EU) št. 581/2010.

— Podaljšana veljavnost certifikata VU_MA je potrebna, da se enoti v vozilu v prvih treh mesecih po poteku veljavnosti omogoči avtentikacija glede na nadzorno kartico ali kartico podjetja in s tem prenos podatkov.

CSM_79 Po tem, ko pripadajočemu certifikatu poteče veljavnost, enota v vozilu v nobenem primeru ne sme uporabiti zasebnega ključa para ključev VU.

CSM_80 Ko enota v vozilu začne delovati, se parov ključev VU (razen kratkotrajnih parov ključev) in pripadajočih certifikatov enote v vozilu med praktično uporabo ne sme nadomestiti ali podaljšati.

Opombi:

— Ta zahteva ne velja za kratkotrajne pare ključev, ker te enota v vozilu ustvari vsakokrat, ko se opravi avtentikacija čipa in uskladitev ključa seje (glej oddelek 10.4). Kratkotrajni pari ključev nimajo pripadajočih certifikatov.

— Ta zahteva ne prepoveduje možnosti, da se v varnem okolju pod nadzorom proizvajalca VU statični par ključev VU med obnovo ali popravilom nadomesti.

CSM_81 Ko enote v vozilu začnejo delovati, morajo vsebovati naslednje kriptografske ključe in certifikate:

— zasebni ključ VU_MA in pripadajoči certifikat,

— zasebni ključ VU_Sign in pripadajoči certifikat,

— certifikat MSCA_VU-EGF, ki vsebuje javni ključ MSCA_VU-EGF.PK, ki se uporablja za preverjanje certifikata VU_MA in certifikata VU_Sign,

▼B

— certifikat EUR, ki vsebuje javni ključ EUR.PK, ki se uporablja za preverjanje certifikata MSCA_VU-EGF,

— certifikat EUR, katerega obdobje veljavnosti je neposredno pred obdobjem veljavnosti certifikata EUR, ki se uporablja za preverjanje certifikata MSCA_VU-EGF, če obstaja,

— vezni certifikat, ki povezuje ta dva certifikata EUR, če obstaja.

CSM_82 Poleg kriptografskih ključev in certifikatov iz CSM_81mora enota v vozilu vsebovati tudi ključe in certifikate iz dela A tega dodatka, ki enoti v vozilu omogočajo interakcijo s tahografskimi karticami prve generacije.

9.1.5 *Raven opreme: tahografske kartice*

CSM_83 Za vsako tahografsko kartico se ustvari en edinstven par ključev ECC, označen kot Card_MA. Poleg tega se za vsako vozniško kartico in vsako kartico servisne delavnice ustvari drug edinstven par ključev ESS, označen kot Card_Sign. To nalogo lahko prevzamejo proizvajalci ali personalizatorji kartic. Kadar koli se ustvari par ključev kartice, mora stran, ki ga ustvari, javni ključ poslati MSCA države, kjer ima sedež, da pridobi pripadajoči certifikat za kartico, podpisan s strani MSCA. Zasebni ključ uporablja samo tahografska kartica.

CSM_84 Certifikata Card_MA in Card_Sign vozniške kartice ali kartice servisne delavnice imata enak začetek veljavnosti.

CSM_85 Proizvajalec ali personalizator kartice izbere moč para ključev kartice, ki je enaka moči para ključev MSCA, ki se uporablja za podpis pripadajočega certifikata kartice.

CSM_86 Tahografska kartica svoj par ključev Card_MA, ki je sestavljen iz zasebnega ključa Card_MA.SK in javnega ključa Card_MA.PK, uporablja izključno za medsebojno avtentikacijo in uskladitev ključa seje glede na enote v vozilu, kot je določeno v oddelkih 10.3 in 10.4 tega dodatka.

CSM_87 Vozniška kartica ali kartica servisne delavnice zasebni ključ Card_Sign.SK svojega para ključev Card_Sign uporablja izključno za podpis prenesenih podatkovnih datotek, kot je določeno v poglavju 14 tega dodatka. Pripadajoči javni ključ Card_Sign.PK se uporablja izključno za preverjanje podpisov, ki jih ustvari kartica.

CSM_88 Veljavnost certifikata Card_MA je:

— za vozniške kartice: 5 let

— za kartice podjetja: 2 leti

— za nadzorne kartice: 2 leti

— za kartice servisne delavnice: 1 leto

▼B

CSM_89 Veljavnost certifikata Card_Sign je:

— za vozniške kartice: 5 let in 1 mesec

— za kartice servisne delavnice: 1 leto in 1 mesec

Opomba: podaljšana veljavnost certifikata Card_Sign vozniški kartici omogoča, da v prvem mesecu po poteku veljavnosti ustvarja veljavne podpise za prenesene podatke. To je potrebno v skladu z Uredbo (EU) št. 581/2010, ki zahteva, da se podatki z vozniške kartice lahko prenesejo do 28 dni po tem, ko so bili zabeleženi zadnji podatki.

CSM_90 Po tem, ko je kartica izdana, se parov ključev in pripadajočih certifikatov tahografske kartice ne sme nadomestiti ali podaljšati.

CSM_91 Ko so tahografske kartice izdane, morajo vsebovati naslednje kriptografske ključe in certifikate:

— zasebni ključ Card_MA in pripadajoči certifikat,

— za vozniške kartice in kartice servisne delavnice dodatno še: zasebni ključ Card_Sign in pripadajoči certifikat,

— certifikat MSCA_Card, ki vsebuje javni ključ MSCA_Card.PK, ki se uporablja za preverjanje certifikata Card_MA in certifikata Card_Sign,

— certifikat EUR, ki vsebuje javni ključ EUR.PK, ki se uporablja za preverjanje certifikata MSCA_Card,

— certifikat EUR, katerega obdobje veljavnosti je neposredno pred obdobjem veljavnosti certifikata EUR, ki se uporablja za preverjanje certifikata MSCA_Card, če obstaja,

— vezni certifikat, ki povezuje ta dva certifikata EUR, če obstaja.

CSM_92 Poleg kriptografskih ključev in certifikatov iz CSM_91 morajo tahografske kartice vsebovati tudi ključe in certifikate iz dela A tega dodatka, ki tem karticam omogočajo interakcijo z enotami v vozilu prve generacije.

9.1.6 *Raven opreme: zunanja GNSS oprema*

CSM_93 Za vsako zunanjo GNSS opremo se ustvari en edinstven par ključev ECC, označen kot EGF_MA. To nalogo prevzamejo proizvajalci zunanje GNSS opreme. Kadar koli se ustvari par ključev EGF_MA, mora stran, ki ga ustvari, javni ključ poslati MSCA države, kjer ima sedež, da pridobi pripadajoči certifikat EGF_MA, podpisan s strani MSCA. Zasebni ključ uporablja samo zunanja GNSS oprema.

CSM_94 Proizvajalec zunanje GNSS opreme (EGF) izbere moč para ključev EGF_MA, ki je enaka moči para ključev MSCA, ki se uporablja za podpis pripadajočega certifikata EGF_MA.

▼B

CSM_95 Zunanja GNSS oprema svoj par ključev EGF_MA, ki je sestavljen iz zasebnega ključa EGF_MA.SK in javnega ključa EGF_MA.PK, uporablja izključno za medsebojno avtentikacijo in uskladitev ključa seje glede na enote v vozilu, kot je določeno v oddelkih 11.4 in 11.4 tega dodatka.

CSM_96 Veljavnost certifikata EGF_MA je 15 let.

CSM_97 Po tem, ko pripadajočemu certifikatu poteče veljavnost, zunanja GNSS oprema za povezavo z enoto v vozilu ne sme uporabiti zasebnega ključa para ključev EGF_MA.

Opomba: kot je navedeno v oddelku 11.3.3, lahko zunanja GNSS oprema uporabi svoj zasebni ključ za medsebojno avtentikacijo z enoto v vozilu, s katero je že povezana, tudi po tem, ko veljavnost pripadajočega certifikata poteče.

CSM_98 Ko EGF začne delovati, se parov ključev EGF_MA in pripadajočega certifikata zunanje GNSS opreme med praktično uporabo ne sme nadomestiti ali podaljšati.

Opomba: ta zahteva ne prepoveduje možnosti, da se v varnem okolju pod nadzorom proizvajalca EGF par ključev EGF med obnovo ali popravilom nadomesti.

CSM_99 Ko zunanja GNSS oprema začne delovati, mora vsebovati naslednje kriptografske ključe in certifikate:

— zasebni ključ EGF_MA in pripadajoči certifikat,

— certifikat MSCA_VU-EGF, ki vsebuje javni ključ MSCA_VU-EGF.PK, ki se uporablja za preverjanje certifikata EGF_MA,

— certifikat EUR, ki vsebuje javni ključ EUR.PK, ki se uporablja za preverjanje certifikata MSCA_VU-EGF,

— certifikat EUR, katerega obdobje veljavnosti je neposredno pred obdobjem veljavnosti certifikata EUR, ki se uporablja za preverjanje certifikata MSCA_VU-EGF, če obstaja,

— vezni certifikat, ki povezuje ta dva certifikata EUR, če obstaja.

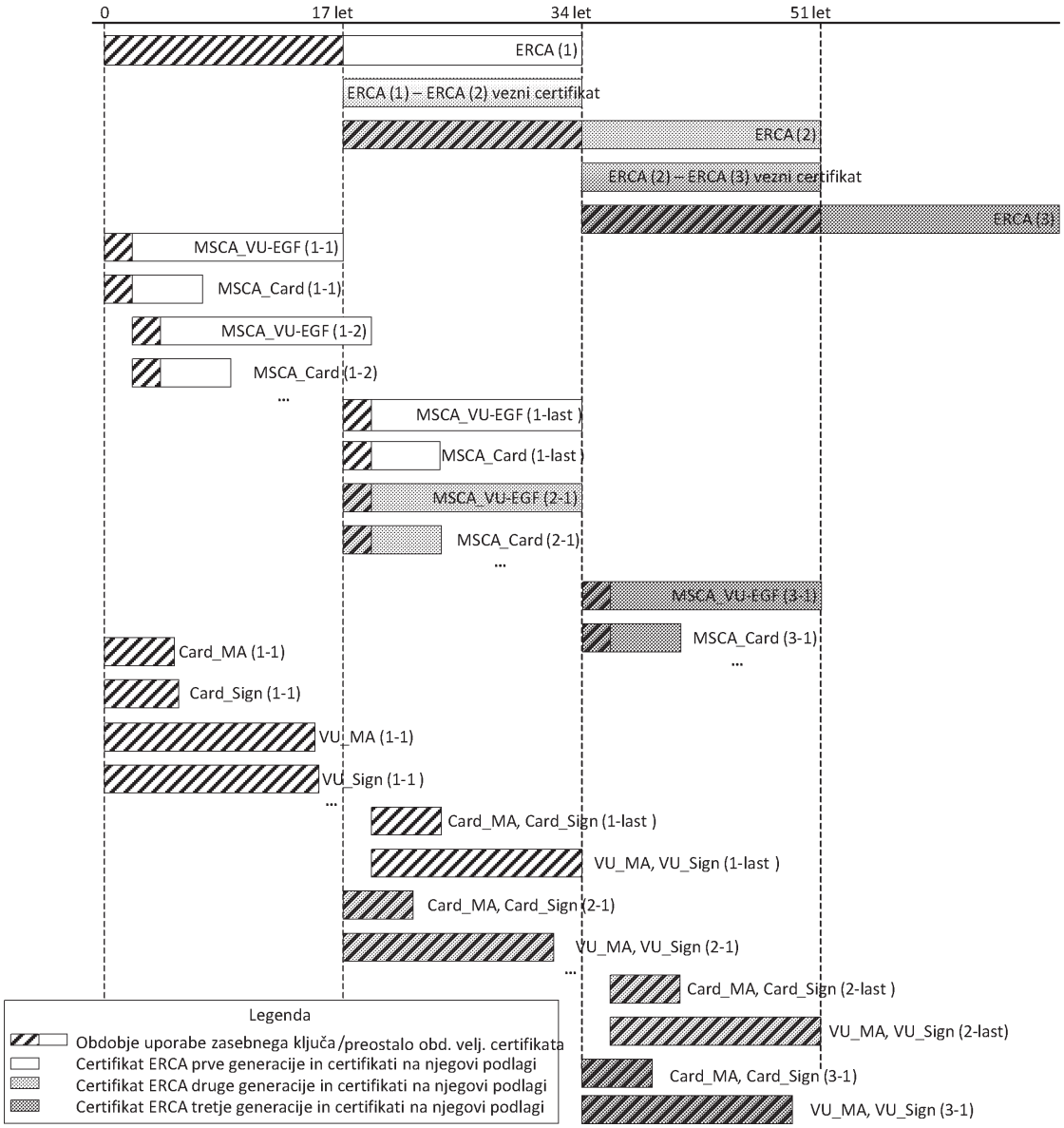
9.1.7 *Pregled: nadomestitev certifikata*

Na sliki 1 je prikazano, kako se skozi čas izdajajo in uporabljajo različne generacije korenskih certifikatov ERCA, veznih certifikatov ERCA, certifikatov MSCA in certifikatov opreme (enot v vozilu in kartic):

▼B

Slika 1

Izdajanje in uporaba različnih generacij korenskih certifikatov ERCA, veznih certifikatov ERCA, certifikatov MSCA in certifikatov opreme



Opombe k sliki 1:

1. Različne generacije korenskega certifikata so označene s številko v oklepaju. Npr. ERCA (1) pomeni korenski certifikat ERCA prve generacije; ERCA (2) druge generacije itd.

2. Drugi certifikati so označeni z dvema številkama v oklepaju, prva pomeni generacijo korenskega certifikata, v skladu s katerim so bili izdani, druga pa generacijo samega certifikata. Npr. MSCA_Card (1-1) pomeni prvi certifikat MSCA_Card, izdan v skladu z ERCA (1); MSCA_Card (2-1) pomeni prvi certifikat MSCA_Card, izdan v skladu z ERCA (2); MSCA_Card (2-last) pomeni zadnji certifikat MSCA_Card, izdan v skladu z ERCA (2); Card_MA(2-1) je prvi certifikat kartice za medsebojno avtentikacijo, izdan v skladu z ERCA (2), itd.

▼B

3. Certifikata MSCA_Card (2-1) in MSCA_Card (1-last) sta izdana skoraj, vendar ne povsem na isti datum. MSCA_Card (2-1) je prvi certifikat MSCA_Card, izdan v skladu z ERCA (2), in bo izdan malo pozneje kot MSCA_Card (1-last), ki je zadnji certifikat MSCA_Card, izdan v skladu z ERCA (1).

4. Kot je prikazano na sliki, bosta prva certifikata enote v vozilu in kartice, izdana v skladu z ERCA (2), ustvarjena skoraj dve leti pred zadnjima certifikatoma enote v vozilu in kartice, izdanima v skladu z ERCA (1). Razlog za to je, da sta certifikata enote v vozilu in kartice izdana v skladu s certifikatom MSCA, ne pa neposredno v skladu s certifikatom ERCA. Certifikat MSCA (2-1) bo izdan neposredno po tem, ko začne veljati ERCA (2), certifikat MSCA (1-last) pa bo izdan le malo pred tem, ob zadnjem trenutku veljavnosti certifikata ERCA (1). Zato bosta imela ta dva certifikata MSCA skoraj enako obdobje veljavnosti, kljub temu da pripadata različnim generacijam.

5. Obdobje veljavnosti za kartice je enako kot za vozniške kartice (5 let).

6. Da se prihrani prostor, je razlika med obdobjem veljavnosti certifikatov Card_MA in Card_Sign ter certifikatov VU_MA in VU_Sign prikazana samo za prvo generacijo.

9.2. **Simetrični ključi**

9.2.1 *Ključi za zavarovanje komunikacije med enoto v vozilu in tipalom gibanja*

9.2.1.1 *Splošno*

Opomba: bralci tega oddelka naj bi bili seznanjeni z vsebino [ISO 16844-3], ki opisuje vmesnik med enoto v vozilu in tipalom gibanja. Proces povezovanja enote v vozilu in tipala gibanja je podrobno opisan v poglavju 12 tega dodatka.

CSM_100 Za povezavo enot v vozilu in tipal gibanja, za medsebojno avtentikacijo med enotami v vozilu in tipali gibanja ter za šifriranje komunikacije med enotami v vozilu in tipali gibanja je potrebnih več simetričnih ključev, kot je prikazano v Table 3. Vsi ti ključi so ključi AES z dolžino, ki je enaka dolžini glavnega ključa tipala gibanja, ki ustreza dolžini (predvidenega) evropskega korenskega para ključev, kot je opisano v CSM_50.

Preglednica 3

Ključi za zavarovanje komunikacije med enoto v vozilu in tipalom gibanja

Ključ	Simbol	Ustvari	Način ustvarjenja	Shrani
Glavni ključ tipala gibanja – del VU	$K_{M\text{-}VU}$	ERCA	Naključno	ERCA, MSCAS, ki sodelujejo pri izdaji certifikatov VU, proizvajalci VU, enote v vozilu
Glavni ključ tipala gibanja – del servisne delavnice	$K_{M\text{-}WC}$	ERCA	Naključno	ERCA, MSCA, proizvajalci kartice, kartice servisne delavnice

▼B

Ključ	Simbol	Ustvari	Način ustvarjenja	Shrani
Glavni ključi tipala gibanja	K_M	Ni ustvarjen neodvisno	Izračunan kot $K_M = K_{M\text{-}VU}$ XOR $K_{M\text{-}WC}$	ERCA, MSCA, ki sodelujejo pri izdaji ključev tipal gibanja (neobvezno) (*)
Identifikacijski ključ	K_{ID}	Ni ustvarjen neodvisno	Izračunan kot $K_{ID} = K_M$ XOR CV, pri čemer je CV določen v CSM_106	ERCA, MSCA, ki sodelujejo pri izdaji ključev tipal gibanja (neobvezno) (*)
Povezovalni ključ	K_P	Proizvajalec tipala gibanja	Naključno	Eno tipalo gibanja
Ključ seje	K_S	VU (med povezovanjem VU in tipala gibanja)	Naključno	Ena VU in eno tipalo gibanja

(*) Shranjevanje K_M in K_{ID} je neobvezno, ker je ta dva ključa mogoče izpeljati iz $K_{M\text{-}VU}$, $K_{M\text{-}WC}$ in CV.

CSM_101 Evropski organ za korenske certifikate (ERCA) ustvari $K_{M\text{-}VU}$ in $K_{M\text{-}WC}$, dva naključna in edinstvena ključa AES, iz katerih je mogoče izračunati glavni ključ tipala gibanja K_M kot $K_{M\text{-}VU}$ XOR $K_{M\text{-}WC}$. ERCA K_M, $K_{M\text{-}VU}$ in $K_{M\text{-}WC}$ na zahtevo sporoči certifikacijskim organom držav članic.

CSM_102 ERCA vsakemu glavnem ključu tipala gibanja K_M dodeli edinstveno številko različice, ki se uporablja tudi za sestavo ključev $K_{M\text{-}VU}$ in $K_{M\text{-}WC}$ ter z njima povezanega identifikacijskega ključa K_{ID}. ERCA MSCA obvesti o številki različice, ko jim pošlje $K_{M\text{-}VU}$ in $K_{M\text{-}WC}$.

Opomba: številka različice se uporablja za razlikovanje različnih generacij teh ključev, kot je podrobno pojasnjeno v oddelku 9.2.1.2.

CSM_103 Certifikacijski organ države članice proizvajalcem enote v vozilu na zahtevo posreduje $K_{M\text{-}VU}$ in številko različice. Proizvajalci VU v vse proizvedene VU vstavijo $K_{M\text{-}VU}$ in njegovo številko različice.

CSM_104 Certifikacijski organ države članice zagotovi, da se $K_{M\text{-}WC}$ in njegova številka različice vstavita v vsako kartico servisne delavnice, izdano pod njeno pristojnostjo.

Opombi:

— Glej opis podatkovnega tipa `SensorInstallationSecData`v Dodatku 2.

— Kot je pojasnjeno v oddelku 9.2.1.2, je v eno kartico servisne delavnice po potrebi treba vstaviti več generacij $K_{M\text{-}WC}$.

▼B

CSM_105 Poleg ključa AES, določenega v CSM_104, mora MSCA zagotoviti, da se ključ TDES Km_{WC}, določen v zahtevi CSM_ 037 dela A tega dodatka, vstavi v vsako kartico servisne delavnice, izdano pod njeno pristojnostjo.

Opombi:

— to omogoča uporabo kartice servisne delavnice druge generacije za povezavo z enoto v vozilu prve generacije.

— Kartica servisne delavnice druge generacije bo vsebovala dve različni aplikaciji – eno v skladu z delom B tega dodatka in eno v skladu z delom A. Slednja bo vsebovala ključ TDES Km_{WC}.

CSM_106 MSCA, ki sodeluje pri izdaji ključev tipal gibanja, identifikacijski ključ izpelje s pomočjo računa XOR s konstantnim vektorjem CV iz glavnega ključa tipala gibanja. Vrednost CV je:

— za 128-bitne glavne ključe tipala gibanja: CV = ‘B6 44 2C 45 0E F8 D3 62 0B 7A 8A 97 91 E4 5E 83’

— za 192-bitne glavne ključe tipala gibanja: 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’

— za 256-bitne glavne ključe tipala gibanja: 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’

Opomba: konstanti vektorji se izračunajo, kot sledi:

Pi_10 = prvih 10 bitov decimalnega deleža matematične konstante π = ‘24 3F 6A 88 85 A3 08 D3 13 19’

CV_128-bits = prvih 16 bitov SHA-256(Pi_10)

CV_192-bits = prvih 24 bitov SHA-384(Pi_10)

CV_256-bits = prvih 32 bitov SHA-512(Pi_10)

CSM_107 Proizvajalci tipal gibanja za vsako tipalo gibanja ustvarijo naključen in edinstven povezovalni ključ K_P in vsak povezovalni ključ pošljejo certifikacijskemu organu države članice. MSCA z glavnim ključem tipala gibanja K_M šifrira vsak povezovalni ključ posebej in šifriran ključ vrne proizvajalcu tipala gibanja. Za vsak šifriran ključ MSCA proizvajalca tipala gibanja obvesti o številki različice ustrezajočega K_M.

Opomba: kot je pojasnjeno v oddelku 9.2.1.2, mora proizvajalec tipala gibanja za eno tipalo gibanja po potrebi ustvariti več edinstvenih povezovalnih ključev.

▼B

CSM_108 Proizvajalci tipal gibanja za vsako tipalo gibanja ustvarijo edinstveno serijsko številko in vse serijske številke pošljejo certifikacijskemu organu države članice. MSCA vsako serijsko številko posebej šifrira z identifikacijskim ključem K_{ID} in šifrirano serijsko številko vrne proizvajalcu tipala gibanja. Za vsako šifrirano serijsko številko MSCA proizvajalca tipala gibanja obvesti o številki različice ustrezajočega K_{ID}.

CSM_109 Za zahtevi CSM_107 in CSM_108 MSCA uporabi algoritem AES v načinu delovanja z veriženjem šifrirnih blokov, kot je določeno v [ISO 10116], pri čemer je parameter prepletanja $m = 1$, vektor inicializacije pa SV = '00' {16}, tj. šestnajst bajtov z binarno vrednostjo 0. MSCA po potrebi uporabi metodo zapolnjevanja 2 iz [ISO 9797-1].

CSM_110 Proizvajalec tipala gibanja v načrtovanem tipalu gibanja shrani šifriran povezovalni ključ in šifrirano serijsko številko skupaj z ustreznimi vrednostmi neformatiranega besedila in številko različice K_M in K_{ID}, uporabljenih za šifriranje.

Opomba: kot je pojasnjeno v oddelku 9.2.1.2, mora proizvajalec tipala gibanja v eno tipalo gibanja po potrebi vstaviti več šifriranih povezovalnih ključev in več šifriranih serijskih številk.

CSM_111 Poleg kriptografskega materiala na podlagi AES iz CSM_110 lahko proizvajalec tipala gibanja v vsako tipalo gibanja shrani tudi kriptografski material na podlagi TDES iz zahteve CSM_037 v delu A tega dodatka.

Opomba: to bo omogočilo povezovanje tipal gibanja druge generacije z enotami v vozilu prve generacije.

CSM_112 Dolžina ključa seje K_S, ki ga ustvari VU med povezovanjem s tipalom gibanja, ustreza dolžini svojega $K_{M\text{-}VU}$, kot je opisano v CSM_50.

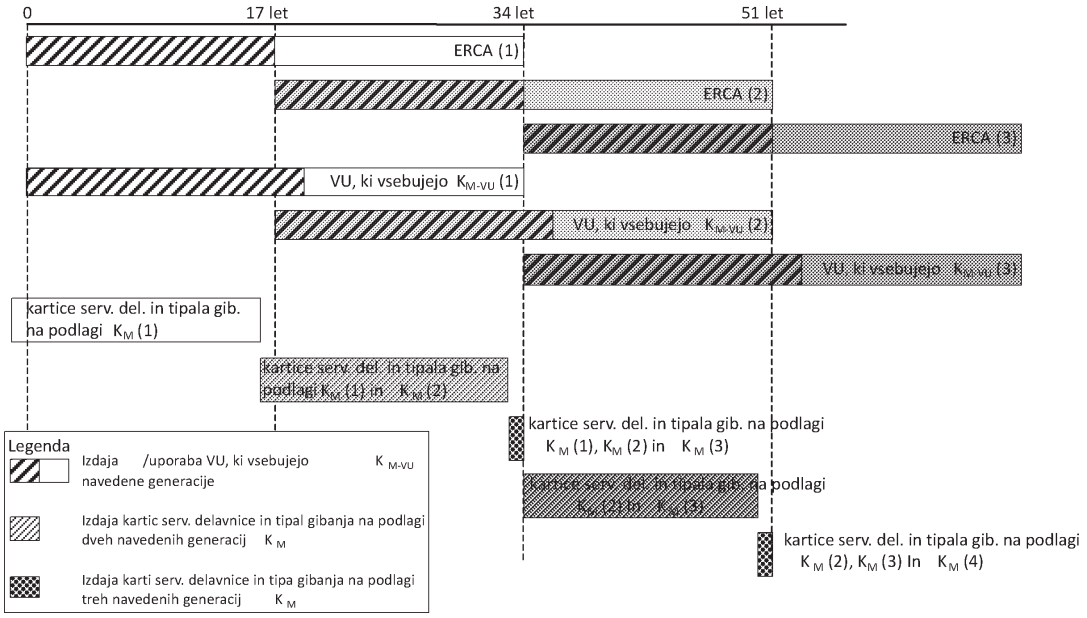
9.2.1.2 *Nadomestitev glavnega ključa tipala gibanja v opremi druge generacije*

CSM_113 Vsak glavni ključ tipala gibanja in vsi povezani ključi (glej Table 3) pripadajo določeni generaciji korenskega para ključev ERCA. Te ključe je zato treba nadomestiti vsakih 17 let. Veljavnost vsakega glavnega ključa tipala gibanja se začne eno leto pred začetkom veljavnosti povezanega korenskega para ključev ERCA in poteče, ko poteče veljavnost povezanega korenskega para ključev ERCA. To je prikazano na sliki 2.

▼B

Slika 2

Izdajanje in uporaba različnih generacij glavnega ključa tipal gibanja v enotah v vozilu, tipalih gibanja in karticah servisne delavnice



CSM_114 Vsaj eno leto, preden ERCA ustvari nov evropski korenski par ključev, kot je opisano v CSM_56, ustvari nov glavni ključ tipala gibanja K_M, in sicer tako, da ustvari nov $K_{M\text{-}VU}$ in $K_{M\text{-}WC}$. Dolžina glavnega ključa tipala gibanja ustreza predvideni moči novega evropskega korenskega para ključev v skladu s CSM_50. ERCA na zahtevo MSCA sporoči nove K_M, $K_{M\text{-}VU}$ in $K_{M\text{-}WC}$ skupaj z njihovimi številkami različice.

CSM_115 MSCA zagotovijo, da se vse veljavne generacije $K_{M\text{-}WC}$ shranijo na vsaki kartici servisne delavnice, izdani pod njihovo pristojnostjo, skupaj z njihovimi številkami različice, kot je prikazano na sliki 2.

Opomba: to pomeni, da bodo v zadnjem letu obdobja veljavnosti certifikata ERCA kartice servisne delavnice izdane s tremi različnimi generacijami $K_{M\text{-}WC}$, kot je prikazano na sliki 2.

CSM_116 V povezavi s postopkom iz CSM_107 in CSM_108: MSCA vsak povezovalni ključ K_P, ki ga prejme od proizvajalca tipala gibanja, šifrira posebej, in sicer z vsako veljavno generacijo glavnega ključa tipala gibanja K_M. MSCA prav tako posebej šifrira vsako serijsko številko, ki jo prejme od proizvajalca tipala gibanja, in sicer z vsako veljavno generacijo identifikacijskega ključa K_{ID}. Proizvajalec tipala gibanja shrani vsa šifriranja povezovalnega ključa in vsa šifriranja serijske številke v načrtovanem tipalu gibanja skupaj z ustreznimi vrednostmi neformatiranega besedila in številkami različic K_M in K_{ID}, uporabljenimi za šifriranje.

▼B

Opomba: to pomeni, da bodo v zadnjem letu obdobja veljavnosti certifikata ERCA tipala gibanja izdana s šifriranimi podatki na podlagi treh različnih generacij $K_{M\text{-}WC}$, kot je prikazano na sliki 2.

CSM_117 V povezavi s postopkom iz CSM_107: ker mora dolžina povezovalnega ključa K_P ustrezati dolžini K_M (glej CSM_100), mora proizvajalec tipala gibanja po potrebi, če imajo nadaljnje generacije K_M različne dolžine, ustvariti do tri različne povezovalne ključe za eno tipalo gibanja. V takem primeru proizvajalec vsak povezovalni ključ pošlje MSCA. MSCA zagotovi, da je vsak povezovalni ključ šifriran s pravilno generacijo glavnega ključa tipala gibanja, tj. s tisto, ki ima enako dolžino.

Opomba: če se proizvajalec tipala gibanja odloči ustvariti povezovalni ključ na podlagi TDES za tipalo gibanja druge generacije (glej CSM_111), proizvajalec MSCA obvesti, da je za šifriranje povezovalnega ključa treba uporabiti glavni ključ tipala gibanja na podlagi TDES. Razlog za to je, da je dolžina ključa TDES lahko enaka dolžini ključa AES, tako da ju MSCA ne more razlikovati samo na podlagi dolžine.

CSM_118 Proizvajalci enote v vozilu v vsako enoto v vozilu vstavijo samo eno generacijo $K_{M\text{-}VU}$ ter njegovo številko različice. Ta generacija $K_{M\text{-}VU}$ je povezana s certifikatom ERCA, na katerem temeljijo certifikati enote v vozilu.

Opombe:

— Enota v vozilu, ki temelji na certifikatu ERCA generacije *X*, lahko vsebuje samo $K_{M\text{-}VU}$ generacije *X*, tudi če je izdana po začetku veljavnosti certifikata ERCA generacije *X+1*. To je prikazano na sliki 2.

— Enota v vozilu generacije *X* se ne more povezati s tipalom gibanja generacije *X-1*.

— Ker imajo kartice servisne delavnice obdobje veljavnosti eno leto, je posledica CSM_113–CSM_118 to, da bodo vse kartice servisne delavnice ob izdaji prve enote v vozilu, ki vsebuje nov $K_{M\text{-}VU}$, vsebovale nov $K_{M\text{-}WC}$. Zato bodo take VU lahko vedno izračunale nov K_M. Poleg tega bo do takrat tudi večina novih tipal gibanja vsebovala šifrirane podatke na podlagi novega K_M.

9.2.2 *Ključi za zavarovanje komunikacije DSRC*

9.2.2.1 *Splošno*

CSM_119 Avtentičnost in zaupnost podatkov iz enote v vozilu, sporočenih nadzornemu organu po kanalu za komunikacijo na daljavo DSRC, se zagotavlja s posebnim nizom ključev AES enote v vozilu, pridobljenim iz enega samega glavnega ključa DSRC, KM_{DSRC}.

▼B

CSM_120 Glavni ključ za DSRC KM_{DSRC} je ključ AES, ki ga ERCA na varen način ustvari, shrani in razdeli. Dolžina ključa je lahko 128, 192 ali 256 bitov in ustreza dolžini evropskega korenskega para ključev, kot je opisano v CSM_50.

CSM_121 ERCA na zahtevo certifikacijskim organom držav članic na varen način sporoči glavni ključ DSRC, da lahko pridobijo posebne ključe DSRC enote v vozilu, in zagotovijo, da se glavni ključ DSRC vstavi v vse nadzorne kartice in kartice servisne delavnice, izdane pod njihovo pristojnostjo.

CSM_122 ERCA vsakemu glavnemu ključu DSRC dodeli edinstveno številko različice. ERCA MSCA obvesti o številki različice, ko jim pošlje glavni ključ DSRC.

Opomba: Številka različice se uporablja za razlikovanje različnih generacij glavnega ključa DSRC, kot je podrobno pojasnjeno v oddelku 9.2.2.2.

CSM_123 Proizvajalec enote v vozilu za vsako enoto v vozilu ustvari edinstveno serijsko številko VU in jo pošlje certifikacijskemu organu države članice, v kateri ima sedež, z zahtevkom za pridobitev dveh posebnih ključev DSRC enote v vozilu. Serijska številka VU ima podatkovni tip `VuSerialNumber`, za kodiranje pa se uporabijo posebna pravila kodiranja (DER) v skladu z [ISO 8825-1].

CSM_124 Po prejemu zahtevka za posebna ključa DSRC enote v vozilu, MSCA ustvari dva ključa AES za enoto v vozilu, in sicer K_VU_{DSRC}_ENC in K_VU_{DSRC}_MAC. Ta posebna ključa VU imata enako dolžino kot glavni ključ DSRC. MSCA uporabi funkcijo za izpeljavo ključa iz [RFC 5869]. Zgoščevalna funkcija, ki je potrebna, da se tvori funkcija HMAC-Hash, ustreza dolžini glavnega ključa DSRC, kot je opisano CSM_50. Funkcija za izpeljavo ključa iz [RFC 5869] se uporabi, kot sledi:

Korak 1 (ekstrakcija):

— *PRK* = HMAC-Hash (*salt, IKM*) pri čemer *salt* predstavlja prazen niz ‘’, *IKM* pa KM_{DSRC}.

Korak 2 (razširitev):

— *OKM* = *T(1)*, pri čemer je

T(1) = HMAC-Hash (*PRK*, *T(0)* || *info* || ‘01’) in

▼B

— *T(0)* = prazen niz (‘ ’)

— *info* = serijska številka VU, kot je določeno v CSM_123

— $K_VU_{DSRC}_ENC$ = prvih L oktetov *OKM* in

$K_VU_{DSRC}_MAC$ = zadnjih L oktetov *OKM*

pri čemer je *L* zahtevana dolžina $K_VU_{DSRC}_ENC$ in $K_VU_{DSRC}_MAC$ v oktetih.

CSM_125 MSCA proizvajalcu VU na varen način razdeli $K_VU_{DSRC}_ENC$ in $K_VU_{DSRC}_MAC$, da jih vstavi v načrtovano enoto v vozilu.

CSM_126 Ob izdaji mora imeti enota v vozilu v svojem varnem pomnilniku shranjena $K_VU_{DSRC}_ENC$ in $K_VU_{DSRC}_MAC$, da lahko zagotovi celovitost, avtentičnost in zaupnost podatkov, poslanih prek kanala za komunikacijo na daljavo. Enota v vozilu shrani tudi številko različice glavnega ključa DSRC, ki se uporablja za izpeljavo teh posebnih ključev VU.

CSM_127 Ob izdaji morajo imeti nadzorne kartice in kartice servisne delavnice v svojem varnem pomnilniku shranjen KM_{DSRC}, da lahko preverjajo celovitost in avtentičnost podatkov, ki jih VU pošlje prek kanala za komunikacijo na daljavo, in te podatke dešifrirajo. Nadzorne kartice in kartice servisne delavnice shranijo tudi številko različice glavnega ključa DSRC.

Opomba: Kot je pojasnjeno v oddelku 9.2.2.2, je v eno kartico servisne delavnice ali nadzorno kartico po potrebi treba vstaviti več generacij KM_{DSRC}.

CSM_128 MSCA vodi evidenco vseh posebnih ključev DSRC VU, ki jih je ustvarila, njihovih številk različice, prav tako pa evidentira identifikacijo VU, za katero je namenjen vsak niz ključev.

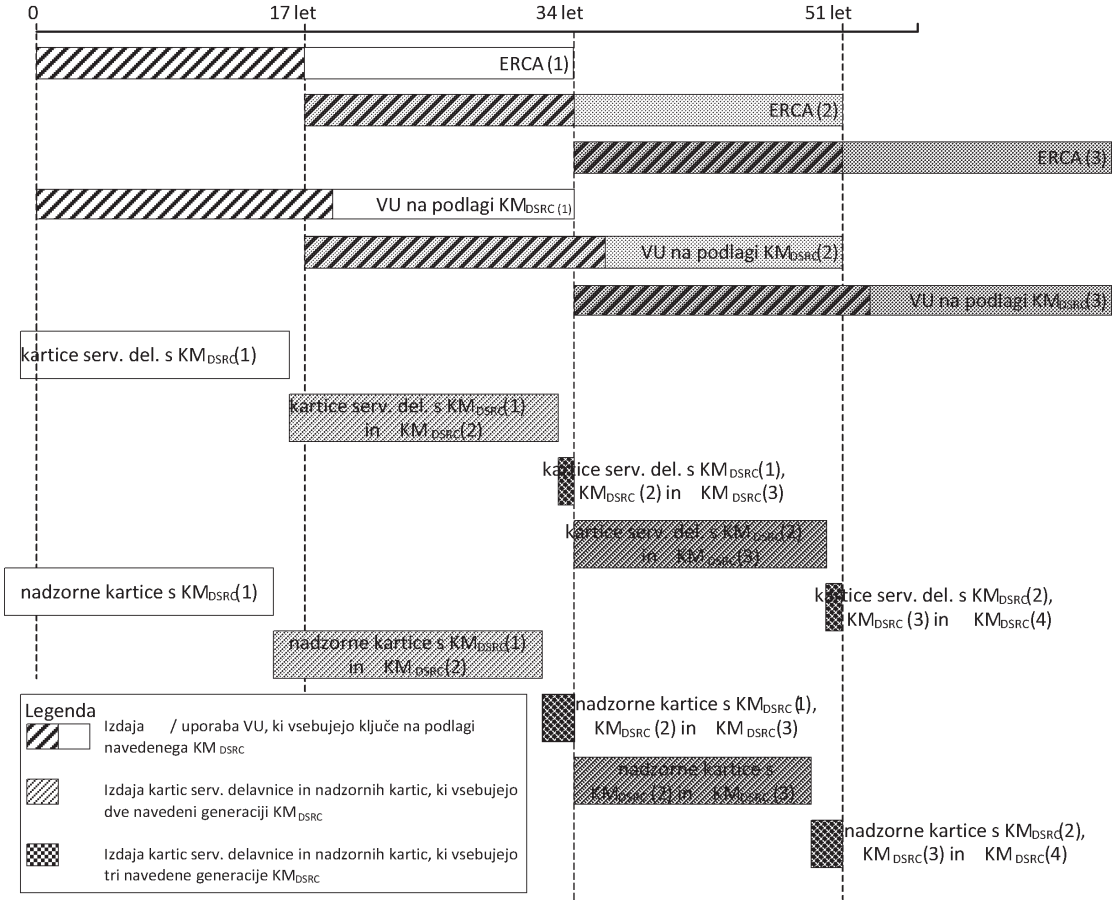
9.2.2.2 *Zamenjava glavnega ključa DSRC*

CSM_129 Vsak glavni ključ DSRC je povezan z določeno generacijo korenskega para ključev ERCA. ERCA zato glavni ključ DSRC zamenja vsakih 17 let. Veljavnost vsakega glavnega ključa DSRC se začne dve leti pred začetkom veljavnosti povezanega korenskega para ključev ERCA in poteče, ko poteče veljavnost povezanega korenskega para ključev ERCA. To je prikazano na sliki 3.

▼B

Slika 3

Izdajanje in uporaba različnih generacij glavnega ključa DSRC v enotah v vozilu, karticah servisne delavnice in nadzornih karticah



CSM_130 Vsaj dve leti, preden ERCA ustvari nov evropski korenski par ključev, kot je opisano v CSM_56, ustvari nov glavni ključ DSRC. Dolžina glavnega ključa DSRC ustreza predvideni moči novega evropskega korenskega para ključev v skladu s CSM_50. ERCA na zahtevo MSCA sporoči nov glavni ključ DSRC skupaj z njegovo številko različice.

CSM_131 MSCA zagotovijo, da se vse veljavne generacije KM_{DSRC} shranijo na vsaki nadzorni kartici, izdani pod njihovo pristojnostjo, skupaj z njihovimi številkami različice, kot je prikazano na sliki 3.

Opomba: To pomeni, da bodo v zadnjih dveh letih obdobja veljavnosti certifikata ERCA nadzorne kartice izdane s tremi različnimi generacijami KM_{DSRC}, kot je prikazano na sliki 3.

CSM_132 MSCA zagotovijo, da se vse generacije KM_{DSRC}, ki so bile veljavne vsaj eno leto in še vedno veljajo, shranijo na vsaki kartici servisne delavnice, izdani pod njihovo pristojnostjo, skupaj z njihovimi številkami različice, kot je prikazano na sliki 3.

▼B

Opomba: To pomeni, da bodo v zadnjem letu obdobja veljavnosti certifikata ERCA kartice servisne delavnice izdane s tremi različnimi generacijami KM_{DSRC}, kot je prikazano na sliki 3.

CSM_133 Proizvajalci enote v vozilu v vsako enoto v vozilu vstavijo samo en niz posebnih ključev DSRC ter njegovo številko različice. Ti ključi se izpeljejo iz generacije KM_{DSRC}, ki ustreza certifikatu ERCA, na katerem temeljijo certifikati VU.

Opombi:

— To pomeni, da enota v vozilu, ki temelji na certifikatu ERCA generacije *X*, lahko vsebuje samo K_VU_{DSRC} in K_VU_{DSRC}_MAC generacije X, tudi če je izdana po začetku veljavnosti certifikata ERCA generacije *X+1*. To je prikazano na sliki 3.

— Ker kartice servisne delavnice veljajo eno leto, nadzorne kartice pa dve leti, je posledica CSM_131–CSM_133 to, da bodo ob izdaji prve enote v vozilu, ki vsebuje posebne ključe VU, ki temeljijo na navedenem glavnem ključu, vse kartice servisne delavnice in nadzorne kartice vsebovale nov glavni ključ DSRC.

9.3. **Certifikati**

9.3.1 *Splošno*

CSM_134 Vsi certifikati v evropskem sistemu pametnih tahografov so samoopisni, s kartico preverljivi (CV) certifikati v skladu z [ISO 7816-4] in [ISO 7816-8].

CSM_135 Posebna pravila kodiranja (DER) v skladu z [ISO 8825-1] se uporabljajo za označevanje tako podatkovnih struktur ASN.1 kot podatkovnih objektov (specifičnih za aplikacije).

Opomba: rezultat takega kodiranja je takšna struktura TLV (Tag-Length-Value; Oznaka-Dolžina-Vrednost):

Oznaka: Oznaka je kodirana v enem ali dveh oktetih in označuje vsebino.

Dolžina: Dolžina je kodirana kot nepodpisano celo število v enem, dveh ali treh oktetih, kar pomeni največjo dolžino 65 535 oktetov. Uporabi se najmanjše število oktetov.

Vrednost: Vrednost je kodirana v nič ali več oktetih.

9.3.2 *Vsebina certifikatov*

CSM_136 Vsi certifikati morajo imeti strukturo, ki je določena v profilu certifikata v Table 4.

Preglednica 4

Profil certifikata, različica 1

Polje	ID polja	Oznaka	Dolžina (bajti)	Podatkovni tip ASN.1 (glej Dodatek 1)
Certifikat ECC	P	‘7F 21’	var	
Certifikat ECC	B	‘7F 4E’	var	

▼B

Polje	ID polja	Oznaka	Dolžina (bajti)	Podatkovni tip ASN.1 (glej Dodatek 1)
Identifikator profila certifikata	CPI	‘5F 29’	‘01’	`INTEGER(0..255)`
Referenca certifikacijskega organa	CAR	‘42’	‘08’	`KeyIdentifier`
Pooblastilo imetnika certifikata	CHA	‘5F 4C’	‘07’	`CertificateHolder Authorisation`
Javni ključ	PK	‘7F 49’	var	
Parametri domen	DP	‘06’	var	`OBJECT IDENTIFIER`
Javna točka	PP	‘86’	var	`OCTET STRING`
Referenca imetnika certifikata	CHR	‘5F 20’	‘08’	`KeyIdentifier`
Začetek veljavnosti certifikata	CEfD	‘5F 25’	‘04’	`TimeReal`
Potek veljavnosti certifikata	CExD	‘5F 24’	‘04’	`TimeReal`
Podpis certifikat ECC	S	‘5F 37’	var	`OCTET STRING`

Opomba: ID polja se v nadaljnjih oddelkih tega dodatka uporablja za določitev posameznih polj certifikata, npr.: X.CAR je referenca certifikacijskega organa iz certifikata uporabnika X.

9.3.2.1 Identifikator profila certifikata

CSM_137 Certifikati za navedbo uporabljenega profila certifikata uporabljajo identifikator profila certifikata. Različica 1, kot je opredeljeno v Table 4, se označi z vrednostjo ‘00’.

9.3.2.2 Referenca certifikacijskega organa

CSM_138 Referenca certifikacijskega organa se uporablja za identifikacijo javnega ključa, ki se uporablja za preverjanje podpisa certifikata. Referenca certifikacijskega organa mora biti zato enaka referenci imetnika certifikata iz certifikata ustrezne certifikacijskega organa.

CSM_139 Korenski certifikat ERCA mora imeti samodejen podpis, tj. referenca certifikacijskega organa in referenca imetnika certifikata v certifikatu morata biti enaki.

▼B

CSM_140 Za vezni certifikat ERCA mora biti referenca imetnika certifikata enaka CHR iz novega korenskega certifikata ERCA. Referenca certifikacijskega organa za vezni certifikat mora biti enaka CHR iz prejšnjega korenskega certifikata ERCA.

9.3.2.3 Pooblastilo imetnika certifikata

CSM_141 Pooblastilo imetnika certifikata se uporablja za identifikacijo tipa certifikata. Sestavljeno je iz šestih bitov z največjo težo ID aplikacije tahografa, povezane s tipom opreme, za katero je certifikat namenjen.

9.3.2.4 Javni ključ

Javni ključ vsebuje dva podatkovna elementa: standardizirane parametre domene, ki se uporabljajo z javnim ključem v certifikatu, in vrednost javne točke.

CSM_142 Podatkovni element „parametri domene“ vsebuje en identifikator objekta iz Table 1, ki označuje niz standardiziranih parametrov domene.

CSM_143 Podatkovni element „javna točka“ vsebuje javno točko. Javne točke na elipsasti krivulji se pretvorijo v oktetne nize, kot je določeno v [TR-03111]. Uporabi se nestisnjeni format kodiranja. Pri pridobivanju točke na eliptični krivulji iz njenega kodiranega formata je treba vedno opraviti preverjanja [TR-03111].

9.3.2.5 Referenca imetnika certifikata

CSM_144 Referenca imetnika certifikata je identifikator za javni ključ iz certifikata. Uporablja se za označevanje tega javnega ključa v drugih certifikatih.

CSM_145 Za certifikate kartic in zunanje GNSS opreme mora biti podatkovni tip reference imetnika certifikata `ExtendedSerialNumber`, kot je določeno v Dodatku 1.

CSM_146 Ko proizvajalec zahteva certifikat, morda ne pozna posebne serijske številke proizvajalca za VU, za katero sta namenjena navedeni certifikat in povezani zasebni ključ. Če jo pozna, mora biti podatkovni tip reference imetnika certifikata `ExtendedSerialNumber`, kot je določeno v Dodatku 1. Če je ne pozna, mora biti podatkovni tip reference imetnika certifikata `CertificateRequestID`, kot je določeno v Dodatku 1.

CSM_147 Za certifikate ERCA in MSCA mora biti podatkovni tip reference imetnika certifikata `CertificationAuthorityKID`, kot je določeno v Dodatku 1.

▼B

9.3.2.6 Začetek veljavnosti certifikata

CSM_148 Datum začetka veljavnosti certifikata označuje datum začetka in čas veljavnosti certifikata. Datum začetka veljavnosti certifikata je datum, ko se certifikat ustvari.

9.3.2.7 Potek veljavnosti certifikata

CSM_149 Datum poteka veljavnosti certifikata označuje datum poteka in čas veljavnosti certifikata.

9.3.2.8 Podpis certifikata

CSM_150 Podpis na certifikatu se ustvari na podlagi kodiranega besedila certifikata, vključno z oznako in dolžino besedila certifikata. Algoritem podpisa mora biti ECDSA, kot je določeno v [DSS], uporablja pa se zgoščevalni algoritem, ki ustreza velikosti ključa podpisnika, kot je določeno v CSM_50. Format podpisa je neformatirano besedilo, kot je določeno v [TR-03111].

9.3.3 *Zahtevek za certifikate*

CSM_151 Pri zahtevku za certifikat mora vložnik svojemu certifikacijskemu organu poslati naslednje podatke:

— identifikator profila certifikata za zahtevani certifikat,

— referenco certifikacijskega organa, ki naj bi se uporabila za podpis certifikata,

— javni ključ, ki ga je treba podpisati.

CSM_152 Poleg podatkov iz CSM_151 mora MSCA v zahtevku za certifikat ERCA poslati naslednje podatke, ki ERCA omogočijo, da ustvari referenco imetnika certifikata novega certifikata MSCA:

— numerično kodo države certifikacijskega organa (podatkovni tip `NationNumeric`, kot je opredeljeno v Dodatku 1),

— alfanumerično kodo države certifikacijskega organa (podatkovni tip `NationAlpha`, kot je opredeljeno v Dodatku 1),

— 1-bitno serijsko številko, po kateri se v primeru sprememb ključev med seboj ločijo različni ključi certifikacisjkega organa,

— 2-bitno polje, ki vsebuje dodatne posebne informacije o certifikacijskem organu.

CSM_153 Poleg podatkov iz CSM_151 mora proizvajalec opreme v zahtevku za certifikat MSCA poslati naslednje podatke, ki MSCA omogočijo, da ustvari referenco imetnika certifikata novega certifikata za opremo:

— posebni identifikator proizvajalca za tip opreme,

— serijsko številko naprave, edinstveno za proizvajalca, vrsto naprave in mesec proizvodnje (če jih pozna, glej CSM_154), sicer pa edinstven identifikator zahtevka za certifikat,

▼B

— mesec in leto izdelave opreme ali zahtevka za certifikat.

Proizvajalec zagotovi, da so ti podatki pravilni in da se certifikat, ki ga MSCA vrne, vnese v opremo, za katero je namenjen.

CSM_154 Proizvajalec, ko zahteva certifikat, morda ne pozna posebne serijske številke proizvajalca za VU, za katero sta namenjena navedeni certifikat in povezani zasebni ključ. Če jo pozna, proizvajalec VU serijsko številko pošlje MSCA. Če je ne pozna, proizvajalec označi vsak zahtevek posebej in to serijsko številko zahtevka za certifikat pošlje MSCA. Certifikat bo v tem primeru vseboval serijsko številko zahtevka za certifikat. Po vnosu certifikata v posamezno VU proizvajalec MSCA sporoči povezavo med serijsko številko zahtevka za certifikat in identifikacijo VU.

10. MEDSEBOJNA AVTENTIKACIJA IN VARNO SPOROČANJE MED VU IN KARTICO

10.1. **Splošno**

CSM_155 Na splošno varna komunikacija med enoto v vozilu in tahografsko kartico temelji na naslednjih korakih:

— prvič, vsaka stran mora drugi strani dokazati, da ima veljaven certifikat javnega ključa, podpisan s strani certifikacijskega organa države članice. Certifikat javnega ključa MSCA mora podpisati evropski organ za korenske certifikate. Ta korak se imenuje preverjanje verige certifikatov in je podrobno opisan v oddelku 10.2.

— Drugič, enota v vozilu kartici dokaže, da ima zasebni ključ, ki ustreza javnemu ključu iz predloženega certifikata. To stori s podpisom naključne številke, ki jo pošlje kartica. Kartica preveri podpis glede na naključno številko. Če je to preverjanje uspešno, se VU avtenticira. Ta korak se imenuje avtentikacija VU in je podrobno opisan v oddelku 10.3.

— Tretjič, obe strani neodvisno izračunata dva ključa seje AES z uporabo asimetričnega algoritma za uskladitev ključev. Z uporabo enega od teh ključev seje kartica ustvari kodo za ugotavljanje avtentičnosti sporočila (MAC) glede na nekatere podatke, ki jih pošlje VU. VU preveri MAC. Če je to preverjanje uspešno, se kartica avtenticira. Ta korak se imenuje avtentikacija kartice in je podrobno opisan v oddelku 10.4.

— Četrtič, VU in kartica uporabita usklajen ključ seje, da zagotovita zaupnost, celovitost in avtentičnost vseh izmenjanih sporočil. Ta korak se imenuje varno sporočanje in je podrobno opisan v oddelku 10.5.

CSM_156 Mehanizem, opisan v CSM_155, sproži enota v vozilu, kadar koli se kartica vstavi v eno od njenih rež za kartico.

▼B

10.2. **Medsebojno preverjanje verige certifikatov**

10.2.1 *Preverjanje verige certifikatov kartice s strani VU*

CSM_157 Enote v vozilu za preverjanje verige certifikatov tahografske kartice uporabljajo protokol, prikazan na sliki 4.

Opombe k sliki 4:

— Certifikati in javni ključi kartice iz slike so tisti za medsebojno avtentikacijo. V oddelku 9.1.5 so označeni kot Card_MA.

— Certifikati in javni ključi Card.CA iz slike so tisti za podpis certifikatov kartic in so navedeni v CAR certifikata kartice. V oddelku 9.1.3 so označeni kot MSCA_Card.

— Certifikat Card.CA.EUR iz slike je evropski korenski certifikat, ki je naveden v CAR certifikata Card.CA.

— Certifikat Card.Link iz slike je vezni certifikat kartice, če obstaja. Kot je določeno v oddelku 9.1.2, je to vezni certifikat za nov evropski korenski par ključev, ki ga ustvari ERCA in se podpiše s prejšnjim evropskim zasebnim ključem.

— Certifikat Card.Link.EUR je evropski korenski certifikat, ki je naveden v CAR certifikata Card.Link.

CSM_158 Kot je prikazano na sliki 4, se preverjanje verige certifikatov kartice začne ob vstavitvi kartice. Enota v vozilu iz EF ICC prebere referenco imetnika kartice (`cardExtendedSerialNumber`). VU preveri, če pozna kartico, tj. če je v preteklosti že uspešno preverila verigo certifikatov kartice in jo shranila za prihodnjo uporabo. Če jo pozna in je certifikat kartice še veljaven, se postopek nadaljuje s preverjanjem verige certifikatov VU. Če je ne pozna, VU iz kartice zaporedoma prebere certifikat MSCA_Card, ki se uporablja za preverjanje certifikata kartice, certifikat Card.CA.EUR, ki se uporablja za preverjanje certifikata MSCA_Card, in po potrebi vezni certifikat, dokler ne najde certifikata, ki ga pozna in lahko preveri. Če najde tak certifikat, ga uporabi za preverjanje osnovnih certifikatov kartice, ki jih je prebrala iz kartice. Če je uspešna, se postopek nadaljuje s preverjanjem verige certifikatov VU. Če ni, VU kartico ignorira.

▼B

Opomba: VU lahko prepozna certifikat Card.CA.EUR na tri načine:

— certifikat Card.CA.EUR je enak certifikatu EUR VU;

— certifikat Card.CA.EUR je predhodnik certifikata EUR VU in VU je ta certifikat vsebovala že ob izdaji (glej CSM_81);

— certifikat Card.CA.EUR je naslednik certifikata EUR VU in VU je v preteklosti prejela vezni certifikat iz druge tahografske kartice, ga preverila in shranila za prihodnjo referenco.

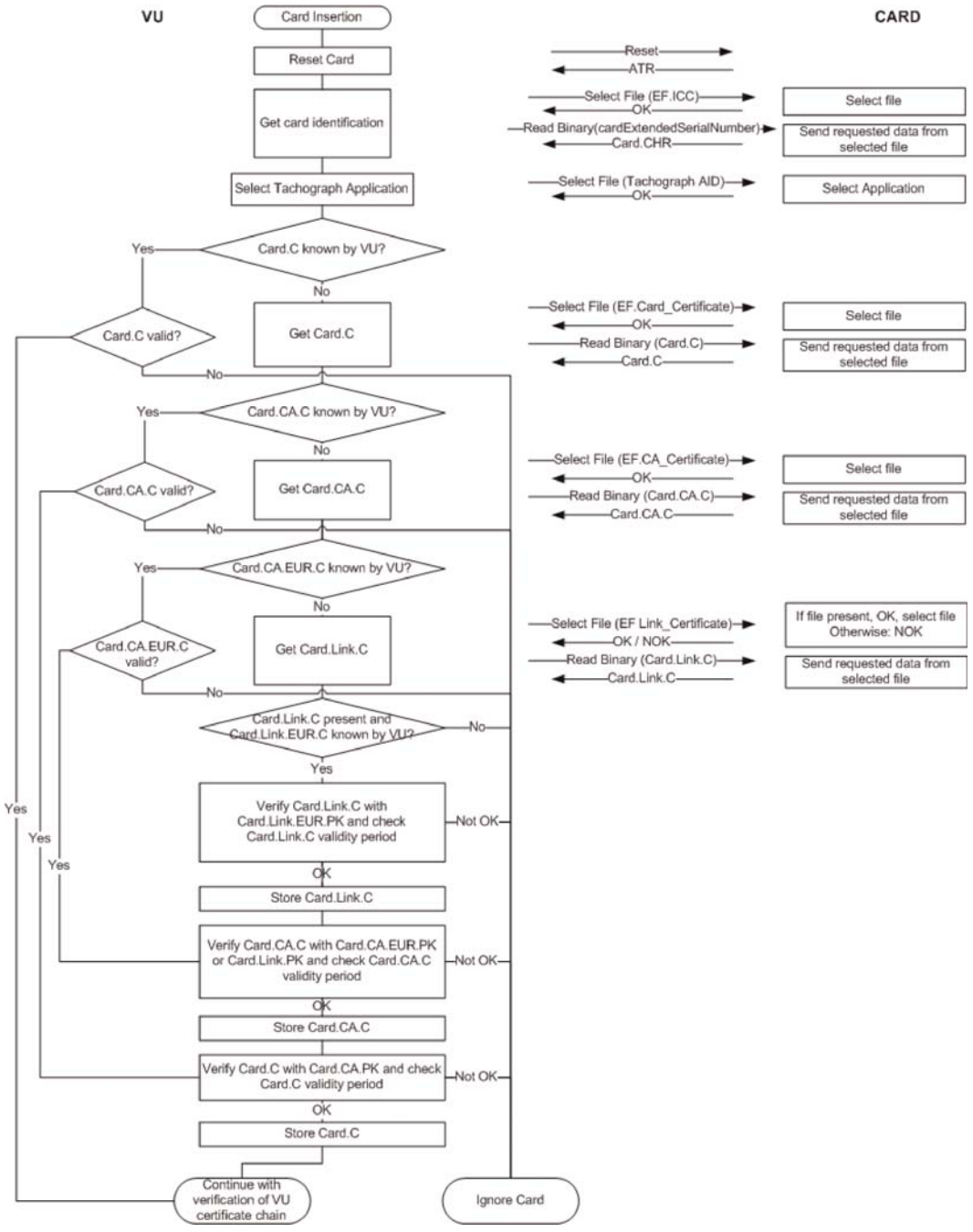
CSM_159 Kot je prikazano na sliki 4, lahko VU, potem ko preveri avtentičnost in veljavnost prej nepoznanega certifikata, ta certifikat shrani za prihodnjo uporabo, tako da ji ni več treba preverjati avtentičnosti navedenega certifikata, če ji je ponovno predložen. Namesto da shrani celoten certifikat lahko VU shrani samo vsebino besedila certifikata, kot je določeno v oddelku 9.3.2.

CSM_160 VU preveri časovno veljavnost katerega koli certifikata, prebranega iz kartice ali shranjenega v pomnilniku, ter zavrne potekle certifikate. Za preverjanje časovne veljavnosti certifikata, ki ga predloži kartica, VU uporabi svojo interno uro.

▼B

Slika 4

Protokol za preverjanje verige certifikatov kartice s strani VU



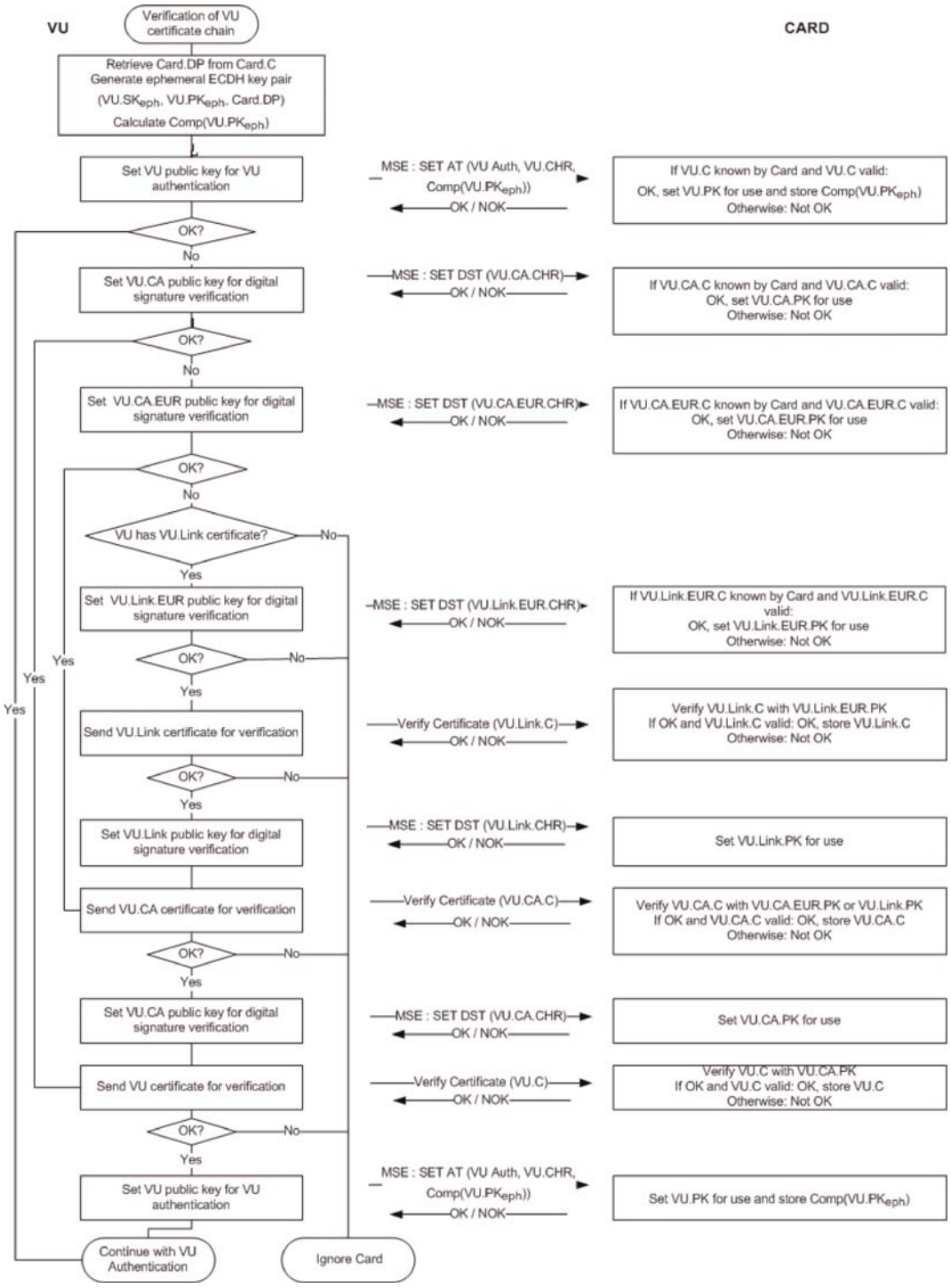
10.2.2 *Preverjanje verige certifikatov VU s strani kartice*

CSM_161 Tahografske kartice za preverjanje verige certifikatov VU uporabljajo protokol, prikazan na sliki 5.

▼B

Slika 5

Protokol za preverjanje verige certifikatov VU s strani kartice



Opombe k sliki 5:

— Certifikati in javni ključi VU iz slike so tisti za medsebojno avtentikacijo. V oddelku 9.1.4 so označeni kot VU_MA.

▼B

— Certifikati in javni ključi VU.CA iz slike so tisti za podpis certifikatov VU in zunanje GNSS opreme. V oddelku 9.1.3 so označeni kot MSCA_VU-EGF.

— Certifikat VU.CA.EUR iz slike je evropski korenski certifikat, ki je naveden v CAR certifikata VU.CA.

— Certifikat VU.Link iz slike je vezni certifikat VU, če obstaja. Kot je določeno v oddelku 9.1.2, je to vezni certifikat za nov evropski korenski par ključev, ki ga ustvari ERCA in se podpiše s prejšnjim evropskim zasebnim ključem.

— Certifikat VU.Link.EUR je evropski korenski certifikat, ki je naveden v CAR certifikata VU.Link.

CSM_162 Kot je prikazano na sliki 5, se preverjanje verige certifikatov enote v vozilu začne tako, da enota v vozilu poskuša nastaviti svoj javni ključ za uporabo v tahografski kartici. Če ji uspe, to pomeni, da je kartica v preteklosti uspešno preverila verigo certifikatov VU in shranila certifikat VU za prihodnjo uporabo. V tem primeru je certifikat VU pripravljen za uporabo in postopek se nadaljuje z avtentikacijo VU. Če kartica certifikata VU ne pozna, VU zaporedoma predloži certifikat VU.CA, ki se uporablja za preverjanje certifikata VU, certifikat VU.CA.EUR, ki se uporablja za preverjanje certifikata VU.CA, in po potrebi vezni certifikat, da najde certifikat, ki ga kartica pozna ali lahko preveri. Če kartica najde tak certifikat, ga uporabi za preverjanje osnovnih certifikatov VU, ki so ji bili predloženi. Če je uspešna, VU nastavi svoj javni ključ za uporabo v tahografski kartici. Če ni, VU kartico ignorira.

Opomba: Kartica lahko prepozna certifikat VU.CA.EUR na tri načine:

— certifikat VU.CA.EUR je enak certifikatu EUR kartice;

— certifikat VU.CA.EUR je predhodnik certifikata EUR kartice in kartica je ta certifikat vsebovala že ob izdaji (glej CSM_91);

— certifikat VU.CA.EUR je naslednik certifikata EUR kartice in kartica je v preteklosti prejela vezni certifikat iz druge enote v vozilu, ga preverila in shranila za prihodnjo uporabo.

CSM_163 VU uporabi ukaz MSE: Set AT, da nastavi svoj javni ključ za uporabo v tahografski kartici. Kot je določeno v Dodatku 2, ta ukaz vsebuje navedbo kriptografskega mehanizma, ki se bo uporabil z nastavljenim ključem. Gre za avtentikacijo VU z uporabo algoritma ECDSA v kombinaciji z zgoščevalnim algoritmom, ki ustreza velikosti ključa para ključev VU VU_MA, kot je določeno v CSM_50'.

▼B

CSM_164 Ukaz MSE: Set AT vsebuje tudi navedbo kratkotrajnega para ključev, ki ga VU uporabi med usklajevanjem ključa seje (glej oddelek 10.4). Zato VU, preden pošlje ukaz MSE: Set AT, ustvari kratkotrajni par ključev ECC. VU kratkotrajni par ključev ustvari z uporabo standardiziranih parametrov domene, navedenih v certifikatu kartice. Kratkotrajni par ključev je označen kot ($VU.SK_{eph}$, $VU.PK_{eph}$, Card.DP). VU za identifikacijo ključa izbere koordinato x kratkotrajne javne točke ECDH; to se imenuje zgoščena predstavitev javnega ključa, ki je v obliki $Comp(VU.PK_{eph})$.

CSM_165 Če je ukaz MSE: Set AT neuspešen, kartica navedeni VU.PK nastavi za poznejšo uporabo med avtentikacijo v vozilu in začasno shrani $Comp(VU.PK_{eph})$. Če sta pred uskladitvijo ključa seje poslana dva ali več ukazov MSA: Set AT, kartica shrani samo zadnji prejeti $Comp(VU.PK_{eph})$.

CSM_166 Kartica preveri časovno veljavnost katerega koli certifikata, ki ga VU predloži ali uporabi kot referenco in je shranjen v pomnilniku kartice, ter zavrne potekle certifikate.

CSM_167 Za preverjanje časovne veljavnosti certifikata, ki ga predloži VU, vsaka tahografska kartica interno shrani nekatere podatke, ki predstavljajo trenutni čas. Teh podatkov VU ne more neposredno posodabljati. Ob izdaji se trenutni čas kartice nastavi na datum začetka veljavnosti certifikata kartice Card_MA. Kartica posodobi trenutni čas, če je datum začetka veljavnosti avtentičnega certifikata, ki ga predloži VU in ki predstavlja veljaven časovni vir, novejši od trenutnega časa kartice. V tem primeru kartica trenutni čas nastavi na datum začetka veljavnosti navedenega certifikata. Kartica kot veljaven časovni vir sprejme samo naslednje certifikate:

— vezne certifikate ERCA druge generacije,

— vezne certifikate MSCA druge generacije,

— certifikate VU druge generacije, ki jih izda ista država kot certifikate kartice.

Opomba: Zadnja zahteva pomeni, da mora biti kartica zmožna prepoznati CAR certifikata VU, tj. certifikat MSCA_VU-EGF. Ta ne bo enak kot CAR lastnega certifikata, ki je certifikat MSCA_Card.

CSM_168 Kot je navedeno na sliki 5, lahko kartica, potem ko preveri avtentičnost in veljavnost prej nepoznanega certifikata, ta certifikat shrani za prihodnjo uporabo, tako da ji ni več

▼B

treba preverjati avtentičnosti navedenega certifikata, če ji je ponovno predložen. Namesto da shrani celoten certifikat lahko kartica shrani samo vsebino besedila certifikata, kot je določeno v oddelku 9.3.2.

10.3. **Avtentikacija VU**

CSM_169 Enote v vozilu in kartice za avtentikacijo VU glede na kartico uporabijo protokol avtentikacije VU, ki je prikazan na sliki 6. Avtentikacija VU tahografski kartici omogoči, da izrecno preveri avtentičnost VU. V ta namen VU uporabi zasebni ključ za podpis poziva, ki ga ustvari kartica.

CSM_170 Poleg poziva kartica VU v podpis vključi referenco imetnika kartice, ki jo pridobi iz certifikata kartice.

Opomba: To zagotavlja, da je kartica, glede na katero se VU avtenticira, enaka kartici, katere verigo certifikatov je VU predhodno preverila.

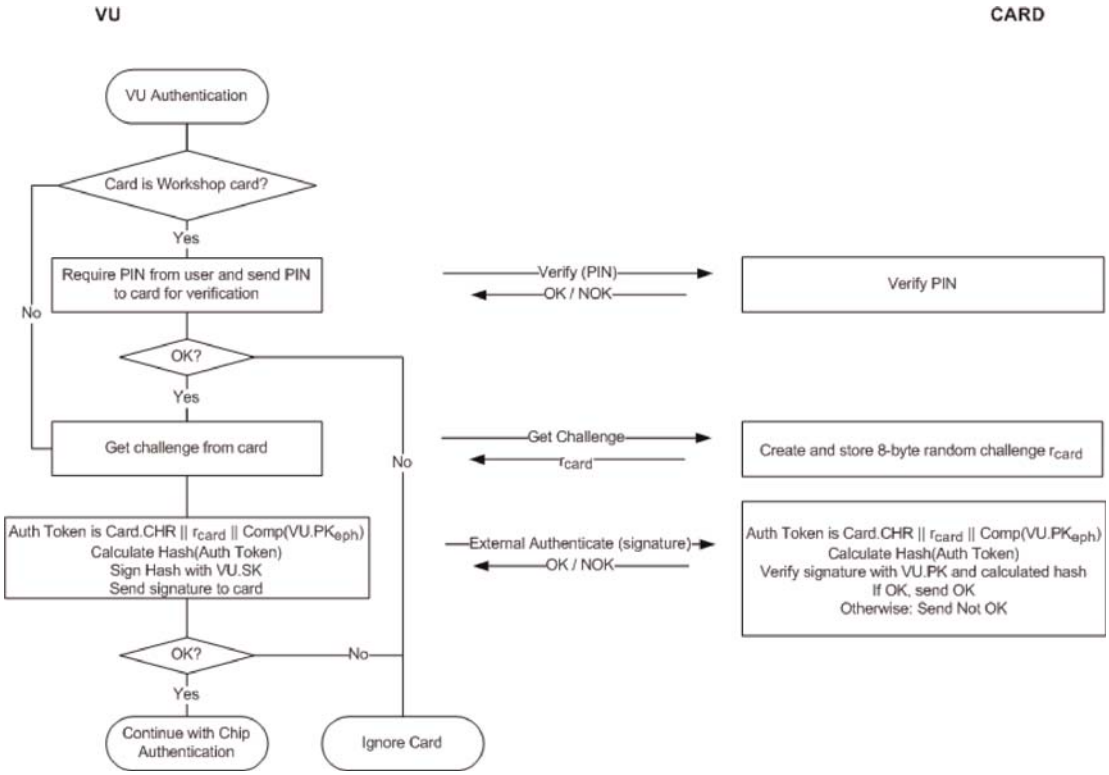
CSM_171 VU v podpis vključi tudi identifikator kratkotrajnega javnega ključa Comp($VU.PK_{eph}$), ki ga VU uporabi za vzpostavitev varnega sporočanja med postopkom avtentikacije čipa, ki je opisan v oddelku 10.4.

Opomba: To zagotavlja, da je VU, s katero kartica komunicira med sejo varnega sporočanja, enaka VU, ki jo je kartica avtenticirala.

▼B

Slika 6

Protokol avtentikacije VU



CSM_172 Če VU med avtentikacijo VU pošlje več ukazov GET CHALLENGE, kartica vsakokrat vrne nov 8-bitni naključni poziv, shrani pa samo zadnjega.

CSM_173 Algoritem podpisa, ki ga VU uporabi za avtentikacijo VU, mora biti ECDSA, kot je določeno v [DSS], uporablja pa se zgoščevalni algoritem, ki ustreza velikosti ključa para ključev VU VU_MA, kot je določeno v CSM_50. Format podpisa je neformatirano besedilo, kot je določeno v [TR-03111]. VU podpis pošlje kartici.

CSM_174 Po prejemu podpisa VU v ukazu EXTERNAL AUTHENTICATE kartica:

— izračuna avtentikacijski žeton tako, da poveže Card.CHR, poziv kartice r_{card} in identifikator kratkotrajnega javnega ključa VU Comp($VU.PK_{eph}$),

— izračuna zgoščeno vrednost glede na avtentikacijski žeton, in sicer z uporabo zgoščevalnega algoritma, povezanega z velikostjo ključa para ključev VU VU_MA, kot je določeno v CSM_50,

— preveri podpis VU z uporabo algoritma ECDSA v povezavi z VU.PK in izračunano zgoščeno vrednostjo.

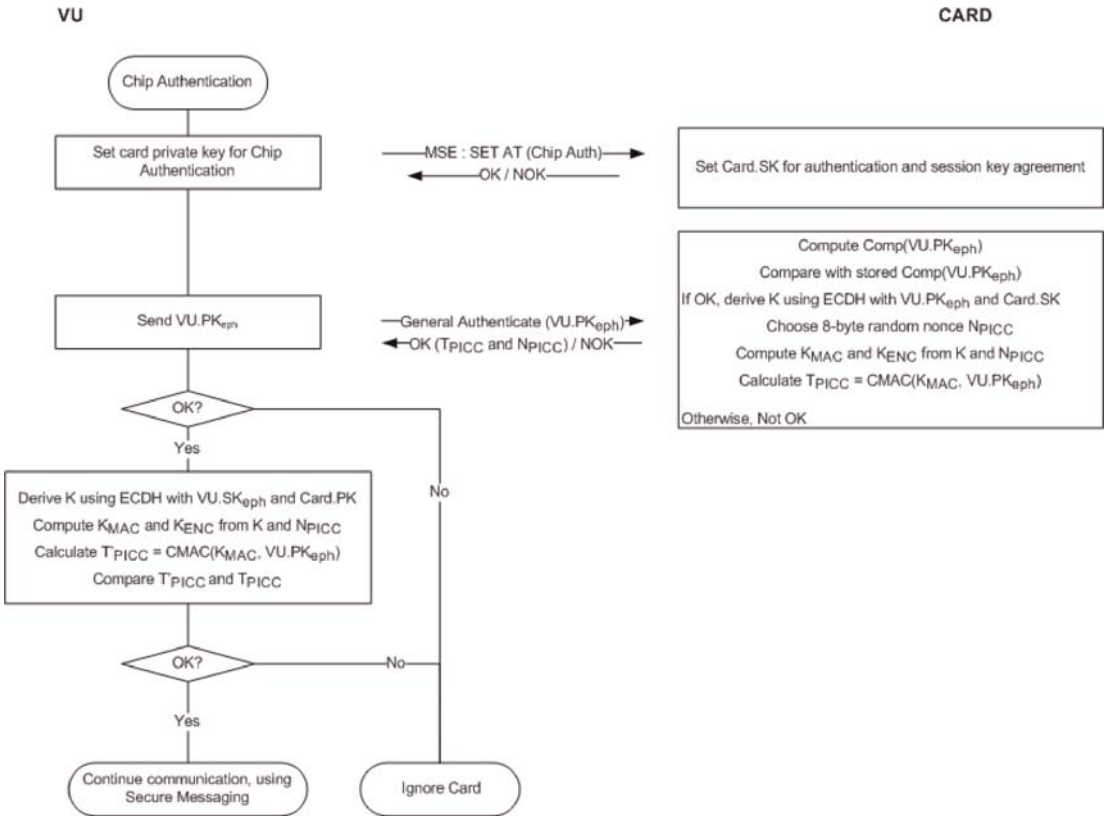
▼B

10.4. **Avtentikacija čipa in uskladitev ključa seje**

CSM_175 Enote v vozilu in kartice za avtentikacijo čipa glede na VU uporabijo protokol avtentikacije čipa, ki je prikazan na **sliki 7**. Avtentikacija čipa enoti v vozilu omogoči, da izrecno preveri avtentičnost kartice.

Slika 7

Avtentikacija čipa in uskladitev ključa seje



CSM_176 VU in kartica opravita naslednje:

1. Enota v vozilu sproži postopek avtentikacije čipa tako, da pošlje ukaz MSE: Set AT, ki označuje avtentikacijo čipa z uporabo algoritma ECDH; dolžina ključa seje AES ustreza velikosti ključa para ključev kartice Card_MA, kot je določeno v CSM_50. VU določi velikost ključa para ključev kartice iz certifikata kartice.

2. VU kartici pošlje javno točko $VU.PK_{eph}$ svojega kratkotrajnega para ključev. Kot je pojasnjeno v CSM_164, je VU ta kratkotrajni par ključev ustvarila pred preverjanjem verige certifikatov VU. VU je identifikator kratkotrajnega javnega ključa $Comp(VU.PK_{eph})$ poslala kartici, ta pa ga je shranila.

▼B

3. Kartica iz $VU.PK_{eph}$ izračuna $Comp(VU.PK_{eph})$ in ga primerja s shranjeno vrednostjo $Comp(VU.PK_{eph})$.

4. Z uporabo algoritma ECDH v kombinaciji s statičnim zasebnim ključem kartice in kratkotrajnim javnim ključem VU kartica izračuna zaupno vrednost K.

5. Kartica izbere naključni 8-bitni enkratnik N_{PICC} in ga uporabi za izpeljavo ključev seje K_{MAC} in K_{ENC} iz K. Glej CSM_179.

6. Z uporabo K_{MAC} kartica izračuna avtentikacijski žeton glede na identifikator kratkotrajnega javnega ključa VU: $T_{PICC} = CMAC(K_{MAC}, VU.PK_{eph})$. Kartica enoti v vozilu pošlje N_{PICC} in T_{PICC}.

7. Z uporabo algoritma ECDH v kombinaciji s statičnim javnim ključem kartice in kratkotrajnim zasebnim ključem VU izračuna enako zaupno vrednost K kot kartica v koraku 4.

8. VU iz K in N_{PICC} izpelje ključa seje K_{MAC} in K_{ENC}; glej CSM_179.

9. VU preveri avtentikacijski žeton T_{PICC}.

CSM_177 V koraku 3 zgoraj kartica izračuna Comp(VU.PKeph) kot koordinato x javne točke v VU.PKeph.

CSM_178 V korakih 4 in 7 zgoraj kartica in enota v vozilu uporabita algoritem ECKA-EG, kot je določeno v [TR-03111].

CSM_179 V korakih 5 in 8 zgoraj kartica in enota v vozilu uporabita funkcijo izpeljave ključa za ključa seje AES, določena v [TR-03111], z naslednjo stopnjo natančnosti in naslednjimi spremembami:

— Vrednost števca za K_{ENC} je ‘00 00 00 01’, za K_{MAC} pa ‘00 00 00 02’.

— Uporabi se neobvezni enkratnik *r*, ki je enak N_{PICC}.

— Za izpeljavo 128-bitnih ključev AES se uporabi zgoščevalni algoritem SHA-256.

— Za izpeljavo 192-bitnih ključev AES se uporabi zgoščevalni algoritem SHA-384.

— Za izpeljavo 256-bitnih ključev AES se uporabi zgoščevalni algoritem SHA-512.

Dolžina ključev sej (tj. dolžina, pri kateri se zgoščena vrednost odreže) ustreza velikosti para ključev Card_MA, kot je določeno v CSM_50.

▼B

CSM_180 V korakih 6 in 9 zgoraj kartica in enota v vozilu uporabita algoritem AES v načinu CMAC, kot je določeno v [SP 800-38B]. Dolžina T_{PICC} ustreza dolžini ključev seje AES, kot je določeno v CSM_50.

10.5. **Varno sporočanje**

10.5.1 *Splošno*

CSM_181 Vsi ukazi in odzivi, izmenjani med enoto v vozilu in tahografsko kartico po uspešni avtentikaciji čipa in do konca seje, so zavarovani z varnim sporočanjem.

CSM_182 Razen pri branju iz datoteke s pogojem dostopa SM-R-ENC-MAC-G2 (glej Dodatek 2, oddelek 4) se varno sporočanje uporablja v načinu „samo avtentikacija“. V tem načinu se kriptografska kontrolna vsota (MAC) doda vsem ukazom in odzivom, da se zagotovita avtentičnost in celovitost sporočila.

CSM_183 Pri branju iz datoteke s pogojem dostopa SM-R-ENC-MAC-G2 se varno sporočanje uporablja v načinu „najprej šifriranje, potem avtentikacija“, tj. podatki odziva se najprej šifrirajo, da se zagotovi zaupnost sporočila, potem pa se glede na šifrirane podatke izračuna MAC, da se zagotovi avtentičnost in celovitost.

CSM_184 Pri varnem sporočanju se AES, kot je določeno v [AES], uporablja s ključema seje K_{MAC} in K_{ENC}, ki sta bila usklajena med avtentikacijo čipa.

CSM_185 Za števec pošiljanj zaporedja (SCC) se uporablja nepodpisano celo število, da se prepreči napade s ponovitvijo. Velikost SSC je enaka velikosti bloka AES, tj. 128 bitov. SCC mora biti v formatu MSB-first. Ko se varno sporočanje začne, se števec pošiljanj zaporedja nastavi na nič (tj ‘00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00’). SSC se poveča vsakič, preden se ustvari ukaz ali odziv APDU: ker je začetna vrednost SSC v seji SM 0, bo v prvem ukazu vrednost SSC 1. Vrednost SSC za prvi odziv bo 2.

CSM_186 Za šifriranje sporočil se uporabi K_{ENC} z AES v načinu delovanja z veriženjem šifrirnih blokov (CBC), kot je določeno v [ISO 10116], pri čemer je parameter prepletanja m = 1, vektor inicializacije pa SV = $E(K_{ENC}, SSC)$, tj. trenutna vrednost števca pošiljanj zaporedja, šifrirana s K_{ENC}.

CSM_187 Za ugotavljanje avtentičnosti sporočila se uporabi K_{MAC} z AES v načinu CMAC, kot je določeno v [SP 800-38B]. Dolžina MAC ustreza dolžini ključev seje AES, kot je določeno v CSM_50. Števec pošiljanj zaporedja se vključi v MAC pred datagram, ki ga je treba avtenticirati.

▼B

10.5.2 *Struktura varnega sporočila*

CSM_188 Pri varnem sporočanju se uporabljajo samo podatkovni objekti varnega sporočanja (glej [ISO 7816-4]) iz Table 5. Ti podatkovni objekti se v vsakem sporočilu uporabljajo v vrstnem redu, določenem v tej preglednici.

Preglednica 5

Podatkovni objekti varnega sporočanja

Ime podatkovnega objekta	Oznaka	Obvezno (O), pogojno (P) ali nedovoljeno (N)	
		Ukazi	Odzivi
Nešifrirana vrednost, nekodirana v BER-TLV	‘81’	P	P
Nešifrirana vrednost, kodirana v BER-TLV, vendar brez SM DO	‘B3’	P	P
Indikator vsebine zapolnjevanja, ki mu sledi kriptogram, nešifrirana vrednost, nekodirana v BER-TLV	‘87’	P	P
Zaščiten Le	‘97’	P	N
Status obdelave	‘99’	N	O
Kriptografska kontrolna vsota	‘8E’	O	O

Opomba: Kot je določeno v Dodatku 2, lahko tahografske kartice podpirajo ukaza READ BINARY in UPDATE BINARY z lihim INS bajtom (‘B1’ oz. ‘D7’). Te različice ukazov se zahtevajo za branje in posodabljanje datotek z 32 768 bajti ali več. Če se uporabi taka različica, se namesto objekta z oznako ‘81’ uporabi podatkovni objekt z oznako ‘B3’. Za več informacij glej Dodatek 2.

CSM_189 Vsi podatkovni objekti SM so kodirani v DER TLV, kot je določeno v [ISO 8825-1]. Rezultat takega kodiranja je takšna struktura TLV (Tag-Length-Value; Oznaka-Dolžina-Vrednost):

Oznaka: Oznaka je kodirana v enem ali dveh oktetih in označuje vsebino.

Dolžina: Dolžina je kodirana kot nepodpisano celo število v enem, dveh ali treh oktetih, kar pomeni največjo dolžino 65 535 oktetov. Uporabi se najmanjše število oktetov.

Vrednost: Vrednost je kodirana v nič ali več oktetih.

CSM_190 APDU, zaščiteni z varnim sporočanjem, se ustvarijo tako:

— Glava ukaza se vključi v izračun MAC, zato se za bajt razreda CLA uporabi vrednost ‘0C’.

▼B

— Kot je določeno v Dodatku 2, morajo biti vsi bajti INS sodi, z možno izjemo lihih bajtov INS za ukaza READ BINARY in UPDATE BINARY.

— Dejanska vrednost Lc bo po varnem sporočanju spremenjena v Lc'.

— Podatkovno polje vsebuje podatkovne objekte SM.

— V zaščitenem ukazu APDU se novi bajt Le nastavi na ‘00’. Po potrebi se v podatkovno polje vključi podatkovni objekt ‘97’, da se navede prvotna vrednost Le.

CSM_191 Vsak podatkovni objekt, ki ga je treba šifrirati, se zapolni v skladu z [ISO 7816-4] z uporabo indikatorja vsebine zapolnjevanja ‘01’. Za izračun MAC se poleg tega vsak podatkovni objekt v APDU ločeno zapolni v skladu z [ISO 7816-4].

Opomba: Zapolnjevanje za varno sporočanje se vedno opravi s plastjo varnega sporočanja, ne pa z algoritmom CMAC ali CBC.

Povzetek in primeri

Ukaz APDU z uporabo varnega sporočanja bo imel naslednjo strukturo, odvisno od ustreznega nezavarovanega ukaza (DO je podatkovni objekt):

Primer 1:	CLA INS P1 P2 || Lc' || DO ‘8E’ || Le
Primer 2:	CLA INS P1 P2 || Lc' || DO ‘97’ || DO ‘8E’ || Le
Primer 3 (sodi INS bajt)	CLA INS P1 P2 || Lc' || DO ‘81’ || DO ‘8E’ || Le
Primer 3 (lihi INS bajt)	CLA INS P1 P2 || Lc' || DO ‘B3’ || DO ‘8E’ || Le
Primer 4 (sodi INS bajt)	CLA INS P1 P2 || Lc' || DO ‘81’ || DO ‘97’ || DO ‘8E’ || Le
Primer 4 (lihi INS bajt)	CLA INS P1 P2 || Lc' || DO ‘B3’ || DO ‘97’ || DO ‘8E’ || Le

pri čemer je Le = ‘00’ ali ‘00 00’, odvisno od tega, ali se uporabljajo kratka podatkovna polja ali podaljšana podatkovna polja; glej [ISO 7816-4].

Odziv APDU z uporabo varnega sporočanja bo imel naslednjo strukturo, odvisno od ustreznega nezavarovanega odziva:

Primer 1 ali 3:	DO ‘99’ || DO ‘8E’ || SW1SW2
Primer 2 ali 4 (sodi INS bajt) s šifriranjem:	DO ‘81’ || DO ‘99’ || DO ‘8E’ || SW1SW2
Primer 2 ali 4 (sodi INS bajt) brez šifriranja:	DO ‘87’ || DO ‘99’ || DO ‘8E’ || SW1SW2
Primer 2 ali 4 (lihi INS bajt) brez šifriranja:	DO ‘B3’ || DO ‘99’ || DO ‘8E’ || SW1SW2

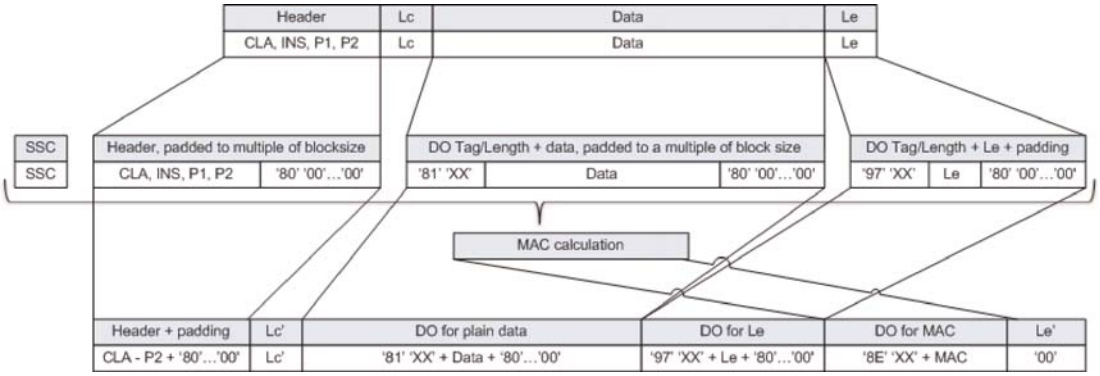
Opomba: Primer 2 ali 4 (lihi INS bajt) s šifriranjem se v komunikaciji med VU in kartico nikoli ne uporablja.

▼B

V nadaljevanju so navedeni trije primeri transformacij APDU za ukaze s sodo INS kodo. Slika 8 prikazuje avtenticiran ukaz APDU za primer 4, slika 9 avtenticiran odziv APDU za primer 2/primer4, slika 10 pa šifriran in avtenticiran odziv APDU za primer 2/primer 4.

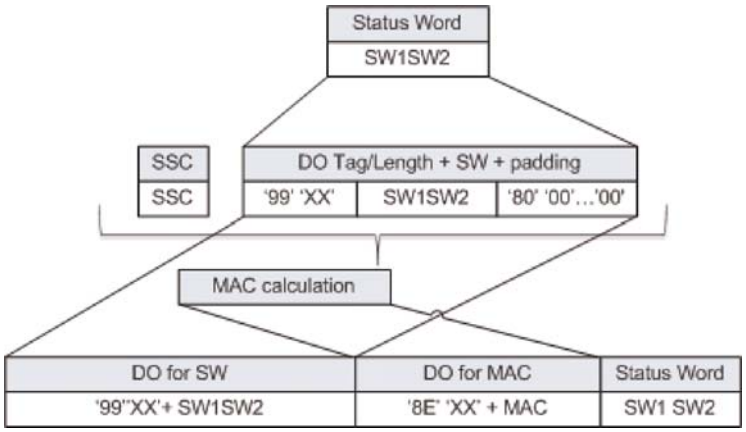
Slika 8

Transformacija avtenticiranega ukaza APDU za primer 4



Slika 9

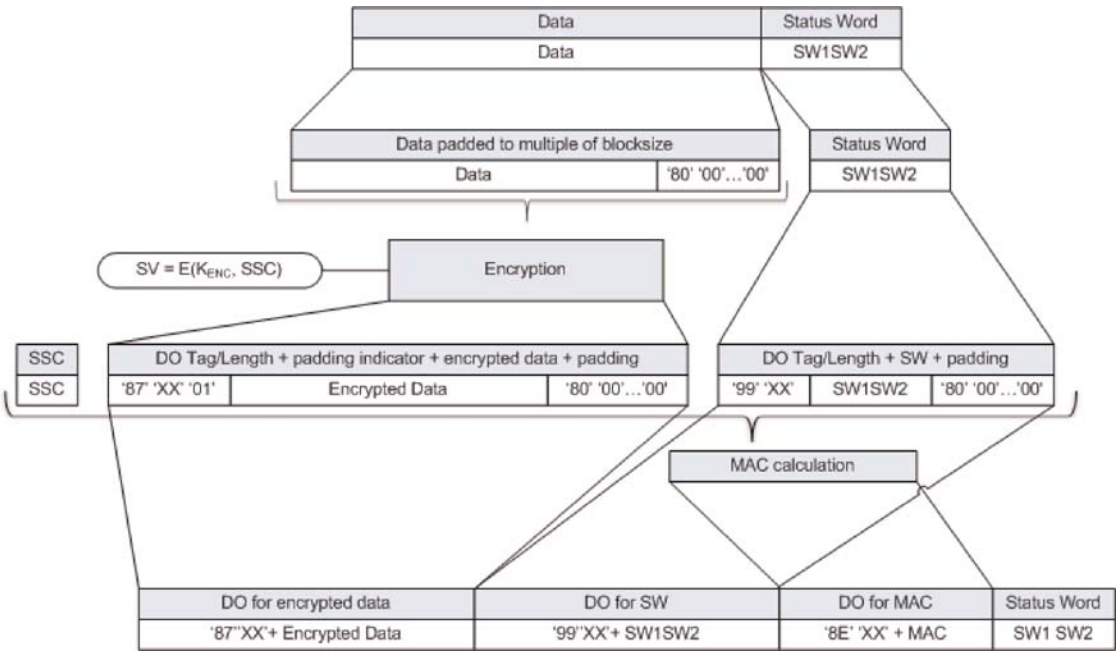
Transformacija avtenticiranega odziva APDU za primer 1/primer 3



▼B

Slika 10

Transformacija šifriranega in avtenticiranega odziva APDU za primer 2/primer 4



10.5.3 *Prekinitev seje varnega sporočanja*

CSM_192 Enota v vozilu prekine sejo varnega sporočanja samo v primeru, da se izpolni kateri od naslednjih pogojev:

— Enota v vozilu prejme odziv APDU v neformatiranem besedilu.

— Enota v vozilu v odzivu APDU zazna napako v varnem sporočanju:

  — ni pričakovanega podatkovnega objekta varnega sporočanja, vrstni red podatkovnih objektov je nepravilen, vključen je nepoznan podatkovni objekt;

  — podatkovni objekt varnega sporočanja je nepravilen, npr. nepravilna vrednost MAC, nepravilna struktura TLV, označevalni zapolnitveni bajt v oznaki ‘87’ ni enak ‘01’.

— Kartica pošlje statusni bajt, ki navaja, da je zaznala napako SM (glej CSM_194).

— Dosežena je mejna vrednost števila ukazov in povezanih odzivov v trenutni seji. Za posamezno VU to mejno vrednost določi proizvajalec ob upoštevanju varnostnih zahtev uporabljene strojne opreme, pri čemer je največja vrednost 240 ukazov in povezanih odzivov SM na sejo.

▼B

CSM_193 Tahografska kartica prekine sejo varnega sporočanja samo v primeru, da se zgodi kar koli od naslednjega:

— Tahografska kartica prejme ukaz APDU v neformatiranem besedilu.

— Tahografska kartica v ukazu APDU zazna napako v varnem sporočanju:

— ni pričakovanega podatkovnega objekta varnega sporočanja, vrstni red podatkovnih objektov je nepravilen, vključen je nepoznan podatkovni objekt;

— podatkovni objekt varnega sporočanja je nepravilen, npr. nepravilna vrednost MAC, nepravilna struktura TLV.

— Tahografska kartica ostane brez napajanja ali se ponastavi.

— VU izbere aplikacijo na kartici.

— VU začne postopek avtentikacije VU.

— Dosežena je mejna vrednost števila ukazov in povezanih odzivov v trenutni seji. Za posamezno kartico to mejno vrednost določi proizvajalec ob upoštevanju varnostnih zahtev uporabljene strojne opreme, pri čemer je največja vrednost 240 ukazov in povezanih odzivov SM na sejo.

CSM_194 Obravnava napake SM s strani tahografske kartice:

— Če v ukazu APDU ni nekaterih pričakovanih podatkovnih objektov varnega sporočanja, če je vrstni red podatkovnih objektov nepravilen ali če so vključeni nepoznani podatkovni objekti, se tahografska kartica odzove s statusnimi bajti ‘69 87’.

— Če je podatkovni objekt varnega sporočanja v ukazu APDU nepravilen, se tahografska kartica odzove s statusnimi bajti ‘69 88’.

V takem primeru se statusni bajti vrnejo brez uporabe SM.

CSM_195 Če se seja varnega sporočanja med VU in tahografsko kartico prekine, VU in tahografska kartica:

— varno uničita shranjeni ključ seje,

— nemudoma vzpostavita novo sejo varnega sporočanja, kot je opisano v oddelkih 10.2–10.5.

CSM_196 Če se VU iz kakršnega koli razloga odloči za ponovni začetek medsebojne avtentikacije glede na vstavljeno kartico, se postopek ponovno začne s pregledom verige certifikatov kartice, kot je opisano v oddelku 10.2, in se nadaljuje, kot je opisano v oddelkih 10.2–10.5.

▼B

11. POVEZAVA MED VU IN ZUNANJO GNSS OPREMO, MEDSEBOJNA AVTENTIKACIJA IN VARNO SPOROČANJE

11.1. **Splošno**

CSM_197 GNSS oprema, ki jo VU uporablja za določitev svojega položaja, je lahko vgrajena v ohišje enote v vozilu brez možnosti odstranitve ali pa je v obliki zunanjega modula. V prvem primeru ni potrebno standardizirati interne komunikacije med GNSS opremo in VU, zahteve iz tega poglavja se ne uporabljajo. V drugem primeru je treba komunikacijo med VU in zunanjo GNSS opremo standardizirani in zavarovati, kot je opisano v tem poglavju.

CSM_198 Varna komunikacija med enoto v vozilu in zunanjo GNSS opremo poteka na enak način kot varna komunikacija med enoto v vozilu in tahografsko kartico, pri čemer zunanja GNSS oprema (EGF) prevzame vlogo kartice. EGF mora izpolniti vse zahteve za tahografske kartice iz poglavja 10, pri čemer se upoštevajo odstopanja, pojasnitve in dodatki iz tega poglavja. Zlasti se opravijo medsebojno preverjanje verige certifikatov, avtentikacija VU in avtentikacija čipa, kot je opisano v oddelkih 11.3 in 11.4.

CSM_199 Komunikacija med enoto v vozilu in EGF se od komunikacije med enoto v vozilu in kartico razlikuje po tem, da je treba enoto v vozilu in EGF enkrat povezati v servisni delavnici, preden si lahko VU in EGF med običajnim delovanjem izmenjata podatke na podlagi GNSS. Postopek povezovanja je opisan v oddelku 11.2.

CSM_200 Za komunikacijo med enoto v vozilu in EGF se uporabijo ukazi in odzivi na podlagi [ISO 7816-4] in [ISO 7816-8]. Natančna struktura teh APDU je opredeljena v Dodatku 2 k tej prilogi.

11.2. **Povezava med VU in zunanjo GNSS opremo**

CSM_201 Enoto v vozilu in EFG v vozilu poveže servisna delavnica. Med običajnim delovanjem lahko komunicirata samo povezani enota v vozilu in EGF.

CSM_202 Povezava enote v vozilu in EGF je mogoča samo, če je enota v vozilu v kalibracijskem načinu. Povezavo začne enota v vozilu.

CSM_203 Delavnica lahko enoto v vozilu kadar koli ponovno poveže na drugo EGF ali isto EGF. Med ponovnim povezovanjem VU na varen način uniči obstoječi certifikat EGF_MA zunanje GNSS opreme, s katero se povezuje.

CSM_204 Delavnica lahko zunanjo GNSS opremo kadar koli ponovno poveže na drugo VU ali isto VU. Med ponovnim povezovanjem mora EGF na varen način uničiti obstoječi certifikat VU_MA enote v vozilu, s katero se povezuje.

▼B

11.3. **Medsebojno preverjanje verige certifikatov**

11.3.1 *Splošno*

CSM_205 Medsebojno preverjanje verige certifikatov med VU in EGF se opravi samo med povezovanjem VU in EGF v servisni delavnici. Med običajnim delovanje povezanih VU in EGF se certifikati ne preverjajo. Namesto tega VU in EGF zaupata certifikatom, ki sta jih shranila med povezovanjem, še prej pa preverita njihovo časovno veljavnost. VU in EGF za zavarovanje komunikacije med njima med običajno uporabo ne zaupata nobenim drugim certifikatom.

11.3.2 *Med povezovanjem VU in EGF*

CSM_206 Med povezovanjem z EGF VU uporabi protokol, prikazan na sliki 4 (oddelek 10.2.1), da preveri verigo certifikatov zunanje GNSS opreme.

Opombe k sliki 4:

— Nadzor komunikacije ne spada na področje uporabe tega dodatka. Vendar EGF ni pametna kartica, zato VU verjetno za začetek komunikacije ne bo poslala ponastavitve in ne bo prejela ATR.

— Certifikati in javni ključi kartice iz slike se razumejo kot certifikati in javni ključi EGF za medsebojno avtentikacijo. V oddelku 9.1.6 so označeni kot EGF_MA.

— Certifikati in javni ključi Card.CA, prikazani na sliki, se razumejo kot certifikati in javni ključi MSCA za podpis certifikatov EGF. V oddelku 9.1.3 so označeni kot MSCA_VU-EGF.

— Certifikat Card.CA.EUR iz slike se razume kot evropski korenski certifikat, ki je naveden v CAR certifikata MSCA_VU-EGF.

— Certifikat Card.Link iz slike se razume kot vezni certifikat EGF, če obstaja. Kot je določeno v oddelku 9.1.2, je to vezni certifikat za nov evropski korenski par ključev, ki ga ustvari ERCA in se podpiše s prejšnjim evropskim zasebnim ključem.

— Certifikat Card.Link.EUR je evropski korenski certifikat, ki je naveden v CAR certifikata Card.Link.

— VU namesto `cardExtendedSerialNumber`iz EF ICC prebere `sensorGNSSserialNumber`.

— VU ne izbere tahografa AID, ampak EGF AID.

— „Ignorira kartico“ se razume kot „ignorira EGF“.

▼B

CSM_207 Ko enota v vozilu preveri certifikat EGF_MA, ga shrani za uporabo med običajnim delovanjem; glej oddelek 11.3.3.

CSM_208 Med povezovanjem z VU zunanja GNSS enota uporabi protokol, prikazan na sliki 5 (oddelek 10.2.2), da preveri verigo certifikatov VU.

Opombe k sliki 5:

— VU z uporabo parametrov domene v certifikatu EGF ustvari nov kratkotrajni par ključev.

— Certifikati in javni ključi VU iz slike so tisti za medsebojno avtentikacijo. V oddelku 9.1.4 so označeni kot VU_MA.

— Certifikati in javni ključi VU.CA iz slike so tisti za podpis certifikatov VU in zunanje GNSS opreme. V oddelku 9.1.3 so označeni kot MSCA_VU-EGF.

— Certifikat VU.CA.EUR iz slike je evropski korenski certifikat, ki je naveden v CAR certifikata VU.CA.

— Certifikat VU.Link iz slike je vezni certifikat VU, če obstaja. Kot je določeno v oddelku 9.1.2, je to vezni certifikat za nov evropski korenski par ključev, ki ga ustvari ERCA in se podpiše s prejšnjim evropskim zasebnim ključem.

— Certifikat VU.Link.EUR je evropski korenski certifikat, ki je naveden v CAR certifikata VU.Link.

CSM_209 Z odstopanjem od zahteve CSM_167 EGF za preverjanje časovne veljavnosti katerega koli predloženega certifikata uporabi čas GNSS.

CSM_210 Ko zunanja GNSS enota preveri certifikat VU_MA, ga shrani za uporabo med običajnim delovanjem; glej oddelek 11.3.3.

11.3.3 *Med običajnim delovanjem*

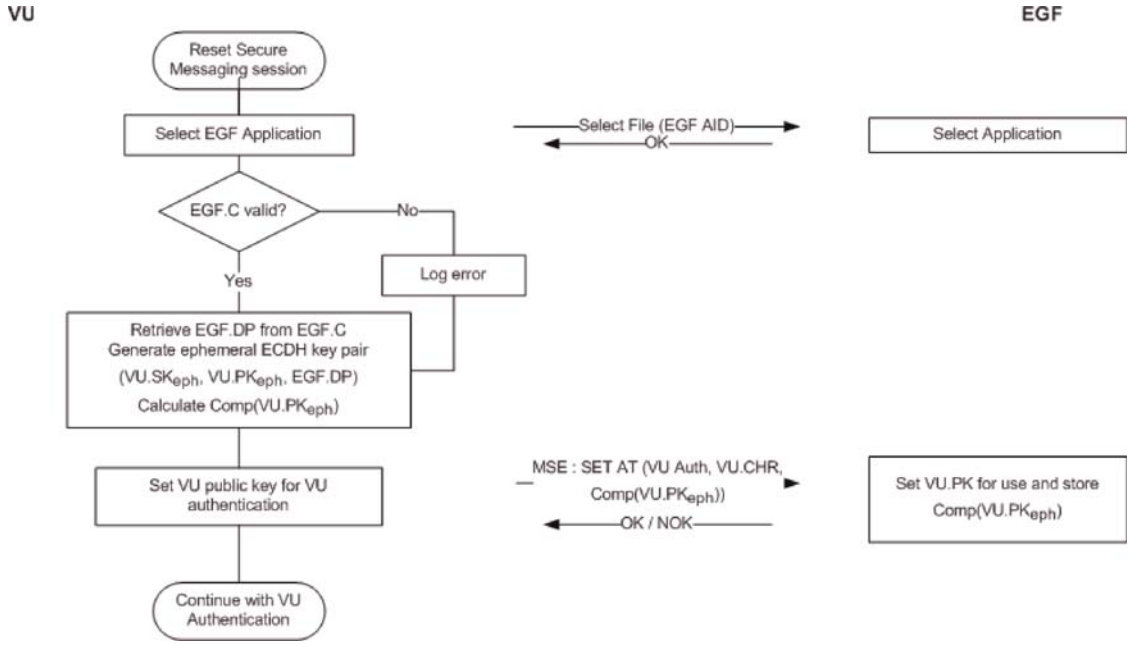
CSM_211 Med običajnim delovanjem enota v vozilu in EGF za preverjanje časovne veljavnosti shranjenih certifikatov EGF_MA in VU_MA ter za nastavitev javnega ključa VU_MA za kasnejšo avtentikacijo VU uporabljata protokol s slike 11. Med običajnim delovanjem se ne opravi nobeno dodatno medsebojno preverjanje.

Opomba: na sliki 11 so v osnovi predstavljeni prvi koraki, opisani v sliki 4 in sliki 5. Vendar EGF ni pametna kartica, zato VU verjetno za začetek komunikacije ne bo poslala ponastavitve in ne bo prejela ATR. Poleg tega to ne spada na področje uporabe tega dodatka.

▼B

Slika 11

Medsebojno preverjanje časovne veljavnosti certifikata med običajnim delovanjem VU–EGF



CSM_212 Kot je prikazano na sliki 11, enota v vozilu javi napako, če certifikat EGF_MA ni več veljaven. Medsebojna avtentikacija, uskladitev ključa in poznejša komunikacija prek varnega sporočanja pa se nadaljujejo kot običajno.

11.4. **Avtentikacija VU, avtentikacija čipa in uskladitev ključa seje**

CSM_213 Avtentikacija VU, avtentikacija čipa in uskladitev ključa seje med VU in EGF poteka med povezovanjem in kadar koli se seja varnega sporočanja ponovno vzpostavi med običajnim delovanjem. VU in ESPG izvedeta postopke iz oddelkov 10.3 in 10.4. Uporabljajo se vse zahteve iz teh oddelkov.

11.5. **Varno sporočanje**

CSM_214 Vsi ukazi in odzivi, izmenjani med enoto v vozilu in zunanjo GNSS opremo po uspešni avtentikaciji čipa in do konca seje, so zavarovani z varnim sporočanjem (v načinu „samo avtentikacija“). Uporabljajo se vse zahteve iz oddelka 10.5.

CSM_215 Če se seja varnega sporočanja med VU in EGF prekine, VU nemudoma vzpostavi novo sejo varnega sporočanja, kot je opisano v oddelkih 11.3.3 in 11.4.

12. POVEZAVA IN KOMUNIKACIJA MED VU IN TIPALOM GIBANJA

12.1. **Splošno**

CSM_216 Enota v vozilu in tipalo gibanja med povezovanjem in običajnim delovanjem komunicirata z uporabo vmesniškega protokola iz [ISO 16844-3] s spremembami, opisanimi v tem poglavju in oddelku 9.2.1.

▼B

Opomba: Bralci tega poglavja naj bi bili seznanjeni z vsebino [ISO 16844-3].

12.2. **Povezava med VU in tipalom gibanja z uporabo različnih generacij ključev**

Kot je pojasnjeno v oddelku 9.2.1, se glavni ključ tipala gibanja in vsi povezani ključi redno menjajo. To pomeni, da so v karticah servisne delavnice prisotni do trije ključi AES K_{M-WC} (zaporednih generacij ključev), povezani s tipalom. Podobno so lahko v tipalih gibanja prisotna do tri različna šifriranja podatkov na podlagi AES (na podlagi zaporednih generacij glavnega ključa tipala gibanja K_M). Enota v vozilu vsebuje samo en ključ K_{M-VU}, povezan s tipalom gibanja.

CSM_217 VU druge generacije in tipalo gibanja druge generacije se povežeta, kot je opisano v nadaljevanju (primerjaj s preglednico 6 v [ISO 16844-3]):

1. Kartica servisne delavnice druge generacije se vstavi v VU, ta pa se poveže s tipalom gibanja.

2. VU iz kartice servisne delavnice prebere vse razpoložljive ključe K_{M-WC}, pregleda njihove številke različice in izbere tistega, ki se ujema s številko različice ključa VU K_{M-VU}. Če ujemajočega ključa K_{M-WC} ni v kartici servisne delavnice, VU prekine proces povezovanja in imetniku kartice servisne delavnice prikaže ustrezno poročilo o napaki.

3. VU iz K_{M-VU} in K_{M-WC} izračuna glavni ključ tipala gibanja K_M ter identifikacijski ključ K_{ID} iz K_M, kot je določeno v oddelku 9.2.1.

4. VU tipalu gibanja pošlje navodilo za začetek procesa povezovanja, kot je opisano v [ISO 16844-3], in z identifikacijskim ključem K_{ID} šifrira serijske številke, ki jih prejme od tipala gibanja. VU tipalu gibanja nazaj pošlje šifrirano serijsko številko.

5. Tipalo gibanja šifrirano serijsko številko zaporedoma poveže z vsakim internim šifriranjem serijske številke. Če najde ujemajočo serijsko številko, se VU avtenticira. Tipalo gibanja prepozna generacijo K_{ID}, ki jo uporablja VU, in vrne ujemajočo šifrirano različico povezovalnega ključa, tj. šifriranje, ki je bilo ustvarjeno z isto generacijo K_M.

6. VU dešifrira povezovalni ključ z uporabo K_M, ustvari ključ seje K_S, ga šifrira s povezovalnim ključem in rezultat pošlje tipalu gibanja. Tipalo gibanja dešifrira K_S.

7. VU zbere informacije o povezavi, kot je določeno v [ISO 16844-3], jih šifrira s povezovalnim ključem in rezultat pošlje tipalu gibanja. Tipalo gibanja dešifrira informacije o povezavi.

8. Tipalo gibanja šifrira prejete informacije o povezavi s prejetim K_S in jih vrne VU. VU preveri, da so informacije o povezavi iste kot tiste, ki jih je VU poslala tipalu

▼B

gibanja v prejšnjem koraku. Če so, je to dokaz, da je tipalo gibanja uporabilo isti K_S kot VU in v koraku 5 poslalo svoj povezovalni ključ, šifriran s pravilno generacijo K_M. Tipalo gibanja se tako avtenticira.

Opomba: koraka 2 in 5 se razlikujeta od standardnega postopka iz [ISO 16844-3], drugi koraki pa so standardni.

Primer: če se povezovanje opravi v prvem letu veljavnosti certifikata ERCA (3), glej sliko 2 v oddelku 9.2.1.2, in

— je bilo tipalo gibanja izdano v zadnjem letu veljavnosti certifikata ERCA (1), bo tipalo gibanja vsebovalo naslednje ključe in podatke:

  — $N_s[1]$: s serijsko številko, šifrirano s K_{ID} prve generacije,

  — $N_s[2]$: s serijsko številko, šifrirano s K_{ID} druge generacije,

  — $N_s[3]$: s serijsko številko, šifrirano s K_{ID} tretje generacije,

  — $K_P[1]$: s povezovalnim ključem prve generacije [1], šifriranim s K_M prve generacije,

  — $K_P[2]$: s povezovalnim ključem druge generacije, šifriranim s K_M druge generacije,

  — $K_P[3]$: s povezovalnim ključem tretje generacije, šifriranim s K_M tretje generacije.

— Če je bila kartica servisne delavnice izdana v prvem letu veljavnosti certifikata ERCA (3), bo vsebovala ključ $K_{M\text{-}WC}$ druge in tretje generacije.

— Če je VU VU druge generacije, ki vsebuje $K_{M\text{-}VU}$ druge generacije,

se bo v korakih 2–5 zgodilo naslednje:

— Korak 2: VU prebere $K_{M\text{-}WC}$ druge in tretje generacije iz kartice servisne delavnice in preveri njuni številki različice.

— Korak 3: VU poveže $K_{M\text{-}WC}$ druge generacije s svojim $K_{M\text{-}VU}$ in izračuna K_M in K_{ID}.

— Korak 4: VU serijsko številko, ki jo prejme od tipala gibanja, šifrira s K_{ID}.

— Korak 5: tipalo gibanja primerja prejete podatke z $N_s[1]$ in ne najde ujemanja. Nato podatke primerja z $N_s[2]$ in najde ujemanje. Sklene, da je VU VU druge generacije, zato $K_P[2]$ pošlje nazaj.

[1] Treba je upoštevati, da so povezovalni ključi prve, druge in tretje generacije dejansko isti ključ ali pa trije različni ključi z različno dolžino, kot je pojasnjeno v CSM_117.

▼B

12.3. **Povezava in komunikacija med VU in tipalom gibanja z uporabo AES**

CSM_218 Kot je določeno v Table 3 v oddelku 9.2.1, so vsi ključi, vključeni v povezovanje enote v vozilu (druge generacije) in tipala gibanja ter v kasnejšo komunikacijo, ključi AES, ne pa ključi TDES podvojene dolžine, kot je določeno v [ISO 16844-3]. Ti ključi AES imajo lahko dolžino 128, 192 ali 256 bitov. Ker je velikost blokov AES 16 bajtov, mora biti dolžina šifriranega sporočila večkratnik 16 bajtov (za TDES 8 bajtov). Poleg tega bodo nekatera od teh sporočil uporabljena za prenos ključev AES, katerih dolžina je lahko 128, 192 ali 256 bitov. Zato se število podatkovnih bajtov na posamezno navodilo iz preglednice 5 [ISO 16844-3] spremeni, kot je prikazano v Preglednici 6.

Preglednica 6

Število podatkovnih bajtov (v neformatiranem besedilu in šifriranih) na posamezno navodilo v skladu z [ISO 16844-3]

Navodilo	Zahtevek/odziv	Opis podatkov	Št. podatkovnih bajtov v neformatiranem besedilu v skladu z [ISO 16844-3]	Št. podatkovnih bajtov v neformatiranem besedilu pri uporabi ključev AES	Št. šifriranih podatkovnih bajtov pri uporabi ključev AES dolžine		
					128	192	256
10	zahtevek	podatki za avtentikacijo + številka datoteke	8	8	16	16	16
11	odziv	podatki za avtentikacijo + vsebina datoteke	16 ali 32, odvisno od datoteke	16 ali 32, odvisno od datoteke	16/32	16/32	16/32
41	zahtevek	serijska številka tipala gibanja	8	8	16	16	16
41	odziv	povezovalni ključ	16	16/24/32	16	32	32
42	zahtevek	ključ seje	16	16/24/32	16	32	32
43	zahtevek	informacije o povezavi	24	24	32	32	32
50	odziv	informacije o povezavi	24	24	32	32	32
70	zahtevek	podatki za avtentikacijo	8	8	16	16	16
80	odziv	vrednost števca tipala gibanja + podatki za avtentikacijo	8	8	16	16	16

CSM_219 Informacije o povezavi, poslane v navodilu 43 (zahtevek VU) in 50 (odziv tipala gibanja) se zberejo, kot je določeno v oddelku 7.6.10 [ISO 16844-3], vendar se namesto algoritma TDES v šifrirni shemi podatkov o povezavi uporabi algoritem AES; tako nastaneta dve šifriranji AES in se uporabi način zapolnjevanja, določen v CSM_220, ki ustreza velikosti bloka AES. Ključ K'_p, ki se uporabi za šifriranje, se ustvari tako:

— če je dolžina povezovalnega ključa K_P 16 bajtov: $K'_p = K_P \text{ XOR } (N_s||N_s)$,

▼B

— če je dolžina povezovalnega ključa K_P 24 bajtov: $K'_P = K_P$ XOR $(N_s||N_s||N_s)$.

— če je dolžina povezovalnega ključa K_P 32 bajtov: $K'_P = K_P$ XOR $(N_s||N_s||N_s||N_s)$,

pri čemer je N_S 8-bitna serijska številka tipala gibanja.

CSM_220 Če dolžina podatkov v neformatiranem besedilu (z uporabo ključa AES) ni večkratnik 16 bajtov, se uporabi način zapolnjevanja 2 iz [ISO 9797-1].

Opomba: v [ISO 16844-3] je število podatkovnih bajtov v neformatiranem besedilu vedno večkratnik 8, tako da zapolnjevanje pri uporabi TDES ni potrebno. Opredelitev podatkov in sporočil v [ISO 16844-3] se s tem delom tega dodatka ne spremeni, zato je potrebno zapolnjevanje.

CSM_221 Za navodilo 11 in če je treba šifrirati več kot en blok podatkov, se uporabi način delovanja z veriženjem šifrirnih blokov, kot je opisano v [ISO 10116], pri čemer je parameter prepletanja *m* = 1. IV, ki ga je treba uporabiti, je:

— za navodilo 11: 8-bajtni blok za avtentikacijo, določen v oddelku 7.6.3.3 [ISO 16844-3], zapolnjen z uporabo načina zapolnjevanja 2 iz [ISO 9797-1]; glej tudi oddelka 7.6.5 in I7.6.6 [ISO 16844-3];

— za vsa druga navodila, pri katerih se prenese več kot 16 bajtov, kot je določeno v Table 6: ‘00’ {16}, tj. šestnajst bajtov z binarno vrednostjo 0.

Opomba: Kot je prikazano v oddelkih 7.6.5 in 7.6.6 [ISO 16844-3], se blok za avtentikacijo, ko tipalo gibanja šifrira podatkovne datoteke za vključitev v navodilo 11,

— uporabi kot vektor inicializacije za šifriranja v načinu CBC;

— šifrira in v podatke, ki se pošljejo VU, vključi kot prvi blok.

12.4. **Povezava med VU in tipalom gibanja za različne generacije opreme**

CSM_222 Kot je pojasnjeno v oddelku 9.2.1, tipalo gibanja druge generacije lahko vsebuje šifrirane podatke o povezovanju na podlagi TDES (kot je določeno v delu A tega dodatka), kar mu omogoča povezavo z VU prve generacije. V tem primeru se VU prve generacije in tipalo gibanja druge generacije povežeta, kot je opisano v delu A tega dodatka in v [ISO 16844-3]. Za postopek povezovanja se lahko uporabi kartica servisne delavnice prve ali druge generacije.

Opombi:

— Povezava VU druge generacije in tipala gibanja prve generacije ni mogoča.

▼B

— Kartice servisne delavnice prve generacije ni mogoče uporabiti za povezavo VU druge generacije s tipalom gibanja.

13. VARNOST KOMUNIKACIJE NA DALJAVO Z DSRC

13.1. **Splošno**

Kot je določeno v Dodatku 14, VU redno tvori podatke za nadzor tahografov na daljavo (RTM) in jih pošilja vgrajeni ali zunanji opremi za komunikacijo na daljavo (RCF). Oprema za komunikacijo na daljavo prek vmesnika DSRC te podatke pošlje daljinskemu poizvedovalniku, kot je opisano v Dodatku 14. Dodatek 1 navaja, da so podatki RTM združitev:

šifriranih koristnih podatkov tahografa šifriranje koristnih podatkov tahografa v neformatiranem besedilu;

zaščitnih podatkov DSRC opisano spodaj.

Format koristnih podatkov tahografa v neformatiranem besedilu je določen v Dodatku 1 in podrobneje opisan v Dodatku 14. V tem oddelku je opisana struktura zaščitnih podatkov DSRC; formalna specifikacija je v Dodatku 1.

CSM_223 Podatki `tachographPayload`v neformatiranem besedilu, ki jih VU pošlje opremi za komunikacijo na daljavo (če je RCF zunaj VU) ali ki se iz VU pošljejo v daljinski poizvedovalnik prek vmesnika DSRC (če je RCF vgrajena v VU) so zavarovani v načinu „najprej šifriranje, potem avtentikacija“, tj. koristni podatki tahografa se najprej šifrirajo, da se zagotovi zaupnost sporočila, nato pa se izračuna MAC, da se zagotovi avtentičnost in celovitost podatkov.

CSM_224 Zaščitni podatki DSRC so sestavljeni iz naslednjih podatkovnih elementov v navedenem vrstnem redu, glej tudi sliko 12:

Trenutni datum in čas	trenutni datum in čas VU (podatkovni tip `TimeReal`)
Števec	3-bitni števec, glej CSM_225
Serijska številka VU	serijska številka VU (podatkovni tip `VuSerialNumber`)
Številka različice glavnega ključa DSRC	1-bitna številka različice glavnega ključa DSRC, iz katerega so bili ustvarjeni posebni ključi DSRC VU, glej oddelek 9.2.2.
MAC	MAC, izračunana na podlagi vseh prejšnjih bajtov v podatkih RTM.

CSM_225 3-bajtni števec zaščitnih podatkov DSRC je v formatu MSB-first. Ko VU po tem, ko je dana v proizvodnjo, prvič izračuna niz podatkov RTM, vrednost števca nastavi na 0. VU vsakokrat, preden izračuna naslednji niz podatkov RTM, poveča vrednost podatkov števca za 1.

▼B

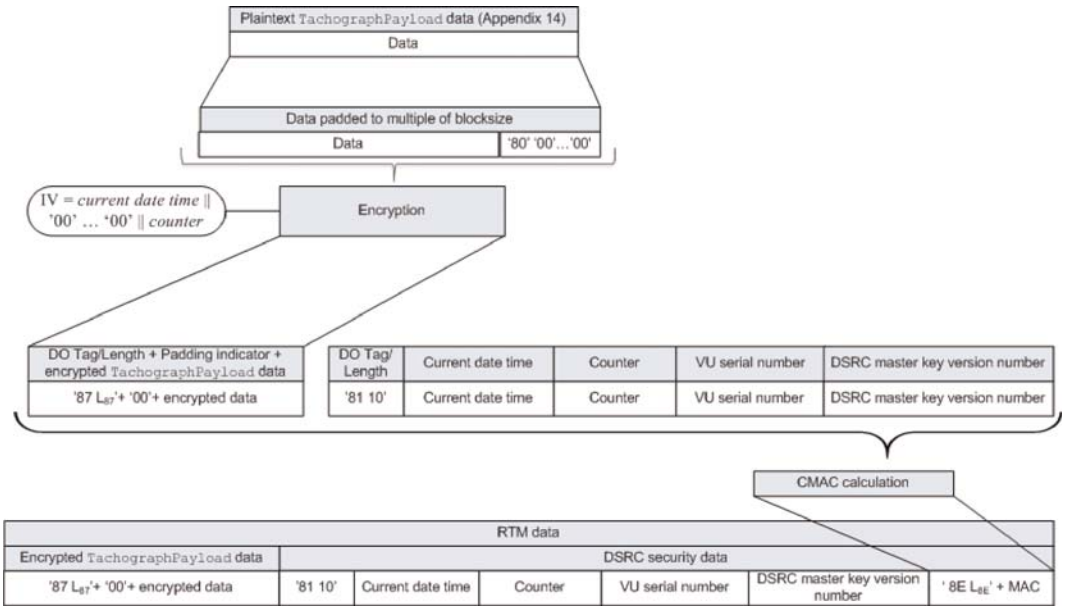
13.2. **Šifriranje koristnih podatkov tahografa in ustvarjanje MAC**

CSM_226 Na podlagi podatkovnega elementa v neformatiranem besedilu s podatkovnim tipom `TachographPayload`, kot je opisano v Dodatku 14, VU te podatke šifrira, kot je prikazano na sliki 12: ključ DSRC VU za šifriranje $K_VU_{DSRC}_ENC$ (glej oddelek 9.2.2) se uporabi z AES v načinu delovanja z veriženjem šifrirnih blokov (CBC), kot je določeno v [ISO 10116], pri čemer je parameter prepletanja *m* = 1. Vektor inicializacije je enak *IV = trenutni datum in čas || '00 00 00 00 00 00 00 00' || števec*, pri čemer so *trenutni datum in čas* ter *števec* opredeljeni v CSM_224. Podatki, ki se šifrirajo, se zapolnijo z načinom 2 iz [ISO 9797-1].

CSM_227 VU izračuna MAC v zaščitnih podatkih DSRC, kot je prikazano na sliki 12: MAC se izračuna na podlagi vseh predhodnih bajtov v podatkih RTM, do in vključno s številko različice glavnega ključa DSRC in vključno z oznakami in dolžinami podatkovnih objektov. VU uporabi svoj ključ DSRC za avtentičnost $K_VU_{DSRC}_MAC$ (glej oddelek 9.2.2) z algoritmom AES v načinu CMAC, kot je določeno v [SP 800-38B]. Dolžina MAC ustreza dolžini ključev DSRC, specifičnih za VU, kot je določeno v CSM_50.

Slika 12

Šifriranje koristnih podatkov tahografa in ustvarjanje MAC



13.3. **Preverjanje in dešifriranje koristnih podatkov tahografa**

CSM_228 Ko daljinski poizvedovalnik prejme podatke RTM od VU, celotne podatke RTM pošlje nadzorni kartici v podatkovnem polju ukaza PROCESS DSRC MESSAGE, kot je opisano v Dodatku 2. Nato:

▼B

1. nadzorna kartica preveri številko različice glavnega ključa DSRC v zaščitnih podatkih DSRC. Če nadzorna kartica ne pozna navedenega glavnega ključa DSRC, sporoči napako, kot je določeno v Dodatku 2, in prekine postopek.

2. Nadzorna kartica uporabi navedeni glavni ključ DSRC v kombinaciji s serijsko številko VU v zaščitnih podatkih DSRC, da ustvari posebna ključa DSRC K_VU_{DSRC}_ENC in K_VU_{DSRC}_MAC za VU, kot je navedeno v CSM_124.

3. Nadzorna kartica uporabi K_VU_{DSRC}_MAC za preverjanje MAC v zaščitnih podatkih DSRC, kot je določeno v CSM_227. Če je MAC nepravilen, nadzorna kartica sporoči napako iz Dodatka 2 in prekine postopek.

4. Nadzorna kartica uporabi K_VU_{DSRC}_ENC za dešifriranje šifriranih koristnih podatkov tahografa, kot je določeno v CSM_226. Nadzorna kartica odstrani zapolnitev in vrne dešifrirane koristne podatke tahografa daljinskemu poizvedovalniku.

CSM_229 Za preprečitev napadov s ponovitvijo daljinski poizvedovalnik preveri svežino podatkov RTM tako, da preveri, da trenutni datum in čas v zaščitnih podatkih DSRC ne odstopata preveč od trenutnega časa daljinskega poizvedovalnika.

Opombi:

— V ta namen mora imeti daljinski poizvedovalnik natančen in zanesljiv časovni vir.

— Ker dodatek 14 zahteva, da VU vsakih 60 sekund izračuna novo množico podatkov RTM, ura VU pa sme od resničnega časa odstopati za eno minuto, je spodnja meja svežine podatkov RTM dve minuti. Dejanska zahtevana svežina je odvisna tudi od natančnosti ure daljinskega poizvedovalnika.

CSM_230 Ko servisna delavnica preveri pravilno delovanje funkcije DSRC VU, celotne prejete podatke RTM pošlje iz VU v kartico servisne delavnice v podatkovnem polju ukaza PROCESS DSRC MESSAGE, kot je opisano v Dodatku 2. Kartica servisne delavnice opravi vse preglede in operacije iz CSM_228.

14. PODPIS PRENOSOV PODATKOV IN PREVERJANJE PODPISOV

14.1. **Splošno**

CSM_231 Inteligentna namenska oprema (IDE) shrani podatke, ki jih prejme od VU ali kartice, v eni seji prenosa podatkov v eni fizični podatkovni datoteki. Podatki so lahko shranjeni na ESM (zunanji pomnilniški medij). Ta datoteka vsebuje digitalne podpise na podlagi podatkovnih blokov, kakor je predpisano v Dodatku 7. Prav tako vsebuje naslednje certifikate (glej oddelek 9.1):

▼B

— v primeru prenosa podatkov VU:

— certifikat VU_Sign,

— certifikat MSCA_VU-EGF, ki vsebuje javni ključ, ki se uporablja za preverjanje certifikata VU_Sign;

— v primeru prenosa podatkov kartice:

— certifikat Card_Sign,

— certifikat MSCA_Card, ki vsebuje javni ključ, ki se uporablja za preverjanje certifikata Card_Sign.

CSM_232 IDE mora imeti tudi:

— če za preverjanje podpisa uporablja nadzorno kartico, kot je prikazano na sliki 13: vezni certifikat, ki povezuje zadnji certifikat EUR in certifikat EUR, ki je bil veljaven neposredno pred njim, če obstaja;

— če podpis preveri sama: vse veljavne evropske korenske certifikate.

Opomba: metoda, ki jo IDE uporablja za pridobivanje teh certifikatov, ni določena v tem dodatku.

14.2. **Ustvarjanje podpisa**

CSM_233 Algoritem podpisa za ustvarjanje digitalnih podpisov na podlagi prenesenih podatkov mora biti ECDSA, kot je določeno v [DSS], uporablja pa se zgoščevalni algoritem, ki ustreza velikosti ključa VU ali kartice, kot je določeno v CSM_50. Format podpisa je neformatirano besedilo, kot je določeno v [TR-03111].

14.3. **Preverjanje podpisa**

CSM_234 IDE lahko preverjanje podpisa na podlagi prenesenih podatkov opravi sama, ali pa za ta namen uporabi nadzorno kartico. Če uporablja nadzorno kartico, se preverjanje podpisa opravi, kot je prikazano na sliki 13. Če preverjanje podpisa opravi sama, IDE preveri avtentičnost in veljavnost vseh certifikatov v verigi certifikatov v podatkovni datoteki ter podpis glede na shemo podpisovanja, določeno v [DSS].

Opombe k sliki 13:

— Oprema, ki je podpisala podatke, ki se jih analizira, je označena kot EQT.

— Certifikati in javni ključi EQT iz slike so tisti za podpis, npr. VU_Sign ali Card_Sign.

— Certifikati in javni ključi EQT.CA iz slike so tisti za podpis certifikatov VU ali kartice, kot je primerno.

— Certifikat VU.CA.EUR iz slike je evropski korenski certifikat, ki je naveden v CAR certifikata EQT.CA.

▼B

— Omenjeni certifikat EQT.Link je vezni certifikat EQT, če obstaja. Kot je določeno v oddelku 9.1.2, je to vezni certifikat za nov evropski korenski par ključev, ki ga ustvari ERCA in se podpiše s prejšnjim evropskim zasebnim ključem.

— Certifikat EQT.Link.EUR je evropski korenski certifikat, ki je naveden v CAR certifikata EQT.Link.

CSM_235 Za izračun zgoščene vrednosti M, poslane v nadzorno kartico z ukazom PSO:Hash, IDE uporabi zgoščevalni algoritem, povezan z velikostjo ključa VU ali kartice, iz katere so podatki preneseni, kot je določeno v CSM_50.

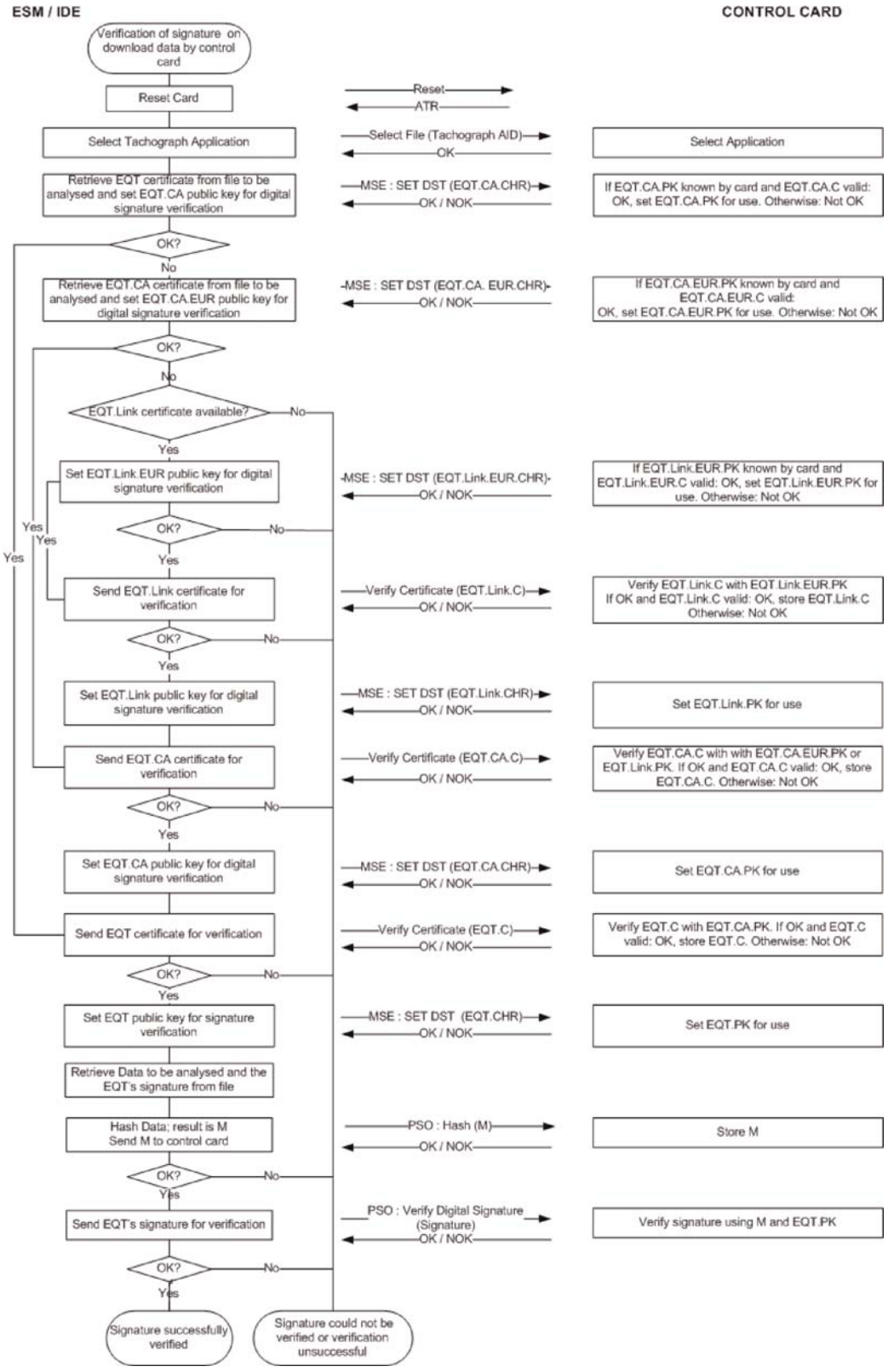
CSM_236 Za preverjanje podpisa EQT nadzorna kartica upošteva shemo podpisovanja, določeno v [DSS].

Opomba: Ta dokument ne določa potrebnih operacij, če podpisa na podlagi prenesene podatkovne datoteke ni mogoče preveriti ali če je preverjanje neuspešno.

▼B

Slika 13

Protokol za preverjanje podpisa glede na preneseno podatkovno datoteko



▼B

Dodatek 12

DOLOČANJE POLOŽAJA NA PODLAGI GLOBALNEGA SATELITSKEGA NAVIGACIJSKEGA SISTEMA (GNSS)

KAZALO

1. UVOD

1.1. Področje uporabe

1.2. Kratice in zapisi

2. SPECIFIKACIJA GNSS SPREJEMNIKA

3. SPOROČILA NMEA

4. ENOTA V VOZILU Z ZUNANJO GNSS OPREMO

4.1. Konfiguracija

4.1.1 Glavni sestavni deli in vmesniki

4.1.2 Stanje zunanje GNSS opreme ob koncu proizvodnje

4.2. Komunikacija med zunanjo GNSS opremo in enoto v vozilu

4.2.1 Komunikacijski protokol

4.2.2 Varen prenos GNSS podatkov

4.2.3 Struktura bralno-zapisovalnega ukaza

4.3. Povezovanje, medsebojna avtentikacija in uskladitev ključa seje med zunanjo GNSS opremo in enoto v vozilu

4.4. Obravnava napak

4.4.1 Napaka pri komuniciranju z zunanjo GNSS opremo

4.4.2 Kršenje fizične celovitosti zunanje GNSS opreme

4.4.3 Ni informacij o položaju s strani GNSS sprejemnika

4.4.4 Certifikat zunanje GNSS opreme je potekel

5. ENOTA V VOZILU BREZ ZUNANJE GNSS OPREME

5.1. Konfiguracija

5.2. Obravnava napak

5.2.1 Ni informacij o položaju s strani GNSS sprejemnika

6. ČASOVNO NAVZKRIŽJE Z GNSS

7. NAVZKRIŽJE V GIBANJU VOZILA

1. UVOD

V tem dodatku so navedene tehnične zahteve za GNSS podatke, ki jih uporablja enota v vozilu, vključno s protokoli, ki jih je treba izvajati, da se zagotovi varen in pravilen prenos informacij o položaju.

Glavni členi v Uredbi (EU) št. 165/2014, iz katerih izhajajo te zahteve, so: člen 8 (Zapisovanje položaja vozila v določenih trenutkih med dnevnim delovnim časom), člen 10 (Vmesnik za povezavo z inteligentnimi prometnimi sistemi) in člen 11 (Podrobne določbe za pametne tahografe).

▼B

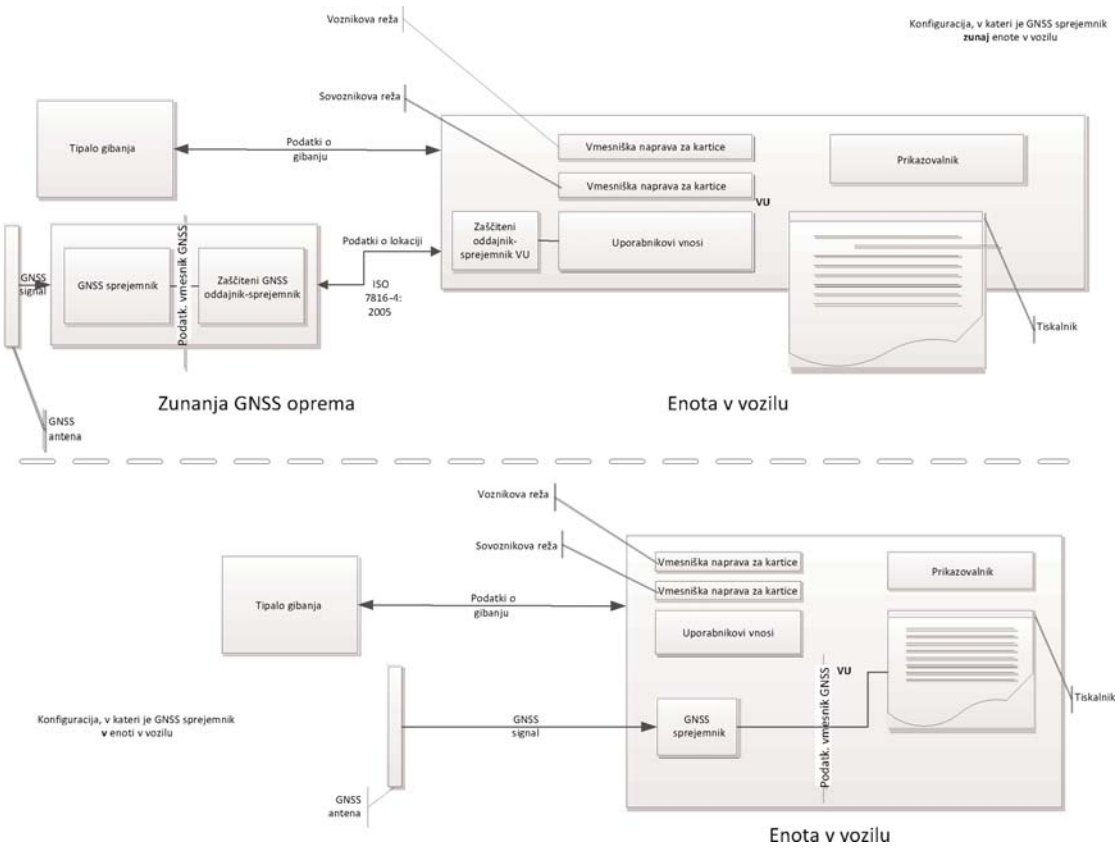
1.1. **Področje uporabe**

GNS_1 Enota v vozilu v podporo izvajanju člena 8 zbira podatke o lokaciji iz najmanj enega GNSS.

Enota v vozilu je lahko opremljena z zunanjo GNSS opremo ali pa ne, kot je opisano v sliki 1:

Slika 1

Različne konfiguracije GNSS sprejemnika



1.2. **Kratice in zapisi**

V tem dodatku se uporabljajo naslednje kratice:

DOP	napaka pri določanju položaja (Dilution of Precision)
EGF	elementarna datoteka GNSS opreme (Elementary file GNSS Facility)
EGNOS	skupna evropska geostacionarna navigacijska storitev (European Geostationary Navigation Overlay System)
GNSS	globalni satelitski navigacijski sistem (Global Navigation Satellite System)
GSA	GPS DOP in aktivni sateliti
HDOP	napaka pri določanju horizontalnega položaja (Horizontal Dilution of Precision)
ICD	kontrolni dokument vmesnika (Interface Control Document)
NMEA	Nacionalna zveza za pomorsko elektroniko ZDA (National Marine Electronics Association)

▼B

PDOP pozicijska napaka pri določanju položaja (Position Dilution of Precision)

RMC priporočeni minimalni specifični (Recommended Minimum Specific)

SIS signal v prostoru (Signal in Space)

VDOP napaka pri določanju vertikalnega položaja

VU enota v vozilu

2. SPECIFIKACIJA GNSS SPREJEMNIKA

Ne glede na to, ali ima pametni tahograf konfiguracijo z ali brez zunanje GNSS opreme, je zagotavljanje točnih in zanesljivih informacij o položaju bistveni element učinkovitega delovanja pametnega tahografa. Zato je primerno zahtevati njegovo združljivost s storitvami, ki jih zagotavljata programa Galileo in EGNOS (skupna evropska geostacionarna navigacijska storitev) iz Uredbe (EU) št. 1285/2013 Evropskega parlamenta in Sveta ([1]). Sistem, vzpostavljen s programom Galileo, je neodvisen globalni satelitski navigacijski sistem, medtem ko je sistem, vzpostavljen s programom EGNOS, regionalni satelitski navigacijski sistem za izboljšanje kakovosti signala globalnega pozicionirnega sistema (GPS).

GNS_2 Proizvajalci zagotovijo, da so GNSS sprejemniki v pametnih tahografih združljivi s storitvami določanja položaja, ki jih zagotavljata sistema Galileo in EGNOS. Proizvajalci lahko poleg tega zagotovijo tudi združljivost z drugimi satelitskimi navigacijskimi sistemi.

GNS_3 Sprejemnik GNSS omogoča podporo avtentikaciji na odprti storitvi Galileo, ko bo sistem Galileo zagotavljal to storitev in jo bodo podpirali proizvajalci GNSS sprejemnikov. Vendar pametnih tahografov, ki se dajo na trg, preden so izpolnjeni zgornji pogoji, in ne omogočajo podpore avtentikaciji na odprti storitvi Galileo, ne bo treba prilagajati.

3. SPOROČILA NMEA

V tem oddelku so opisana sporočila NMEA, ki se uporabljajo pri delovanju pametnih tahografov. Ta oddelek velja tako za konfiguracijo pametnih tahografov z zunanjo GNSS opremo kot tudi za konfiguracijo brez nje.

GNS_4 Podatki o lokaciji temeljijo na priporočenih minimalnih specifičnih (RMC) GNSS podatkih, ki vsebujejo informacijo o položaju (zemljepisna širina in dolžina), času v formatu UTC (hhmmss.ss) in hitrosti v primerjavi s tlemi v vozlih ter dodatne vrednosti.

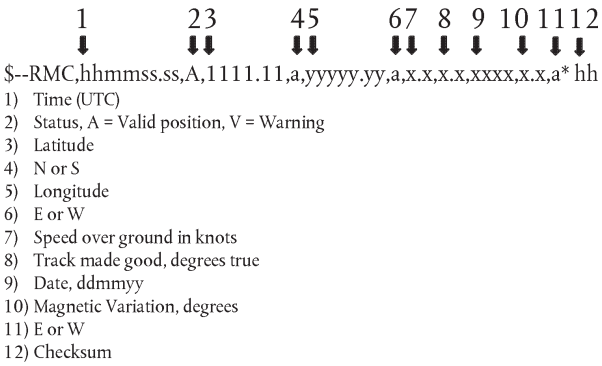
Format RMC sporočila je naslednji (povzeto po standardu NMEA V4.1):

([1]) Uredba (EU) št. 1285/2013 Evropskega parlamenta in Sveta z dne 11. decembra 2013 o vzpostavitvi in obratovanju evropskih satelitskih navigacijskih sistemov ter razveljavitvi Uredbe Sveta (ES) št. 876/2002 in Uredbe (ES) št. 683/2008 Evropskega parlamenta in Sveta (UL L 347, 20.12.2013, str. 1).

▼B

Slika 2

Struktura RMC sporočila



Stanje podaja informacijo o razpoložljivosti GNSS signala. Dokler stanje ni določeno kot A, se sprejeti podatki (npr. o času ali zemljepisni širini/dolžini) ne morejo uporabiti za zapisovanje položaja vozila v VU.

Ločljivost določitve položaja temelji na formatu zgoraj opisanega RMC sporočila. Prvi del polja 3 in polja 5 (prvi dve števki) predstavljata stopinje. Preostala mesta predstavljajo minute s tremi decimalnimi mesti. Ločljivost je tako 1/1000 minute ali 1/60000 stopinje (kajti ena minuta je 1/60 stopinje).

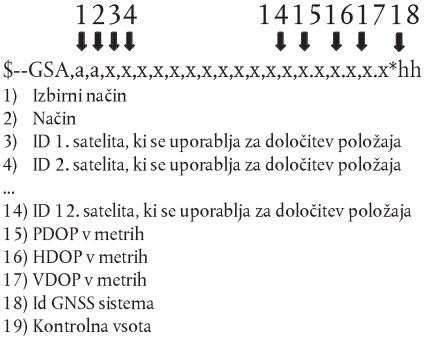
GNS_5 Enota v vozilu v svoj pomnilnik shrani informacijo o položaju glede na zemljepisno širino in dolžino z ločljivostjo 1/10 minute ali 1/600 stopinje, kot je opisano v Dodatku 1 za tip GeoCoordinates.

VU lahko uporabi ukaz GPS DOP in aktivni sateliti (GSA), da določi in zapiše razpoložljivost signala in točnost meritve. Za oceno ravni točnosti zapisanih podatkov o lokaciji se uporablja zlasti HDOP (glej 4.2.2). VU shrani vrednost napake pri določanju horizontalnega položaja (HDOP), izračunano kot minimalno vrednost HDOP, pridobljeno od razpoložljivih sistemov GNSS.

GNSS System Id označuje bodisi GPS, Glonass, Galileo, Beidou ali satelitski dopolnilni sistem (SBAS).

Slika 3

Struktura sporočila GSA



▼B

Način (2) podaja informacijo, da določitev položaja ni na voljo (Način=1) ali da določitev položaja je na voljo v 2D (Način=2) ali 3D (Način=3).

GNS_6 Sporočilo *GSA* se shrani pod številko zapisa ‘06’.

GNS_7 Največja velikost sporočil NMEA (npr. RMC, GSA ali drugih), ki se lahko uporabi za bralno-zapisovalni ukaz, je 85 bajtov (glej preglednico 1).

4. ENOTA V VOZILU Z ZUNANJO GNSS OPREMO

4.1. **Konfiguracija**

4.1.1 *Glavni sestavni deli in vmesniki*

V tej konfiguraciji je GNSS sprejemnik del zunanje GNSS opreme.

GNS_8 Zunanjo GNSS opremo mora napajati posebni vmesnik z vozilom.

GNS_9 Zunanja GNSS oprema sestoji iz naslednjih delov (glej sliko 4):

a) komercialnega GNSS sprejemnika za zagotavljanje podatkov o položaju preko podatkovnega vmesnika GNSS. Tako je na primer podatkovni vmesnik GNSS lahko standard NMEA V4.10, pri čemer sprejemnik GNSS deluje kot govorec in prenaša sporočila NMEA zaščitenemu GNSS oddajniku-sprejemniku s frekvenco 1Hz za predhodno opredeljen nabor sporočil NMEA, ki morajo vključevati vsaj RMC sporočila in sporočila GSA. Izvedba podatkovnega vmesnika GNSS je v domeni proizvajalcev zunanje GNSS opreme;

b) Oddajno-sprejemne enote (zaščiteni GNSS oddajnik-sprejemnik) z zmožnostjo podpore za standard ISO/IEC 7816-4:2013 (glej 4.2.1) za komuniciranje z enoto v vozilu in podporo podatkovnemu vmesniku GNSS s sprejemnikom GNSS. Enota vsebuje pomnilnik za shranjevanje identifikacijskih podatkov GNSS sprejemnika in zunanje GNSS opreme;

c) ohišje s funkcijo zaznavanja poskusov manipulacije, ki vsebuje tako GNSS sprejemnik kot tudi zaščiteni GNSS oddajnik-sprejemnik. Funkcija zaznavanja poskusov manipulacije je dopolnjena z varnostno-zaščitnimi ukrepi, kot jih zahteva profil zaščite pametnega tahografa;

d) GNSS anteno, ki je nameščena na vozilo in preko ohišja povezana z GNSS sprejemnikom.

GNS_10 Zunanja GNSS oprema ima vsaj naslednja zunanja vmesnika:

a) vmesnik z GNSS anteno, nameščeno na strehi tovornega vozila, če se antena uporablja;

b) vmesnik z enoto v vozilu.

GNS_11 V VU je drugi, končni del varne komunikacije z zaščitenim GNSS oddajnikom-sprejemnikom oddajnik-sprejemnik VU, ki mora podpirati standard ISO/IEC 7816-4:2013 za povezavo z zunanjo GNSS opremo.

▼B

GNS_12 Za fizični sloj komunikacije z zunanjo GNSS opremo enota v vozilu podpira standard ISO/IEC 7816-12:2005 ali drug standard, ki omogoča podporo standardu ISO/IEC 7816-4:2013 (glej 4.2.1).

4.1.2 *Stanje zunanje GNSS opreme ob koncu proizvodnje*

GNS_13 Ko zapusti tovarno, ima zunanja GNSS oprema v trajnem pomnilniku zaščitenega GNSS oddajnika-sprejemnika shranjene naslednje vrednosti:

— par ključev EGF_MA in ustrezni certifikat,

— certifikat MSCA_VU-EGF, ki vsebuje javni ključ MSCA_VU-EGF.PK, ki se uporablja za preverjanje certifikata EGF_MA,

— certifikat EUR, ki vsebuje javni ključ EUR.PK, ki se uporablja za preverjanje certifikata MSCA_VU-EGF,

— certifikat EUR, katerega obdobje veljavnosti je neposredno pred obdobjem veljavnosti certifikata EUR, ki se uporablja za preverjanje certifikata MSCA_VU-EGF, če obstaja,

— vezni certifikat, ki povezuje ta dva certifikata EUR, če obstaja,

— podaljšano serijsko številko zunanje GNSS opreme,

— identifikator operacijskega sistema GNSS opreme,

— homologacijsko številko zunanje GNSS opreme,

— identifikator varnostnega dela zunanjega GNSS modula.

4.2. **Komunikacija med zunanjo GNSS opremo in enoto v vozilu**

4.2.1 *Komunikacijski protokol*

GNS_14 Komunikacijski protokol za komunikacijo med zunanjo GNSS opremo in enoto v vozilu podpira tri funkcije:

1. zbiranje in distribucijo GNSS podatkov (npr. položaj, čas, hitrost),

2. zbiranje podatkov o konfiguraciji zunanje GNSS opreme,

3. protokol za upravljanje za podporo povezovanju, medsebojni avtentikaciji in uskladitvi ključa seje med GNSS opremo in VU.

GNS_15 Komunikacijski protokol temelji na standardu ISO/IEC 7816-4:2013, pri čemer ima zaščiteni oddajnik-sprejemnik VU nadrejeno, zaščiteni GNSS oddajnik-sprejemnik pa podrejeno vlogo. Fizična povezava med zunanjo GNSS opremo in enoto v vozilu temelji na standardu ISO/IEC 7816-12:2005 ali drugem standardu, ki omogoča podporo standardu ISO/IEC 7816-4:2013.

▼B

GNS_16 V komunikacijskem protokolu podaljšana podatkovna polja niso podprta.

GNS_17 Komunikacijski protokol iz standarda ISO 7816 (tako *-4:2013 kot tudi *-12:2005) za komunikacijo med zunanjo GNSS opremo in VU je nastavljen na T=1.

GNS_18 V zvezi s funkcijami 1 (zbiranje in distribucija GNSS podatkov), 2 (zbiranje podatkov o konfiguraciji zunanje GNSS opreme) in 3 (protokol za upravljanje) zaščiteni GNSS oddajnik-sprejemnik simulira pametno kartico, katere arhitektura datotečnega sistema sestoji iz glavne datoteke (MF), namenske datoteke (DF) z identifikatorjem aplikacije v skladu s poglavjem 6.2 Dodatka 1 (‘FF 44 54 45 47 4D’) ter tremi elementarnimi datotekami, ki vsebujejo certifikate, in eno samo elementarno datoteko (EF.EGF) z identifikatorjem datotek ‘2F2F’, kot je opisano v preglednici 1.

GNS_19 Zaščiteni GNSS oddajnik-sprejemnik podatke, ki prihajajo od GNSS sprejemnika, in konfiguracijo shrani v EF.EGF. To je linearna datoteka spremenljive dolžine z identifikatorjem ‘2F2F’ v šestnajstiški obliki.

GNS_20 Zaščiteni GNSS oddajnik-sprejemnik za shranjevanje podatkov uporablja pomnilnik, ki je zmožen opraviti vsaj 20 milijonov bralno/pisalnih ciklov. Razen tega sta zasnova notranjosti in izvedba zaščitenega GNSS oddajnika-sprejemnika v domeni proizvajalcev.

Preslikava zapisanih števil in podatkov je določena v preglednici 1. Treba je opozoriti, da obstajajo štiri sporočila GSA za štiri satelitske sisteme in satelitski dopolnilni sistem (SBAS).

GNS_21 Datotečna struktura je določena v preglednici 1. Za pogoje dostopa (ALW, NEV, SM-MAC) glej poglavje 3.5 Dodatka 2.

Preglednica 1

Datotečna struktura

		Pogoji dostopa		
Datoteka	ID datoteke	Branje	Posodobitev	Šifrirana
MF	3F00			
EF.ICC	0002	ALW	NEV (prek VU)	Ne
DF GNSS opreme	0501	ALW	NEV	Ne
EF EGF_MACertificate	C100	ALW	NEV	Ne
EF CA_Certificate	C108	ALW	NEV	Ne
EF Link_Certificate	C109	ALW	NEV	Ne
EF.EGF	2F2F	SM-MAC	NEV (prek VU)	Ne

▼B

Datoteka/podatkovni element	Št. zapisa	Velikost (v bajtih)		Privzete vrednosti
		Min.	Maks.	
MF		552	1 031	
EF.ICC				
sensorGNSSSerialNumber		8	8	
DF GNSS opreme		*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				
RMC sporočilo NMEA	‘01’	85	85	
1. sporočilo GSA NMEA	‘02’	85	85	
2. sporočilo GSA NMEA	‘03’	85	85	
3. sporočilo GSA NMEA	‘04’	85	85	
4. sporočilo GSA NMEA	‘05’	85	85	
5. sporočilo GSA NMEA	‘06’	85	85	
Podaljšana serijska številka zunanje GNSS opreme, v Dodatku 1 opredeljena kot SensorGNSSSerialNumber.	‘07’	8	8	
Identifikator operacijskega sistema zaščitenega GNSS oddajnika-sprejemnika, v Dodatku 1 opredeljen kot SensorOSIdentifier.	‘08’	2	2	
Homologacijska številka zunanje GNSS opreme, v Dodatku 1 opredeljena kot SensorExternalGNSSApprovalNumber.	‘09’	16	16	
Identifikator varnostnega dela zunanje GNSS opreme, v Dodatku 1 opredeljen kot SensorExternalGNSSSCIdentifier.	‘10’	8	8	
RFU – rezervirana za prihodnjo uporabo	Od ‘11’ do ‘FD’			

4.2.2 *Varen prenos GNSS podatkov*

GNS_22 Varen prenos GNSS podatkov o položaju je dovoljen samo, če sta izpolnjena naslednja pogoja:

1. postopek povezovanja je bil dokončan, kot je opisano v Dodatku 11 (Skupni varnostni mehanizmi);

▼B

2. redna medsebojna avtentikacija in uskladitev ključa seje med VU in zunanjo GNSS opremo, kot sta prav tako opisana v Dodatku 11 (Skupni varnostni mehanizmi), sta bila izvedena z ustrezno pogostostjo.

GNS_23 Vsakih T sekund, pri čemer je vrednost T manjša ali enaka 10, razen če se izvaja povezovanje ali medsebojna avtentikacija in uskladitev ključa seje, VU od zunanje GNSS opreme zahteva informacije o položaju v skladu z naslednjim postopkom:

1. VU od zunanje GNSS opreme zahteva podatke o lokaciji, skupaj s podatki o napaki pri določanju položaja (iz sporočila GSA NMEA). Zaščiteni oddajnik-sprejemnik VU prek varnega sporočanja v načinu „samo avtentikacija“, kot je opisano v oddelku 11.5 Dodatka 11, uporabi ukaza SELECT in READ RECORD(S) v skladu s standardom ISO/IEC 7816-4:2013 z identifikatorjem datotek ‘2F2F’ ter številko zapisa RECORD ‘01’ za RMC sporočilo NMEA ter ‘02’, ‘03’, ‘04’, ‘05’ in ‘06’ za sporočilo GSA NMEA.

2. Zadnji prejeti podatki o lokaciji se shranijo v EF z identifikatorjem ‘2F2F’, zapisi, opisani v preglednici 1, pa v zaščitenem GNSS oddajniku-sprejemniku, pri čemer zaščiteni GNSS oddajnik-sprejemnik podatke NMEA sprejema od GNSS sprejemnika preko podatkovnega vmesnika GNSS s frekvenco najmanj 1 Hz.

3. Zaščiteni GNSS oddajnik-sprejemnik pošlje odziv zaščitenemu oddajniku-sprejemniku VU s sporočilom odziva APDU prek varnega sporočanja v načinu „samo avtentikacija“, kot je opisano v oddelku 11.5 Dodatka 11.

4. Zaščiteni oddajnik-sprejemnik VU preverja avtentičnost in celovitost prejetega odziva. Če je rezultat pozitiven, se podatki o lokaciji preko podatkovnega vmesnika GNSS prenesejo procesorju VU.

5. Procesor VU preveri prejete podatke z izluščenjem informacij (npr. o zemljepisni širini in dolžini, času) iz RMC sporočila NMEA. RMC sporočilo NMEA vključuje informacijo o tem, ali je položaj veljaven. Če položaj ni veljaven, podatki o lokaciji še niso na voljo in se jih ne sme uporabiti za zapisovanje položaja vozila. Če je položaj veljaven, procesor VU iz stavkov GSA NMEA izlušči tudi vrednosti HDOP in izračuna povprečno vrednost za razpoložljive satelitske sisteme (tj. ko je določitev položaja na voljo).

6. Prejete in obdelane informacije, kot so zemljepisna širina/dolžina, čas in hitrost, procesor VU shrani v VU v formatu, opredeljenem v Dodatku 1 (Slovar podatkov) kot GeoCoordinates, skupaj z vrednostjo HDOP, izračunano kot najmanjša od vrednosti, zbranih preko razpoložljivih sistemov GNSS.

▼B

4.2.3 *Struktura bralno-zapisovalnega ukaza*

V tem oddelku je podobno opisana struktura bralno-zapisovalnega ukaza. Doda se varno sporočanje (v načinu „samo avtentikacija“), kot je opisano v Dodatku 11 (Skupni varnostni mehanizmi).

GNS_24 Ukaz podpira varno sporočanje v načinu „samo avtentikacija“, glej Dodatek 11.

GNS_25 Ukazno sporočilo

Bajt	Dolžina	Vrednost	Opis
CLA	1	‘0CH’	Zahtevano varno sporočanje.
INS	1	‘B2h’	Read Record (branje in zapisovanje)
P1	1	‘XXh’	Številka zapisa (‘00’ pomeni tekoči zapis)
P2	1	‘04h’	Preberi zapis s številko zapisa, navedeno v P1
Le	1	‘XXh’	Pričakovana dolžina podatkov. Število bajtov, ki se preberejo.

GNS_26 Zapis iz P1 postane tekoči zapis.

Bajt	Dolžina	Vrednost	Opis
#1-#X	X	‘XX..XXh’	Prebrani podatki
SW	2	‘XXXXh’	Opis stanja (SW1, SW2)

— Če je ukaz uspešen, zaščiteni GNSS oddajnik-sprejemnik vrne sporočilo ‘**9000**’.

— Če tekoča datoteka ni namenjena zapisu, zaščiteni GNSS oddajnik-sprejemnik vrne sporočilo ‘**6981**’.

— Če se ukaz uporabi s P1 = ‘00’, vendar tekoča EF ne obstaja, zaščiteni GNSS oddajnik-sprejemnik vrne sporočilo ‘**6986**’ (ukaz ni dovoljen).

— Če zapis ni bil najden, zaščiteni GNSS oddajnik-sprejemnik vrne sporočilo ‘**6A 83**’.

— Če je zunanja GNSS oprema zaznala poskus manipulacije, vrne sporočilo z opisom stanja ‘**66 90**’.

GNS_27 Zaščiteni GNSS oddajnik-sprejemnik podpira naslednje ukaze tahografov druge generacije, kot so opredeljene v Dodatku 2:

Ukaz	Referenca
Select	poglavje 3.5.1 Dodatka 2
Read Binary	poglavje 3.5.2 Dodatka 2
Get Challenge	poglavje 3.5.4 Dodatka 2
PSO: Verify Certificate	poglavje 3.5.7 Dodatka 2
External Authenticate	poglavje 3.5.9 Dodatka 2
General Authenticate	poglavje 3.5.10 Dodatka 2
MSE:SET	poglavje 3.5.11 Dodatka 2

▼B

4.3. **Povezovanje, medsebojna avtentikacija in uskladitev ključa seje med zunanjo GNSS opremo in enoto v vozilu**

Povezovanje, medsebojna avtentikacija in uskladitev ključa seje med zunanjo GNSS opremo in enoto v vozilu so opisani v poglavju 11 Dodatka 11 (Skupni varnostni mehanizmi).

4.4. **Obravnava napak**

V tem oddelku je opisano, kako zunanja GNSS naprava obravnava morebitna stanja z napakami in kako se zapišejo v VU.

4.4.1 *Napaka pri komuniciranju z zunanjo GNSS opremo*

GNS_28 Če VU povezani zunanji GNSS opremi več kot 20 zaporednih minut ne uspe sporočiti ničesar, VU ustvari in v VU zapiše dogodek vrste EventFaultType z vrednostjo enum ‘53’H *External GNSS communication fault*, ki mu dodeli časovni žig s trenutnim časom. Dogodek bo ustvarjen samo, če sta izpolnjena naslednja pogoja: a) pametni tahograf ni v kalibracijskem načinu in b) vozilo se premika. V tem kontekstu se napaka pri komuniciranju sproži, kadar zaščiteni oddajnik-sprejemnik VU ne prejme sporočila odziva po poslanem sporočilu z zahtevkom, kot je opisano v oddelku 4.2.

4.4.2 *Kršenje fizične celovitosti zunanje GNSS opreme*

GNS_29 Če je prekršena celovitost zunanje GNSS opreme, zaščiteni GNSS oddajnik-sprejemnik v celoti izbriše svoj pomnilnik, vključno s kriptografskimi gradivi. Kot je opisano v GNS_25 in GNS_26, VU zazna poskus manipulacije, če je stanje odziva ‘6690’. VU nato ustvari dogodek vrste EventFaultType z vrednostjo enum *‘55’H Tamper detection of GNSS*.

4.4.3 *Ni informacij o položaju s strani GNSS sprejemnika*

GNS_30 Če zaščiteni GNSS oddajnik-sprejemnik več kot 3 zaporedne ure od GNSS sprejemnika ne prejme nobenih podatkov, zaščiteni GNSS oddajnik-sprejemnik na ukaz READ RECORD ustvari sporočilo odziva s številko RECORD ‘01’ in podatkovnim poljem v dolžini 12 bajtov, ki so vsi nastavljeni na 0xFF. Po prejemu sporočila odziva s to vrednostjo podatkovnega polja, VU ustvari in zapiše dogodek vrste EventFaultType z vrednostjo enum ‘52’H *External GNSS receiver fault*, ki mu dodeli časovni žig s trenutnim časom, samo, če sta izpolnjena naslednja pogoja: a) pametni tahograf ni v kalibracijskem načinu in b) vozilo se premika.

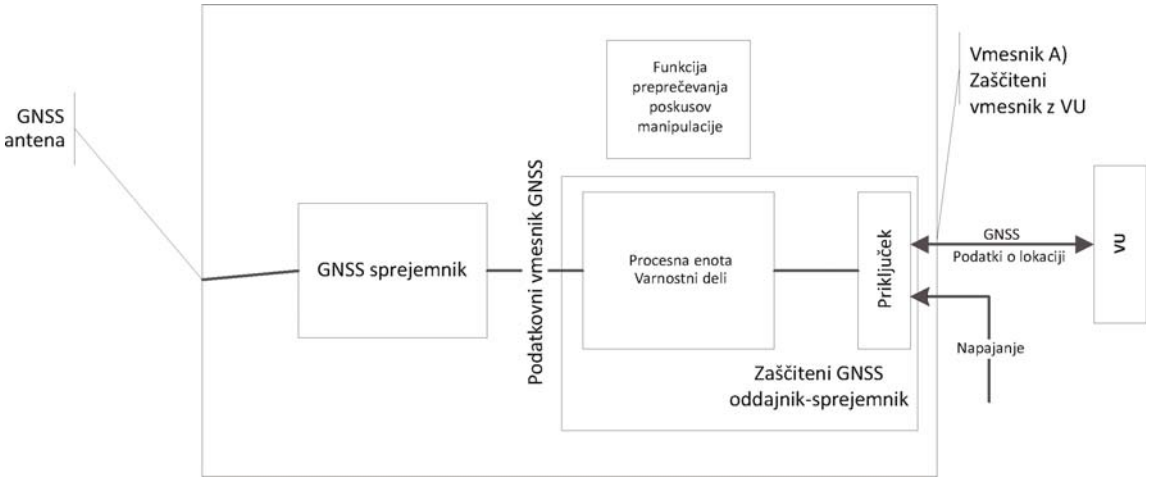
4.4.4 *Certifikat zunanje GNSS opreme je potekel*

GNS_31 Če VU zazna, da certifikat EGF, ki se uporablja za medsebojno avtentikacijo, ni več veljaven, VU ustvari in zapiše napako na zapisovalni napravi vrste EventFaultType z vrednostjo enum *‘56’H External GNSS facility certificate expired*, ki ji dodeli časovni žig s trenutnim časom. VU kljub temu uporabi prejete GNSS podatke o položaju.

▼B

Slika 4

Shema zunanje GNSS opreme



5. ENOTA V VOZILU BREZ ZUNANJE GNSS OPREME

5.1. **Konfiguracija**

V tej konfiguraciji je GNSS sprejemnik v enoti v vozilu, kot je opisano v sliki 1.

GNS_32 Sprejemnik GNSS deluje kot govorec in prenaša sporočila NMEA procesorju VU, ki deluje kot poslušalec, s frekvenco 1/10 Hz ali hitreje za predhodno opredeljen nabor sporočil NMEA, ki vključujejo vsaj RMC sporočila in sporočila GSA.

GNS_33 Zunanja GNSS antena, nameščena na vozilo, ali notranja GNSS antena je priključena na VU.

5.2. **Obravnava napak**

5.2.1 *Ni informacij o položaju s strani GNSS sprejemnika*

GNS_34 Če VU več kot 3 zaporedne ure od GNSS sprejemnika ne prejme nobenih podatkov, VU ustvari in zapiše dogodek vrste EventFaultType z vrednostjo enum '51'H *Internal GNSS receiver fault*, ki mu dodeli časovni žig s trenutnim časom, samo, če sta izpolnjena naslednja pogoja: a) pametni tahograf ni v kalibracijskem načinu in b) vozilo se premika.

6. ČASOVNO NAVZKRIŽJE Z GNSS

Če VU zazna odstopanje, večje od 1 minute, med časom, ki ga beleži funkcija za merjenje časa enote v vozilu, in časom, ki ga posreduje GNSS sprejemnik, VU zapiše dogodek vrste EventFaultType z vrednostjo enum *'0B'H Time conflict (GNSS versus VU internal clock)*. Ta dogodek se zapiše skupaj z internim časom enote v vozilu in ga spremlja samodejna nastavitev časa. Po sproženju dogodka časovnega navzkrižja enota v vozilu naslednjih 12 ur ne preverja časovnega navzkrižja. Ta dogodek se ne sproži, kadar GNSS sprejemnik v zadnjih 30 dneh ni mogel odkriti veljavnega GNSS signala. Ko so informacije o položaju prek GNSS sprejemnika spet na voljo, se opravi samodejna nastavitev časa.

▼B

7. NAVZKRIŽJE V GIBANJU VOZILA

GNS_35 VU sproži in zapiše dogodek „navzkrižje v gibanju vozila“ (glej zahtevo 84 v tej prilogi) s časovnim žigom s trenutnim časom, če informacije o gibanju vozila, izračunane na podlagi podatkov iz tipala gibanja, nasprotujejo informacijam o gibanju vozila, pridobljenih prek notranje ali zunanje GNSS opreme Za odkrivanje takih protislovij se uporabi mediana razlik v hitrosti med tema viroma, kot je določeno spodaj:

— največ vsakih 10 sekund se izračuna absolutna vrednost razlike med hitrostjo vozila, ocenjeno na podlagi podatkov iz GNSS, in hitrostjo vozila, ocenjeno na podlagi podatkov s tipala gibanja;

— za izračun mediane se uporabijo vse izračunane vrednosti v časovnem oknu, ki vključuje zadnjih pet minut gibanja;

— mediana se izračuna kot povprečje 80 % vrednosti, preostalih po izločitvi najvišjih absolutnih vrednosti.

Dogodek „navzkrižje v gibanju vozila“ se sproži, če je mediana večja od 10 km/h za zadnjih pet neprekinjenih minut gibanja vozila. Neobvezno se lahko uporabijo tudi drugi neodvisni viri zaznavanja gibanja vozila, da se omogoči bolj zanesljivo zaznavanje manipuliranja s tahografom. (*Opomba:* uporaba mediane za zadnjih 5 minut zmanjša tveganje osamelcev in prehodnih vrednosti.) Ta dogodek se ne sproži v naslednjih okoliščinah: (a) med prevozom s trajektom/vlakom, (b) kadar informacije o položaju s strani GNSS sprejemnika niso na voljo in (c) v kalibracijskem načinu.

▼B

Dodatek 13

VMESNIK Z ITS

KAZALO

1. UVOD

2. PODROČJE UPORABE

2.1. Kratice, opredelitve in zapisi

3. REFERENČNE UREDBE IN STANDARDI

4. NAČELA DELOVANJA VMESNIKA

4.1. Predpogoji za prenos podatkov prek vmesnika z ITS

4.1.1 Podatki, ki se zagotovijo prek vmesnika z ITS

4.1.2 Vsebina podatkov

4.1.3 Aplikacije ITS

4.2. Komunikacijska tehnologija

4.3. Avtorizacija PIN

4.4. Format sporočil

4.5. Privolitev voznika

4.6. Pridobivanje standardnih podatkov

4.7. Pridobivanje osebnih podatkov

4.8. Pridobivanje podatkov o dogodkih in napakah

1. UVOD

Ta dodatek določa zasnovo in postopke, ki jih je treba upoštevati pri namestitvi vmesnika z inteligentnimi prometnimi sistemi (ITS), kot je zahtevano v členu 10 Uredbe (EU) št. 165/2014 (v nadaljnjem besedilu: *Uredba*).

Uredba določa, da se tahografi vozil lahko opremijo s standardiziranimi vmesniki, ki v delovnem načinu na zunanji napravi omogočajo uporabo podatkov, ki jih je zapisal ali izdelal tahograf, če so izpolnjeni naslednji pogoji:

(a) vmesnik ne vpliva na avtentičnost in celovitost podatkov tahografa;

(b) vmesnik izpolnjuje podrobne določbe iz člena 11 Uredbe;

(c) zunanja naprava, povezana z vmesnikom, ima dostop do osebnih podatkov, vključno s podatki za geografsko določitev položaja, samo po preverljivi privolitvi voznika, na katerega se podatki nanašajo.

2. PODROČJE UPORABE

Namen tega dodatka je opredeliti, kako lahko aplikacije na zunanji napravi prek povezave Bluetooth® pridobijo podatke (v nadaljnjem besedilu: *podatki*) iz tahografa.

Podatki, dostopni prek tega vmesnika, so opisani v Prilogi 1 tega dokumenta. Vmesnik ne prepoveduje uporabe vmesnikov (npr. prek vodila CAN) za prenos podatkov VU na druge procesne enote vozila.

▼B

Ta dodatek opredeljuje:

— *podatke*, dostopne prek vmesnika z ITS,

— profil Bluetooth®, ki se uporablja za prenos podatkov,

— postopke za zahtevek in prenos ter zaporedje operacij,

— povezovalni mehanizem med tahografom in zunanjo napravo,

— mehanizem privolitve voznika.

Ta priloga ne opredeljuje naslednjega:

— operacij in vodenja v zvezi z zbiranjem *podatkov* v VU (to je opredeljeno drugje v *Uredbi* ali pa je odvisno od zasnove izdelka),

— oblike predstavitve zbranih podatkov v aplikaciji na zunanji napravi,

— določb o varnosti podatkov, ki presegajo Bluetooth® (npr. šifriranje) in zadevajo vsebino *podatkov* (te so določene drugje v *Uredbi* [Dodatek 10 Skupni varnostni mehanizmi]).

— protokolov Bluetooth®, ki jih uporablja vmesnik z ITS.

2.1. **Kratice, opredelitve in zapisi**

V tem dodatku se uporabljajo naslednje kratice in opredelitve, specifične za ta dodatek:

komunikacija	izmenjava informacij/podatkov med glavno enoto (tj. tahografi) in zunanjo enoto prek vmesnika z ITS z uporabo Bluetooth®
podatki	nizi podatkov, kot so določeni v Prilogi 1
Uredba	Uredba (EU) št. 165/2014 Evropskega parlamenta in Sveta z dne 4. februarja 2014 o tahografih v cestnem prometu, razveljavitvi Uredbe Sveta (EGS) št. 3821/85 o tahografu (nadzorni napravi) v cestnem prometu in spremembi Uredbe (ES) št. 561/2006 Evropskega parlamenta in Sveta o usklajevanju določene socialne zakonodaje v zvezi s cestnim prometom
BR	Basic Rate (osnovna stopnja prenosa)
EDR	Enhanced Data Rate (povečana stopnja prenosa podatkov)
GNSS	Global Navigation Satellite System (globalni satelitski navigacijski sistem)
IRK	Identity Resolution Key (ključ za določanje identitete)
ITS	Intelligent Transport System (inteligentni prometni sistem)
LE	Low Energy (nizkoenergijski)
PIN	Personal Identification Number (osebna identifikacijska številka)
PUC	Personal Unblocking Code (osebna številka za odklepanje)
SID	Service Identifier (identifikator storitev)
SPP	Serial Port Profile (profil serijskih vrat)

▼B

SSP	Secure Simple Pairing (varna enostavna povezava)
TRTP	Transfer Request Parameter (parameter zahtevka za prenos)
TREP	Transfer Response Parameter (parameter zahtevka za odziv)
VU	Vehicle Unit (enota v vozilu)

3. REFERENČNE UREDBE IN STANDARDI

Opredelitve iz tega dodatka se sklicujejo na naslednje uredbe in standarde in so od njih odvisne. V določbah tega dodatka so opredeljeni zadevni standardi ali zadevne določbe standardov. V primeru protislovij imajo prednost določbe tega dodatka.

Referenčne uredbe in standardi za ta dodatek so:

— Uredba (EU) št. 165/2014 Evropskega parlamenta in Sveta z dne 4. februarja 2014 o tahografih v cestnem prometu, razveljavitvi Uredbe Sveta (EGS) št. 3821/85 o tahografu (nadzorni napravi) v cestnem prometu in spremembi Uredbe (ES) št. 561/2006 Evropskega parlamenta in Sveta o usklajevanju določene socialne zakonodaje v zvezi s cestnim prometom

— Uredba (ES) št. 561/2006 Evropskega parlamenta in Sveta z dne 15. marca 2006 o usklajevanju določene socialne zakonodaje v zvezi s cestnim prometom in spremembi uredb Sveta (EGS) št. 3821/85 in (ES) št. 2135/98 ter razveljavitvi Uredbe Sveta (EGS) št. 3820/85

— ISO 16844 – 4: Road vehicles – Tachograph systems – Part 4: Can interface

— ISO 16844 – 7: Road vehicles – Tachograph systems – Part 7: Parameters

— Bluetooth® – Serial Port Profile – V1.2

— Bluetooth® – Core Version 4.2

— NMEA 0183 V4.1 protocol

4. NAČELA DELOVANJA VMESNIKA

4.1. **Predpogoji za prenos podatkov prek vmesnika z ITS**

VU je odgovorna za posodabljanje in vzdrževanje podatkov, ki se shranijo v VU, brez vključevanja vmesnika z ITS. VU to opravi z internimi sredstvi, ki so določena drugje v Uredbi in niso opredeljena v tem dodatku.

4.1.1 *Podatki, ki se zagotovijo prek vmesnika z ITS*

VU je odgovorna za posodabljanje podatkov, ki se zagotovijo prek vmesnika z ITS, in sicer tako pogosto, kot je določeno v postopkih VU, in brez vključevanja vmesnika ITS. Podatki VU se uporabljajo kot podlaga za vnos in posodobitev *podatkov*; sredstva, s katerimi se to opravi, so opredeljena drugje v *Uredbi* ali, če takih določb ni, odvisna od zasnove izdelka in niso opredeljena v tem dodatku.

▼B

4.1.2 *Vsebina podatkov*

Vsebina *podatkov* je takšna, kot je določeno v Prilogi 1 k temu dodatku.

4.1.3 *Aplikacije ITS*

Aplikacije ITS bodo podatke, ki se zagotovijo prek vmesnika z ITS, uporabljale npr. za optimizacijo upravljanja voznikovih dejavnosti ob upoštevanju Uredbe, za zaznavanje morebitnih napak tahografa ali za uporabo podatkov GNSS. Aplikacije niso opredeljene v tem dodatku.

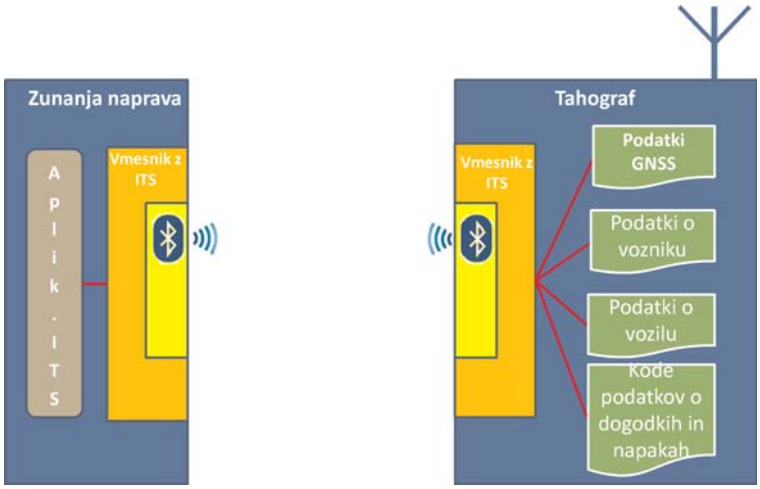
4.2. **Komunikacijska tehnologija**

Izmenjava *podatkov* z uporabo vmesnika z ITS se opravi prek vmesnika Bluetooth®, združljivega z različico 4.2 ali kasnejšo različico. Bluetooth® deluje v brezlicenčnem pasu 2,4 do 2,485 GHz, ki je namenjen za industrijske, znanstvene in medicinske namene (ISM). Bluetooth® 4.2 omogoča okrepljene mehanizme zasebnosti in zaščite ter večjo hitrost in zanesljivost prenosa podatkov. Za namene te opredelitve se radijski sistem Bluetooth® razreda 2 uporablja z dosegom do 10 metrov. Več informacij o Bluetooth® 4.2 je na voljo na www.bluetooth.com (https://www.bluetooth.org/en-us/specification/adopted-specifications?_ga=1.215147412.2083380574.1435305676).

Komunikacija se vzpostavi s komunikacijsko opremo po tem, ko pooblaščena naprava opravi postopek povezave. Ker Bluetooth® za nadziranje, kdaj in kam se podatki lahko pošljejo, uporablja model strežnik/odjemalec, bo imel tahograf vlogo strežnika, zunanja naprava pa vlogo odjemalca.

Ko zunanja naprava prvič pride v območje dosega VU, se postopek povezave Bluetooth® lahko začne (glej tudi Prilogo 2). Napravi si izmenjata naslova, imeni, profila in skupni zaupni ključ, tako da se lahko v prihodnosti kadar koli povežeta. Ko je ta korak zaključen, VU zaupa zunanji napravi, ki lahko začne pošiljati zahtevke za prenos podatkov s tahografa. Dodatni šifrirni mehanizmi, ki presegajo Bluetooth®, niso predvideni. Če pa so potrebni dodatni varnostni mehanizmi, se določijo v skladu z Dodatkom 10 Skupni varnostni mehanizmi.

Splošna načela komunikacije so prikazana v naslednji sliki.



▼B

Za prenos podatkov iz VU na zunanjo napravo se uporablja profil SPP (profil serijskih vrat) Bluetooth®.

4.3. **Avtorizacija PIN**

Iz varnostnih razlogov VU uporablja avtorizacijski sistem s kodo PIN, ločen od povezave Bluetooth. Vsaka VU mora biti za namene avtentikacije zmožna ustvariti kode PIN iz vsaj 4 števk. Vsakič, ko se zunanja naprava poveže z VU, mora vnesti pravilno kodo PIN, preden lahko prejme katere koli podatke.

Po uspešnem vnosu PIN se naprava doda na beli seznam. Na belem seznamu je shranjenih vsaj 64 naprav, povezanih z določeno VU.

Če naprava trikrat zapored vnese napačno kodo PIN, se jo začasno doda na črni seznam. Dokler je na črnem seznamu, se vsak poskus povezave naprave zavrne. Če naprava nadalje še trikrat zapored vnese napačno kodo PIN, se trajanje blokade podaljšuje (glej preglednico 1). Po uspešnem vnosu kode PIN se trajanje blokade in število možnih poskusov ponastavi. Slika 1 v Prilogi 2 predstavlja diagram zaporedja pri poskusu validacije PIN.

Preglednica 1

Trajanje blokade glede na število zaporednih napačnih vnosov kode PIN

Število zaporednih napačnih vnosov	Trajanje blokade
3	30 sekund
6	5 minut
9	1 ura
12	24 ur
15	trajno

Če naprava petnajstkrat zapored vnese napačno kodo PIN (5 × 3), se jo trajno uvrsti na črni seznam enote ITS. Ta trajna blokada se odpravi samo z vnosom pravilne kode PUC.

Koda PUC, ki jo proizvajalec zagotovi skupaj z VU, je sestavljena iz 8 števk. Če naprava desetkrat zapored vnese napačno kodo PUC, se jo nepreklicno uvrsti na črni seznam enote ITS.

Proizvajalec lahko ponudi možnost za neposredno zamenjavo kode PIN v VU, kode PUC pa ne sme biti možno zamenjati. Za spremembo kode PIN, če je mogoča, je treba vnesti veljavno kodo PIN neposredno v VU.

Poleg tega je treba vse naprave z belega seznama hraniti, dokler jih uporabnik ročno ne odstrani (npr. prek vmesnika človek–stroj v VU ali z drugimi sredstvi). Tako se izgubljene ali ukradene enote ITS lahko odstrani z belega seznama. Poleg tega se vsaka enota ITS, ki za več kot 24 ur zapusti območje dosega povezave Bluetooth, samodejno črta z belega seznama VU in mora ob ponovni vzpostavitvi povezave še enkrat vnesti pravilno kodo PIN.

▼B

Format sporočil med vmesnikom VU in VU ni določen in je prepuščen odločitvi proizvajalca. Vendar mora proizvajalec zagotoviti, da se upošteva format sporočila med enoto ITS in vmesnikom VU (glej specifikacije ASN.1).

Pri vsakem zahtevku za podatke je treba pred kakršno koli obliko obdelave preveriti varnostne podatke pošiljatelja. Slika 2 v Prilogi 2 predstavlja diagram zaporedja za ta postopek. Vse naprave s črnega seznama se samodejno zavrnejo, naprave, ki niso niti na črnem niti na belem seznamu, pa prejmejo zahtevek za PIN, ki ga morajo izpolniti, preden pošljejo zahtevek za podatke.

4.4. **Format sporočil**

Vsa sporočila, ki si jih izmenjujeta enota ITS in vmesnik VU, so formatirana tako, da jih sestavljajo po trije deli: glava, ki jo sestavlja ciljni bajt (TGT), izvorni bajt (SRC) in bajt dolžine (LEN);

podatkovno polje, ki ga sestavljajo bajt identifikatorja storitve (SID) in spremenljivo število podatkovnih bajtov (največ 255);

bajt kontrolne vsote, ki je 1-bajtni rezultat ostanka vsote po modulu 256 vseh bajtov sporočila razen bajta CS samega.

Sporočilo je v formatu Big Endian.

Preglednica 2

Splošni format sporočil

Glava			Podatkovno polje					Kontrolna vsota
TGT	SRC	LEN	SID	TRTP	CC	CM	DATA	CS
3 bajti			Največ 255 bajtov					1 bajt

Glava

TGT in SRC: ID ciljne (TGT) in izvorne (SRC) naprave sporočila. Vmesnik VU ima privzeto ID ‘EE’. Te ID ni mogoče spremeniti. Enota ITS za prvo komunikacijsko sejo uporabi privzeto ID ‘A0’. Vmesnik VU nato enoti ITS dodeli in sporoči edinstveno ID za prihodnja sporočila med sejo.

Bajt LEN upošteva samo del ‘DATA’ podatkovnega polja (glej preglednico 2), prvi štirje bajti so implicirani.

Vmesnik VU potrdi avtentičnost pošiljatelja sporočila tako, da svoj seznam ID primerja s podatki Bluetooth in preveri, ali je enota ITS, ki je na seznamu pod določeno ID, trenutno v dosegu povezave Bluetooth.

Podatkovno polje

Poleg SID podatkovno polje vsebuje tudi druge parametre: parameter zahtevka za prenos (TRTP) in bajte števca.

▼B

Če podatki, ki jih je treba prenesti, presegajo razpoložljivi prostor v enem sporočilu, se razdelijo na več delnih sporočil. Vsako delno sporočilo ima enako glavo in SID, vendar za navedbo številke sporočila vsebuje 2-bajtni števec, tj. Counter Current (CC) in Counter Max (CM). Da se omogoči preverjanje napak in prekinitev prenosa, sprejemna naprava potrdi vsako delno sporočilo. Sprejemna naprava lahko delno sporočilo sprejme, zahteva njegov ponovni prenos, zahteva od naprave pošiljateljice, naj začne prenos znova, ali prekine prenos.

Če se CC in CM ne uporabljata, se jima dodeli vrednost 0×FF.

Naslednje sporočilo:

GLAVA	SID	TRTP	CC	CM	DATA	CS
3 bajti	Daljše od 255 bajtov					1 bajt

se prenese v tej obliki:

GLAVA	SID	TRTP	01	n	DATA	CS
3 bajti	255 bajtov					1 bajt

GLAVA	SID	TRTP	02	n	DATA	CS
3 bajti	255 bajtov					1 bajt

…

GLAVA	SID	TRTP	N	N	DATA	CS
3 bajti	Največ 255 bajtov					1 bajt

Preglednica 3 vsebuje sporočila, ki naj bi si jih VU in enota ITS lahko izmenjala Vsebina vsakega parametra je navedena v šestnajstiški vrednosti Zaradi jasnosti CC in CM nista vključena v tabelo, za popoln format glej zgoraj.

Preglednica 3

Podrobna vsebina sporočila

Sporočilo	Glava			DATA			Kontrolna vsota
	TGT	SRC	LEN	SID	TRTP	DATA	
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

Sporočilo	Glava			DATA			Kontrolna vsota
	TGT	SRC	LEN	SID	TRTP	DATA	
BanLiftingResult	*ITSID*	EE	01	06	FF	BOOLEAN (T/F)	
RequestRejected	*ITSID*	EE	08	07	FF	Time	
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	Data	
DataUnavailable							
Ni razpoložljivih podatkov	*ITSID*	EE	02	0A	TREP	10	
Ni izmenjave osebnih podatkov	*ITSID*	EE	02	0A	TREP	11	
NegativeAnswer							
Splošna zavrnitev	*ITSID*	EE	02	0B	SID Req	10	
Storitev ni podprta	*ITSID*	EE	02	0B	SID Req	11	
Podfunkcija ni podprta	*ITSID*	EE	02	0B	SID Req	12	
Nepravilna dolžina sporočila	*ITSID*	EE	02	0B	SID Req	13	
Nepravilni pogoji ali napaka v zaporedju zahtev-kov	*ITSID*	EE	02	0B	SID Req	22	
Zahtevek izven območja dosega	*ITSID*	EE	02	0B	SID Req	31	
Čakanje na odziv	*ITSID*	EE	02	0B	SID Req	78	
Neusklajenost ITSID	*ITSID*	EE	02	0B	SID Req	FC	
ITSID ni najdena	*ITSID*	EE	02	0B	SID Req	FB	

RequestPIN (SID 01)

To sporočilo izda vmesnik VU, če zahtevek za podatke pošlje enota ITS, ki ni niti na črnem niti na belem seznamu.

▼B

SendITSID (SID 02)

To sporočilo izda vmesnik VU, kadar koli zahtevek pošlje nova naprava. Ta naprava uporabi privzeto ID ‘A0’, preden ji je za komunikacijsko sejo dodeljena edinstvena ID.

SendPIN (SID 03)

To sporočilo izda enota ITS, da se jo doda na beli seznam vmesnika VU. Vsebina tega sporočila je koda, sestavljena iz štirih celih števil (INTEGER) med 0 in 9.

PairingResult (SID 04)

To sporočilo izda vmesnik VU, da enoto ITS obvesti, ali je bila poslana koda PIN pravilna. Vsebina tega sporočila je Boolova vrednost (BOOLEAN), ki je ‘True’, če je koda PIN pravilna, in ‘False’, če ni.

SendPUC (SID 05)

To sporočilo izda enota ITS, da se jo črta s črnega seznama vmesnika VU. Vsebina tega sporočila je koda, sestavljena iz osmih celih števil (INTEGER) med 0 in 9.

BanLiftingResult (SID 06)

To sporočilo izda vmesnik VU, da enoto ITS obvesti, ali je bila poslana koda PUC pravilna. Vsebina tega sporočila je Boolova vrednost (BOOLEAN), ki je ‘True’, če je koda PUC pravilna, in ‘False’, če ni.

RequestRejected (SID 07)

To sporočilo izda vmesnik VU kot odziv na katero koli sporočilo enote ITS s črnega seznama, razen ‘SendPUC’. V poročilu je navedeno, kako dolgo bo enota ITS še na črnem seznamu, in sicer v skladu s formatom zaporedja ‘Time’, kot je določeno v Prilogi 3.

RequestData (SID 08)

To sporočilo za dostop do podatkov izda enota ITS. Enobajtni parameter zahtevka za prenos (TRTP) označuje vrsto zahtevanih podatkov. Obstaja več vrst podatkov:

— standardTachData (TRTP 01): podatki iz tahografa, ki niso klasificirani kot osebni;

— personalTachData (TRTP 02): podatki iz tahografa, ki so klasificirani kot osebni;

— gnssData (TRTP 03): podatki GNSS, ki so vedno osebni;

— standardEventData (TRTP 04): zapisani podatki o dogodkih, ki niso klasificirani kot osebni;

— personalEventData (TRTP 05): zapisani podatki o dogodkih, ki so klasificirani kot osebni;

— standardFaultData (TRTP 06): zapisani podatki o napakah, ki niso klasificirani kot osebni;

— manufacturerData (TRTP 07): podatki, ki jih da na voljo proizvajalec.

▼B

Za več informacij o vsebini vsakega podatkovnega tipa glej Prilogo 3.

Za več informacij o formatu in vsebini podatkov GNSS glej Dodatek 12.

Za več informacij o kodah podatkov o dogodkih in napakah glej Prilogo IB in IC.

ResquestAccepted (SID 09)

To sporočilo izda vmesnik VU, če je bilo sporočilo 'RequestData' enote ITS sprejeto. To sporočilo vsebuje enobajtni TREP, ki je enak bajtu TRTP povezanega sporočila RequestData, in vse podatke zahtevanega tipa.

DataUnavailable (SID 0A)

To sporočilo izda vmesnik VU, če iz katerega koli razloga zahtevani podatki niso na voljo za posredovanje enoti ITS z belega seznama. Sporočilo vsebuje enobajtni TREP, ki je enak TRTP zahtevanih podatkov, in enobitno kodo napake, določeno v preglednici 3. Možne so naslednje kode:

— Ni razpoložljivih podatkov (10): vmesnik VU iz neopredeljenih razlogov nima dostopa do podatkov VU;

— Ni izmenjave osebnih podatkov (11): enota ITS poskuša pridobiti osebne podatke, ki se jih ne izmenjuje.

NegativeAnswer (SID 0B)

Ta sporočila izda vmesnik VU, če zahtevka ni mogoče dokončati iz katerega koli razloga razen nerazpoložljivosti podatkov. Ta sporočila so običajno, vendar ne vedno, posledica slabega formata zahtevka (dolžina, SID, ITSID...). TRTP v podatkovnem polju vsebuje SID zahtevka. Podatkovno polje vsebuje kodo, ki označuje vzrok za negativni odgovor. Možne so naslednje kode:

— Splošna zavrnitev (koda: 10)

— Operacije ni mogoče izvesti iz razloga, ki ni naveden spodaj ali v oddelku (vnesti številko oddelka *DataUnavailable*).

— Storitev ni podprta (koda: 11)

— SID zahtevka ni mogoče tolmačiti.

— Podfunkcija ni podprta (koda: 12)

— TRTP zahtevka ni mogoče tolmačiti. Lahko ga na primer ni ali pa je zunaj sprejemljivih vrednosti.

— Nepravilna dolžina sporočila (koda: 13)

— Dolžina prejetega sporočila ni pravilna (neujemanje med bajtom LEN in dejansko dolžino sporočila).

— Nepravilni pogoji ali napaka v zaporedju zahtevkov (koda: 22)

— Zahtevana storitev ni aktivna ali pa ni pravilno zaporedje sporočil zahtevkov

— Zahtevek izven območja dosega (koda: 33)

▼B

— Parameter zapisa (podatkovno polje) v zahtevku ni veljaven

— Čakanje na odziv (koda: 78)

— Zahtevane operacije ni mogoče zaključiti pravočasno in VU ni pripravljena za sprejem novega zahtevka.

— Neusklajenost ITSID (koda: FB)

— *ITSID* SRC se po primerjavi s podatki Bluetooth ne ujema z zadevno napravo.

— ITSID ni najdena (koda: FC)

— *ITSID* SRCS se ne ujema z nobeno napravo.

Vrstice 1 do 72 (**FormatMessageModule**) kode ASN.1 v Prilogi 3 določajo format sporočil, kot je opisano v preglednici 3. Več podrobnosti o vsebini sporočil je navedenih spodaj.

4.5. **Privolitev voznika**

Vsi razpoložljivi podatki so klasificirani kot standardni ali osebni. Osebni podatki so dostopni le, če je voznik privolil, da se njegovi osebni podatki iz tahografa prenesejo iz omrežja vozila za uporabo v aplikacijah tretjih strani.

Voznik da svojo privolitev, ko je ob prvi vstavitvi vozniške kartice ali kartice servisne delavnice, ki enoti v vozilu še ni poznana, vprašan, ali privoljuje v iznos osebnih podatkov, povezanih s tahografom, preko neobveznega vmesnika z ITS. (glej tudi Prilogo I C, odstavek 3.6.2).

Status privolitve (aktivirana/deaktivirana) je prikazan v pomnilniku tahografa.

Če je voznikov več, se z vmesnikom z ITS delijo samo osebni podatkov tistih voznikov, ki so dali svojo privolitev. Če sta na primer v vozilu dva voznika in je samo prvi privolil, da se njegovi osebni podatki posredujejo, se osebni podatki drugega voznika ne posredujejo.

4.6. **Pridobivanje standardnih podatkov**

Slika 3 v Prilogi 2 predstavlja diagrame zaporedja veljavnega zahtevka enote ITS za dostop do standardnih podatkov. Enota ITS je na belem seznamu in ne zahteva osebnih podatkov, dodatno preverjanje ni potrebno. V diagramih je predpostavljeno, da je bil pravilni postopek iz slike 2 v Prilogi 2 že upoštevan. Ustrezajo sivemu polju v sliki 2 *REQUEST TREATMENT*.

Med razpoložljivimi podatki naslednji veljajo za standardne:

— standardTachData (TRTP 01)

— StandardEventData (TRTP 04)

— standardFaultData (TRTP 06)

4.7. **Pridobivanje osebnih podatkov**

Slika 4 v Prilogi 2 predstavlja diagram zaporedja za obdelavo zahtevkov za osebne podatke. Kot je bilo že navedeno, vmesnik VU osebne podatke pošlje le, če je voznik dal svojo izrecno privolitev (glej tudi 4.5). V nasprotnem je treba zahtevek avtomatsko zavrniti.

▼B

Med razpoložljivimi podatki naslednji veljajo za osebne:

— personalTachData (TRTP 02)

— gnssData (TRTP 03)

— personalEventData (TRTP 05)

— manufacturerData (TRTP 07)

4.8. **Pridobivanje podatkov o dogodkih in napakah**

Enote ITS morajo biti zmožne zahtevati podatke o dogodkih, ki vsebujejo seznam vseh nepredvidenih dogodkov. Ti podatki se lahko štejejo za standardne ali osebne (glej Prilogo 3). Vsebina vsakega dogodka je v skladu z dokumentacijo iz Priloge 1 tega dodatka.

▼B

PRILOGA 1

SEZNAM RAZPOLOŽLJIVIH PODATKOV PREK VMESNIKA Z ITS

▼C2

Podatki	Vir	Klasifikacija podatkov (Osebni/Niso osebni)
VehicleIdentificationNumber	Enota v vozilu	**Niso osebni**
CalibrationDate	Enota v vozilu	**Niso osebni**
TachographVehicleSpeed speed instant t	Enota v vozilu	Osebni
Driver1WorkingState Selector driver	Enota v vozilu	Osebni
Driver2WorkingState	Enota v vozilu	Osebni
DriveRecognize Speed Threshold detected	Enota v vozilu	**Niso osebni**
Driver1TimeRelatedStates Weekly day time	Vozniška kartica	Osebni
Driver2TimeRelatedStates	Vozniška kartica	Osebni
DriverCardDriver1	Enota v vozilu	**Niso osebni**
DriverCardDriver2	Enota v vozilu	**Niso osebni**
OverSpeed	Enota v vozilu	Osebni
TimeDate	Enota v vozilu	**Niso osebni**
HighResolutionTotalVehicleDistance	Enota v vozilu	**Niso osebni**
ServiceComponentIdentification	Enota v vozilu	**Niso osebni**
ServiceDelayCalendarTimeBased	Enota v vozilu	**Niso osebni**
Driver1Identification	Vozniška kartica	Osebni
Driver2Identification	Vozniška kartica	Osebni
NextCalibrationDate	Enota v vozilu	**Niso osebni**
Driver1ContinuousDrivingTime	Vozniška kartica	Osebni
Driver2ContinuousDrivingTime	Vozniška kartica	Osebni
Driver1CumulativeBreakTime	Vozniška kartica	Osebni
Driver2CumulativeBreakTime	Vozniška kartica	Osebni
Driver1CurrentDurationOfSelectedActivity	Vozniška kartica	Osebni
Driver2CurrentDurationOfSelectedActivity	Vozniška kartica	Osebni
SpeedAuthorised	Enota v vozilu	**Niso osebni**
TachographCardSlot1	Vozniška kartica	**Niso osebni**
TachographCardSlot2	Vozniška kartica	**Niso osebni**
Driver1Name	Vozniška kartica	Osebni
Driver2Name	Vozniška kartica	Osebni

▼C2

Podatki	Vir	Klasifikacija podatkov (Osebni/Niso osebni)
OutOfScopeCondition	Enota v vozilu	**Niso osebni**
ModeOfOperation	Enota v vozilu	**Niso osebni**
Driver1CumulatedDrivingTimePreviousAndCurrentWeek	Vozniška kartica	Osebni
Driver2CumulatedDrivingTimePreviousAndCurrentWeek	Vozniška kartica	Osebni
EngineSpeed	Enota v vozilu	Osebni
RegisteringMemberState	Enota v vozilu	**Niso osebni**
VehicleRegistrationNumber	Enota v vozilu	**Niso osebni**
Driver1EndOfLastDailyRestPeriod	Vozniška kartica	Osebni
Driver2EndOfLastDailyRestPeriod	Vozniška kartica	Osebni
Driver1EndOfLastWeeklyRestPeriod	Vozniška kartica	Osebni
Driver2EndOfLastWeeklyRestPeriod	Vozniška kartica	Osebni
Driver1EndOfSecondLastWeeklyRestPeriod	Vozniška kartica	Osebni
Driver2EndOfSecondLastWeeklyRestPeriod	Vozniška kartica	Osebni
Driver1CurrentDailyDrivingTime	Vozniška kartica	Osebni
Driver2CurrentDailyDrivingTime	Vozniška kartica	Osebni
Driver1CurrentWeeklyDrivingTime	Vozniška kartica	Osebni
Driver2CurrentWeeklyDrivingTime	Vozniška kartica	Osebni
Driver1TimeLeftUntilNewDailyRestPeriod	Vozniška kartica	Osebni
Driver2TimeLeftUntilNewDailyRestPeriod	Vozniška kartica	Osebni
Driver1CardExpiryDate	Vozniška kartica	Osebni
Driver2CardExpiryDate	Vozniška kartica	Osebni
Driver1CardNextMandatoryDownloadDate	Vozniška kartica	Osebni
Driver2CardNextMandatoryDownloadDate	Vozniška kartica	Osebni
TachographNextMandatoryDownloadDate	Enota v vozilu	**Niso osebni**
Driver1TimeLeftUntilNewWeeklyRestPeriod	Vozniška kartica	Osebni
Driver2TimeLeftUntilNewWeeklyRestPeriod	Vozniška kartica	Osebni
Driver1NumberOfTimes9hDailyDrivingTimesExceeded	Vozniška kartica	Osebni
Driver2NumberOfTimes9hDailyDrivingTimesExceeced	Vozniška kartica	Osebni

▼C2

Podatki	Vir	Klasifikacija podatkov (Osebni/Niso osebni)
Driver1CumulativeUninterruptedRestTime	Vozniška kartica	Osebni
Driver2CumulativeUninterruptedRestTime	Vozniška kartica	Osebni
Driver1MinimumDailyRest	Vozniška kartica	Osebni
Driver2MinimumDailyRest	Vozniška kartica	Osebni
Driver1MinimumWeeklyRest	Vozniška kartica	Osebni
Driver2MinimumWeeklyRest	Vozniška kartica	Osebni
Driver1MaximumDailyPeriod	Vozniška kartica	Osebni
Driver2MaximumDailyPeriod	Vozniška kartica	Osebni
Driver1MaximumDailyDrivingTime	Vozniška kartica	Osebni
Driver2MaximumDailyDrivingTime	Vozniška kartica	Osebni
Driver1NumberOfUsedReducedDailyRestPeriods	Vozniška kartica	Osebni
Driver2NumberOfUsedReducedDailyRestPeriods	Vozniška kartica	Osebni
Driver1RemainingCurrentDrivingTime	Vozniška kartica	Osebni
Driver2RemainingCurrentDrivingTime	Vozniška kartica	Osebni
GNSS position	Enota v vozilu	Osebni

▼B

(2) STALNI PODATKI GNSS DATA, NA VOLJO PO PRIVOLITVI VOZNIKA

Glej Dodatek 12 – GNSS

(3) KODE DOGODKOV, NA VOLJO BREZ PRIVOLITVE VOZNIKA

Dogodek	Pravila shranjevanja	Podatki, ki se zapišejo za vsak dogodek
Vstavitev neveljavne kartice	— 10 najnovejših dogodkov	— datum in čas dogodka — vrsta, številka, država izdajateljica in generacija kartice, s katero je dogodek nastopil — število podobnih dogodkov v danem dnevu
Navzkrižje med karticami	— 10 najnovejših dogodkov	— datum in čas začetka dogodka — datum in čas konca dogodka — vrsta, številka, država izdajateljica in generacija kartic, s katerima je navzkrižje nastopilo
Zadnja seja s kartico nepravilno zaključena	— 10 najnovejših dogodkov	— datum in čas vstavitve kartice — vrsta, številka, država izdajateljica in generacija kartic — podatki zadnje seje, prebrani s kartice: — datum in čas vstavitve kartice — registrska številka vozila, država članica registracije in generacija enote v vozilu

▼B

Dogodek	Pravila shranjevanja	Podatki, ki se zapišejo za vsak dogodek
Izpad napajanja (2)	— najdaljši dogodek za vsakega od 10 zadnjih dni nastopov dogodkov — 5 najdaljših dogodkov v zadnjih 365 dneh	— datum in čas začetka dogodka — datum in čas konca dogodka — vrsta, številka, država izdajateljica in generacija katere koli kartice, vstavljene ob začetku in/ali koncu dogodka — število podobnih dogodkov v danem dnevu
Napaka pri komuniciranju z opremo za komunikacijo na daljavo	— najdaljši dogodek za vsakega od 10 zadnjih dni nastopov dogodkov — 5 najdaljših dogodkov v zadnjih 365 dneh	— datum in čas začetka dogodka — datum in čas konca dogodka — vrsta, številka, država izdajateljica in generacija katere koli kartice, vstavljene ob začetku in/ali koncu dogodka — število podobnih dogodkov v danem dnevu
Ni informacij o položaju s strani GNSS sprejemnika	— najdaljši dogodek za vsakega od 10 zadnjih dni nastopov dogodkov — 5 najdaljših dogodkov v zadnjih 365 dneh	— datum in čas začetka dogodka — datum in čas konca dogodka — vrsta, številka, država izdajateljica in generacija katere koli kartice, vstavljene ob začetku in/ali koncu dogodka — število podobnih dogodkov v danem dnevu
Napaka v podatkih o gibanju	— najdaljši dogodek za vsakega od 10 zadnjih dni nastopov dogodkov — 5 najdaljših dogodkov v zadnjih 365 dneh	— datum in čas začetka dogodka — datum in čas konca dogodka — vrsta, številka, država izdajateljica in generacija katere koli kartice, vstavljene ob začetku in/ali koncu dogodka — število podobnih dogodkov v danem dnevu
Navzkrižje v gibanju vozila	— najdaljši dogodek za vsakega od 10 zadnjih dni nastopov dogodkov — 5 najdaljših dogodkov v zadnjih 365 dneh	— datum in čas začetka dogodka — datum in čas konca dogodka — vrsta, številka, država izdajateljica in generacija katere koli kartice, vstavljene ob začetku in/ali koncu dogodka — število podobnih dogodkov v danem dnevu
Poskus kršenja varnosti	10 najnovejših dogodkov za vsako vrsto dogodka	— datum in čas začetka dogodka — datum in čas konca dogodka (če je ustrezno) — vrsta, številka, država izdajateljica in generacija katere koli kartice, vstavljene ob začetku in/ali koncu dogodka — vrsta dogodka

▼B

Dogodek	Pravila shranjevanja	Podatki, ki se zapišejo za vsak dogodek
Časovno navzkrižje	— najdaljši dogodek za vsakega od 10 zadnjih dni nastopov dogodkov — 5 najdaljših dogodkov v zadnjih 365 dneh	— datum in čas zapisovalne naprave — datum in čas GNSS — vrsta, številka, država izdajateljica in generacija katere koli kartice, vstavljene ob začetku in/ali koncu dogodka — število podobnih dogodkov v danem dnevu

(4) KODE DOGODKOV, NA VOLJO S PRIVOLITVIJO VOZNIKA

Dogodek	Pravila shranjevanja	Podatki, ki se zapišejo za vsak dogodek
Vožnja brez ustrezne kartice	— najdaljši dogodek za vsakega od 10 zadnjih dni nastopov dogodkov — 5 najdaljših dogodkov v zadnjih 365 dneh	— datum in čas začetka dogodka — datum in čas konca dogodka — vrsta, številka, država izdajateljica in generacija katere koli kartice, vstavljene ob začetku in/ali koncu dogodka — število podobnih dogodkov v danem dnevu
Vstavitev kartice med vožnjo	— zadnji dogodek za vsakega od 10 zadnjih dni nastopov dogodkov	— datum in čas dogodka — vrsta, številka, država izdajateljica in generacija kartic — število podobnih dogodkov v danem dnevu
Prekoračitev hitrosti (1)	— najresnejši dogodek za vsakega od 10 zadnjih dni nastopov dogodkov (tj. tisti z najvišjo povprečno hitrostjo) — 5 najresnejših dogodkov v zadnjih 365 dneh — prvi dogodek, ki je nastopil po zadnji kalibraciji	— datum in čas začetka dogodka — datum in čas konca dogodka — najvišja hitrost, izmerjena med dogodkom — aritmetična sredina hitrosti, izmerjenih med dogodkom — vrsta, številka, država izdajateljica in generacija vozniške kartice (če je ustrezno) — število podobnih dogodkov v danem dnevu

(5) KODE PODATKOV O NAPAKAH, NA VOLJO BREZ PRIVOLITVE VOZNIKA

Napaka	Pravila shranjevanja	Podatki, ki se zapišejo za vsako napako
Napaka na kartici	— 10 najnovejših napak na vozniški kartici	— datum in čas začetka napake — datum in čas konca napake — vrsta, številka, država izdajateljica in generacija kartic
Napaka na zapisovalni napravi	— 10 najnovejših napak za vsako vrsto napake — prva napaka po zadnji kalibraciji	— datum in čas začetka napake — datum in čas konca napake — vrsta napake — vrsta, številka, država izdajateljica in generacija katere koli kartice, vstavljene ob začetku in/ali koncu napake

▼B

Ta napaka se sproži, kadar zapisovalna naprava ni v kalibracijskem načinu, ob kateri koli od naslednjih napak:

— notranja napaka VU,

— napaka na tiskalniku,

— napaka na prikazovalniku,

— napaka pri prenosu podatkov,

— napaka na tipalu,

— napaka na GNSS sprejemniku ali zunanji GNSS opremi,

— napaka na opremi za komunikacijo na daljavo.

(6) POSEBNI DOGODKI IN NAPAKE PROIZVAJALCA, BREZ PRIVOLITVE VOZNIKA

Dogodek ali napaka	Pravila shranjevanja	Podatki, ki se zapišejo za vsak dogodek
Določi proizvajalec	Določi proizvajalec	Določi proizvajalec

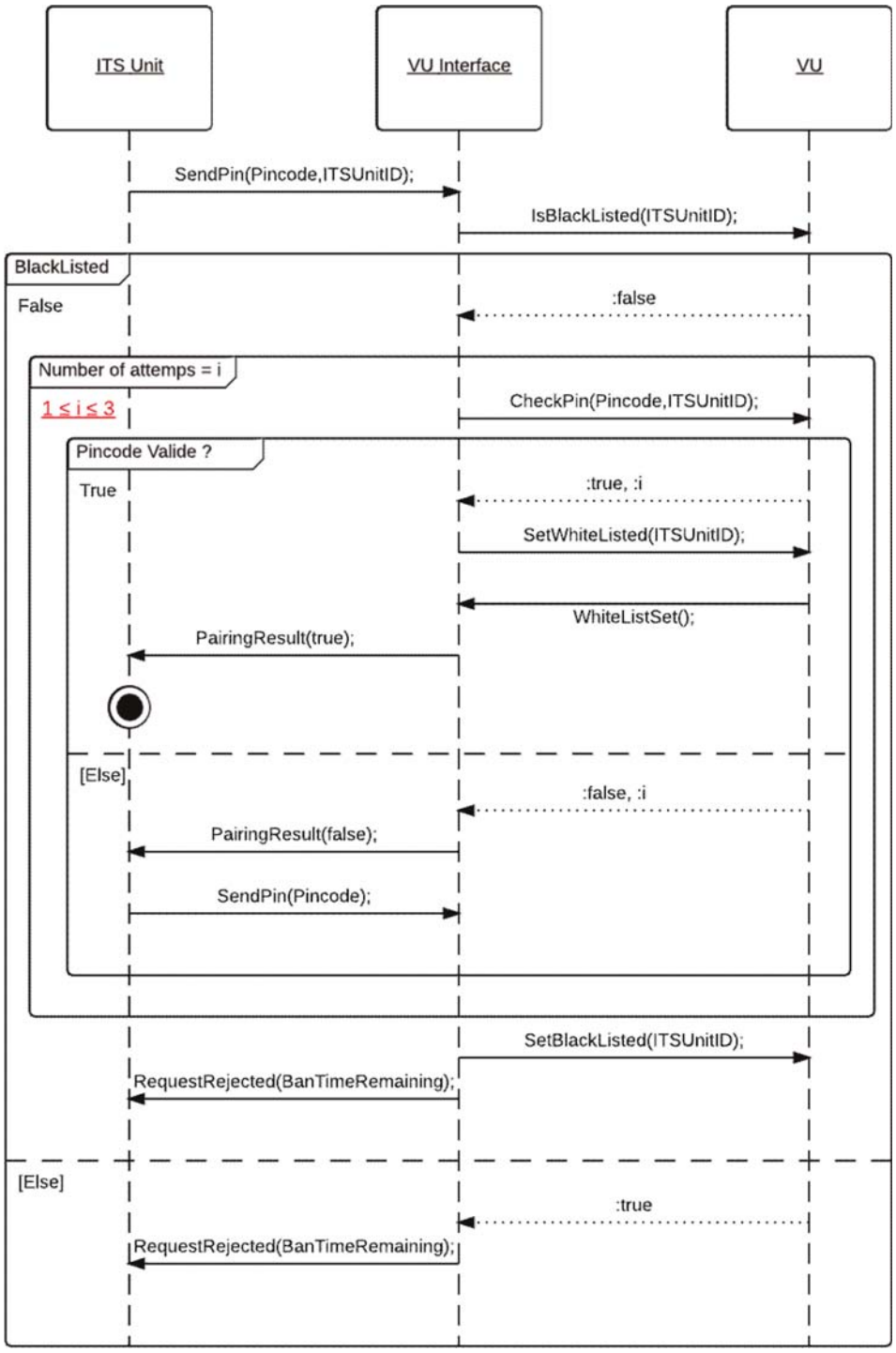
▼B

PRILOGA 2

DIAGRAMI ZAPOREDJA IZMENJAVE SPOROČIL Z ENOTO ITS

Slika 1

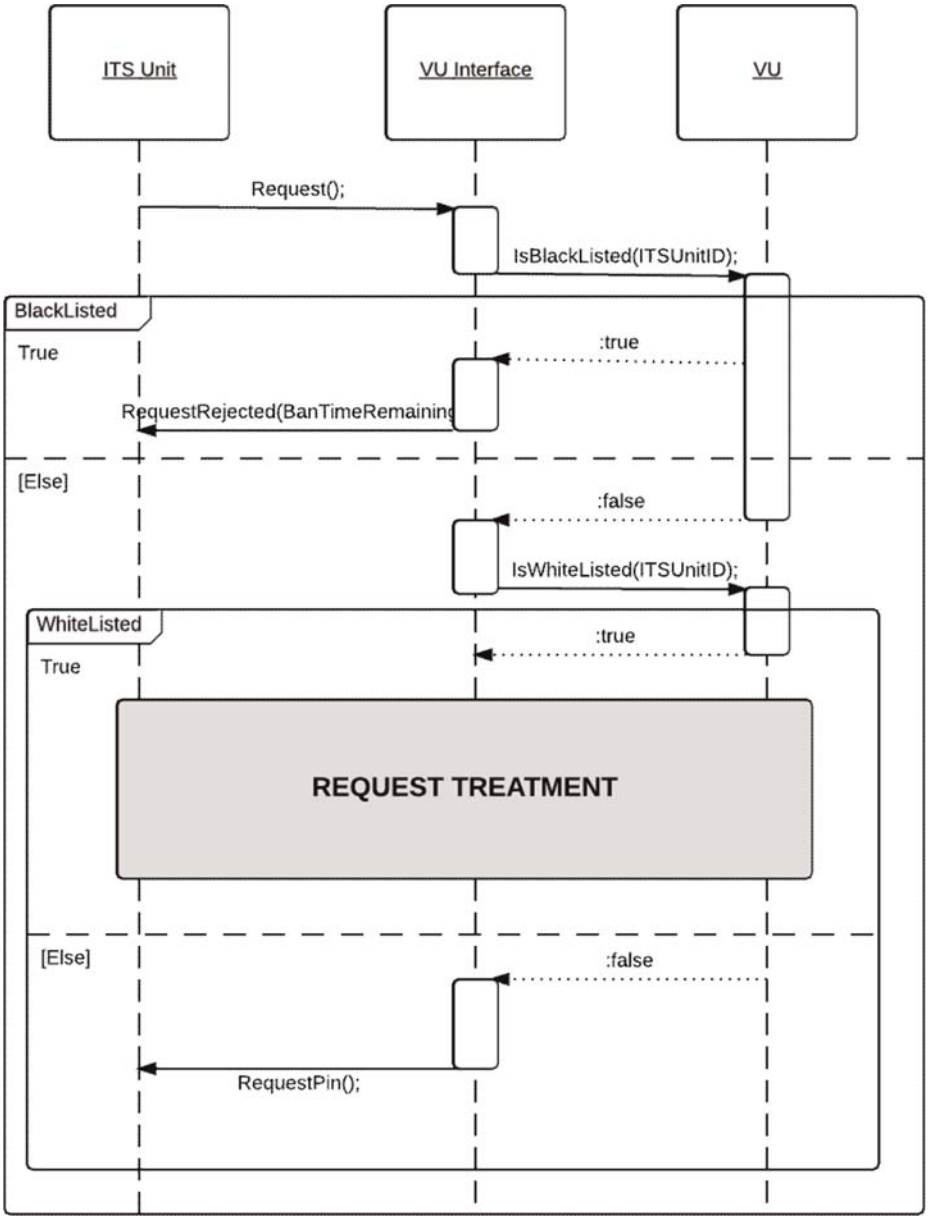
Diagram zaporedja za poskus validacije PIN



▼B

Slika 2

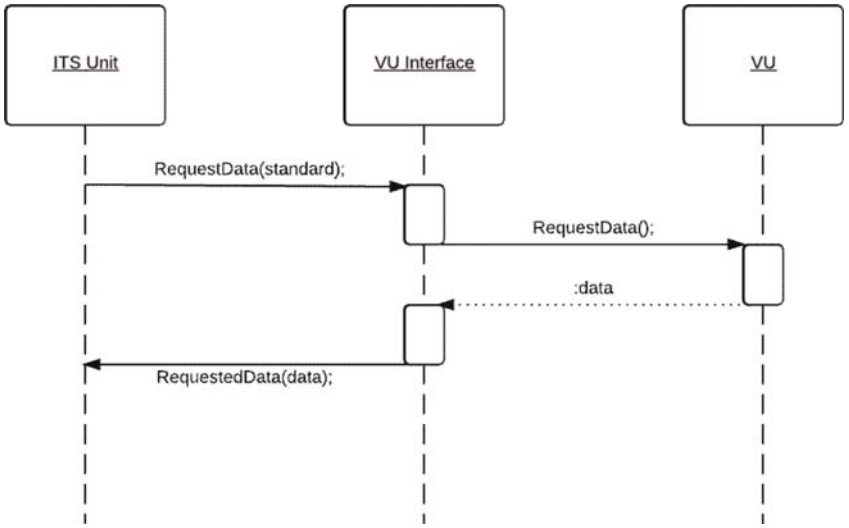
Diagram zaporedja za preverjanje pooblastila enote ITS



▼B

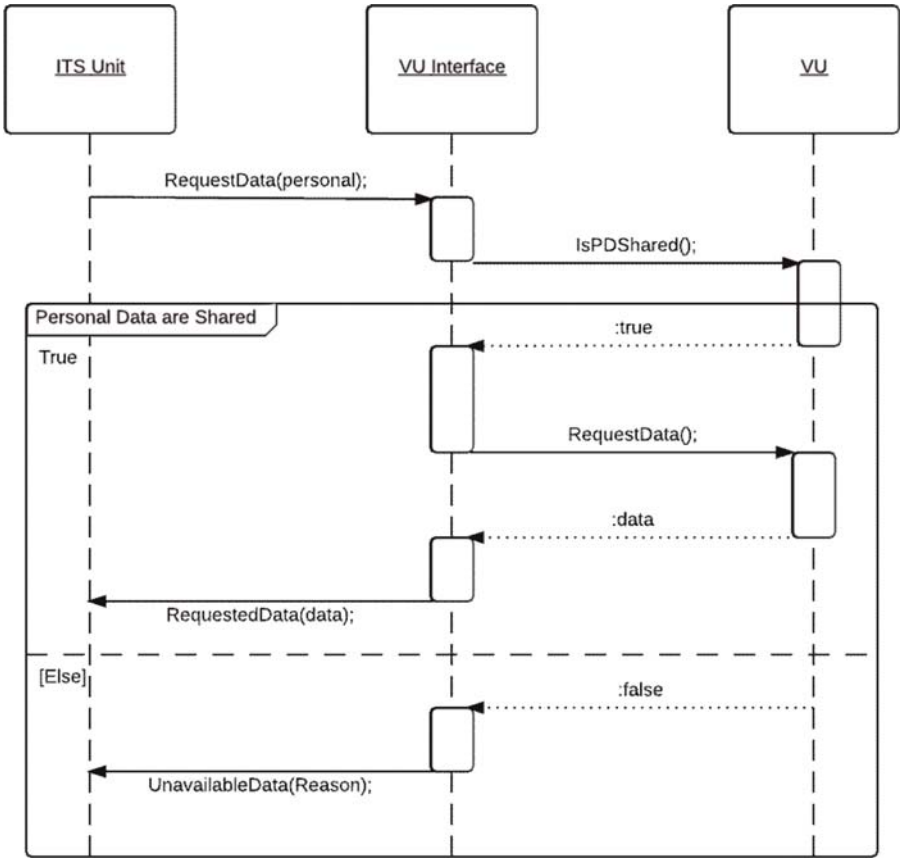
Slika 3

Diagram zaporedja za obdelavo zahtevka za podatke, ki niso klasificirani kot osebni podatki (po dostopu s pravilnim PIN)



Slika 4

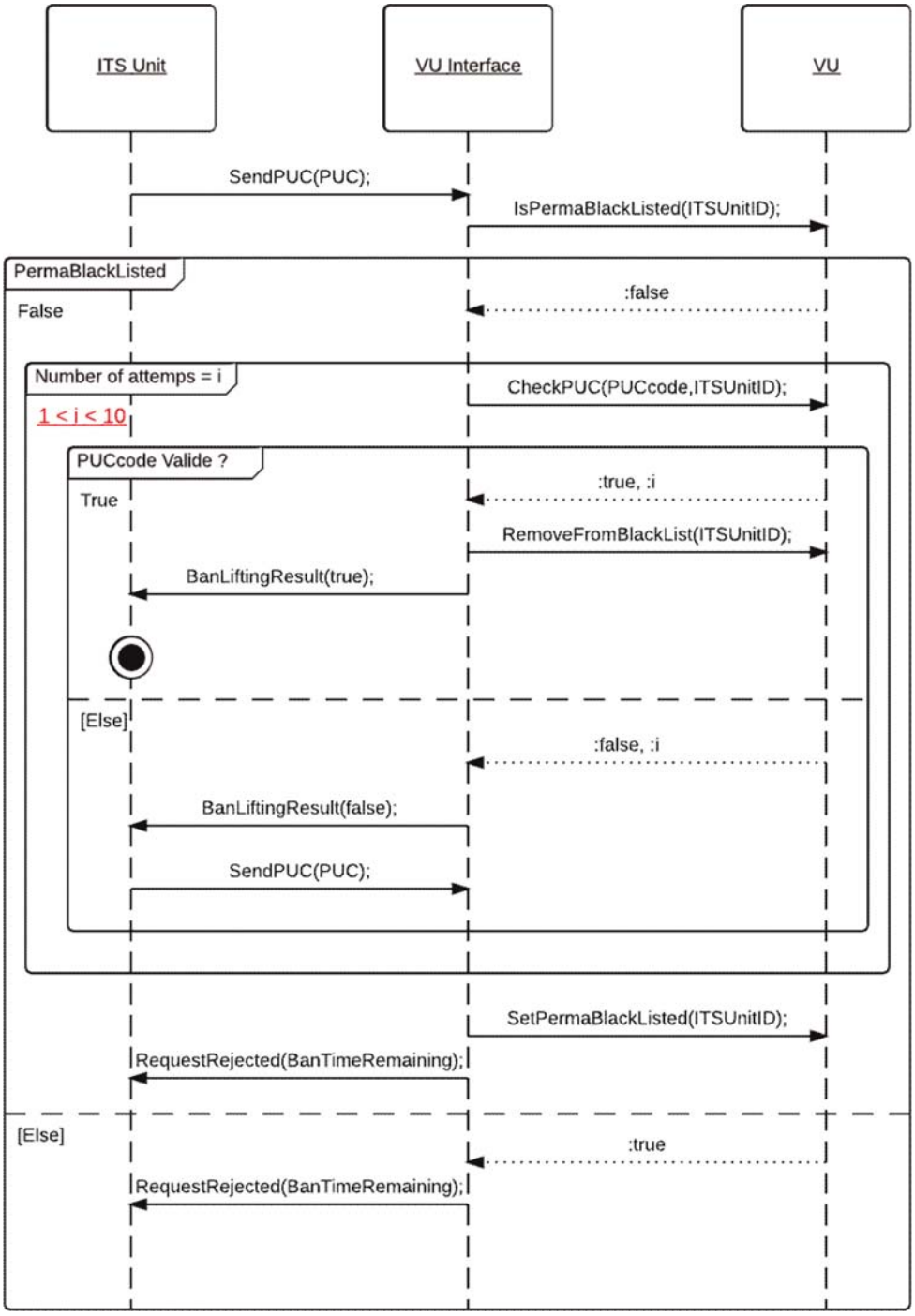
Diagram zaporedja za obdelavo zahtevka za podatke, ki so klasificirani kot osebni podatki (po dostopu s pravilnim PIN)



▼B

Slika 5

Diagram zaporedja za poskus validacije PUC



▼B

PRILOGA 3

SPECIFIKACIJE 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

```
PINPUCDataFieldsModule DEFINITIONS AUTOMATIC TAGS ::= BEGIN
EXPORTS SendPIN, SendPUC, PairingResult, RequestPIN, RequestRejected,
BanLiftingResult;
IMPORTS ;

      ----------
      ---Utils--
      ----------

      PUC ::= SEQUENCE (SIZE(8)) OF
      INTEGER (SIZE(0..9))

      PIN ::=      SEQUENCE (SIZE(4)) OF
            INTEGER (SIZE(0..9))

      -------------------------
      --Messages From ITS Unit--
      -------------------------

      SendPIN {PIN:pin} ::= SEQUENCE {
            sid BIT STRING ('03'H),
            pin PIN (pin)
      }

      SendPUC {PUC:puc} ::= SEQUENCE {
            sid BIT STRING ('05'H),
            puc PUC (puc)
      }
      --------------------
      --Messages From VU--
      --------------------

      PairingResult ::= SEQUENCE{
            sid BIT STRING ('04'H),
            result BOOLEAN
      }

      RequestPIN {MType:receivedRequest}::= SEQUENCE{
            sid BIT STRING ('01'H)
      }

      RequestRejected ::= SEQUENCE{
            sid BIT STRING ('07'H),
            banTimeRemaining GeneralizedTime, --PermaBan == 1k years-- }

      BanLiftingResult ::= SEQUENCE{
            sid BIT STRING ('06'H),
            result BOOLEAN
      }
END
```

▼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

Dodatek 14

FUNKCIJA KOMUNIKACIJE NA DALJAVO

KAZALO

1 UVOD

2 PODROČJE UPORABE

3 KRATICE, OPREDELITVE IN OZNAKE

4 SCENARIJI DELOVANJA

4.1 Pregled

4.1.1 Predpogoji za prenos podatkov preko vmesnika 5,8 GHz DSRC

4.1.2 Profil 1a: z bralnikom komunikacije za zgodnje odkrivanje na daljavo, namerjenim z roko ali začasno nameščenim na nosilcu ob cesti

4.1.3 Profil 1b: z bralnikom komunikacije za zgodnje odkrivanje na daljavo (REDCR), nameščenim na vozilu in usmerjenim v določeno smer

4.2 Varnost/celovitost

5 ZASNOVA KOMUNIKACIJE NA DALJAVO IN PROTOKOLI ZANJO

5.1 Zasnova

5.2 Postopek dela

5.2.1 Operacije

5.2.2 Razlaga podatkov, prejetih preko komunikacije DSRC

5.3 Parametri fizičnega vmesnika DSRC za komunikacijo na daljavo

5.3.1 Omejitve glede kraja namestitve

5.3.2 Parametri za navzdolnjo in navzgornjo povezavo

5.3.3 Zasnova antene

5.4 Zahteve protokola DSRC za RTM

5.4.1 Pregled

5.4.2 Ukazi

5.4.3 Zaporedje ukazov pri poizvedbi

5.4.4 Strukture podatkov

5.4.5 Elementi RtmData, izvedena dejanja in opredelitve

5.4.6 Mehanizem za prenos podatkov

5.4.7 Podroben opis transakcije DSRC

5.4.8 Opis preskusne transakcije DSRC

5.5 Podpora za Direktivo 2015/71/EU

5.5.1 Pregled

5.5.2 Ukazi

▼B

5.5.3 Zaporedje ukazov pri poizvedbi

5.5.4 Strukture podatkov

5.5.5 Modul ASN.1 za transakcijo OWS DSRC

5.5.6 Elementi OwsData, izvedena dejanja in opredelitve

5.5.7 Mehanizem za prenos podatkov

5.6 Prenos podatkov med DSRC-VU in VU

5.6.1 Fizična povezava in vmesniki

5.6.2 Protokol aplikacije

5.7 Obravnava napak

5.7.1 Beleženje in sporočanje podatkov v DSRC-VU

5.7.2 Napake v brezžični komunikaciji

6 NAROČANJE IN REDNI KONTROLNI PREGLEDI ZA FUNKCIJO KOMUNIKACIJE NA DALJAVO

6.1 Splošno

6.2 ECHO

6.3 Preskus za preveritev vsebine zaščitenih podatkov

1 UVOD

Ta dodatek določa zasnovo in postopke za izvedbo funkcije komunikacije na daljavo (v nadaljnjem besedilu: komunikacija), kot se zahteva v členu 9 Uredbe (EU) št. 165/2014 (v nadaljnjem besedilu: Uredba).

DSC_1 Uredba (EU) št.. 165/2014 določa, da mora biti tahograf opremljen s funkcijo komunikacije na daljavo, s pomočjo katere lahko predstavniki pristojnih nadzornih organov berejo podatke s tahografov mimo vozečih vozil z uporabo opreme za poizvedbe na daljavo („bralnik komunikacije za zgodnje odkrivanje na daljavo“, REDCR), konkretno opreme za poizvedbo po brezžični povezavi z uporabo vmesnikov posebne komunikacije kratkega dosega CEN 5,8 GHz (Dedicated Short Range Communication, DSRC).

Pomembno je razumeti, da je ta funkcija namenjena samo za predhodno filtriranje, s katerim se izberejo vozila za natančnejši kontrolni pregled, in ne nadomešča formalnega postopka kontrolnega pregleda, kot je opredeljen v določbah Uredbe (EU) št. 165/2014. Glej uvodno izjavo 9 v preambuli te uredbe, v kateri je navedeno, da komunikacija na daljavo med tahografom in nadzornimi organi zaradi cestnega preverjanja olajša usmerjen cestni nadzor.

DSC_2 *Podatki* se izmenjujejo z uporabo *komunikacije*, ki pomeni brezžično izmenjavo podatkov z uporabo brezžičnih komunikacij 5,8 GHz DSRC, ki so skladni s to prilogo in preskušeni glede na ustrezne parametre standarda EN 300 674-1 {Elektromagnetna združljivost in zadeve v zvezi z radijskim spektrom (ERM)); Cestna transportna in prometna telematika (RTTT); Oddajniška oprema za enouporabniško (osebno) komunikacijo

▼B

kratkega dosega (DSRC) (s prenosnima hitrostma 500 kbit/s / 250 kbit/s), ki deluje v pasu 5,8 GHz, namenjenem industrijski, znanstveni in medicinski uporabi; del 1: Splošne značilnosti in metode preskušanja za obcestne enote (RSU) in enote, nameščene v vozilu (OBU)}.

DSC_3 *Komunikacija* se vzpostavi s komunikacijsko opremo, in sicer samo, če tako zahteva oprema pristojnega nadzornega organa z uporabo skladnih radiokomunikacijskih sredstev (*bralnik sporočil o zgodnjem odkrivanju na daljavo (REDCR)*).

DSC_4 *Podatki* morajo biti zaščiteni, da se zagotovi celovitost.

DSC_5 Dostop do sporočenih *podatkov* imajo samo pristojni nadzorni organi, ki so pooblaščeni za preverjanje kršitev Uredbe (ES) št. 561/2006 in Uredbe (EU) št. 165/2014 ter servisne delavnice, kolikor je potrebno za preverjanje pravilnega delovanja tahografa.

DSC_6 Izmenjava *podatkov* med *komunikacijo* je omejena na podatke, potrebne za usmerjen cestni nadzor vozil z morebitnim prirejenim ali zlorabljenim tahografom.

DSC_7 Celovitost in varnost podatkov sta zagotovljeni tako, da so *podatki* zavarovani v enoti vozila in da se preko sredstva za komunikacijo na daljavo 5,8 GHz DSRC posredujejo samo zavarovani koristni podatki ter podatki, povezani z varnostjo (glej 5.4.4), kar pomeni, da lahko podatke, posredovane preko *komunikacije*, razumejo in njihovo pristnost preverijo samo pooblaščene osebe pristojnih nadzornih organov. Glej Dodatek 11, „Skupni varnostni mehanizmi“.

DSC_8 *Podatki* vsebujejo časovni žig s časom njihove zadnje posodobitve.

DSC_9 Vsebino zaščitnih podatkov bodo poznali samo pristojni organi, ki bodo tudi lahko edini upravljali z njimi, ter osebe, ki jim bodo posredovale te informacije, zanjo pa ne veljajo določbe za *komunikacijo*, za katero se uporablja ta priloga, razen da *komunikacija* omogoča prenos varnostnih podatkov z vsakim paketom koristnih podatkov.

DSC_10 Isto arhitekturo in opremo mora biti možno uporabljati za pridobivanje drugih podatkovnih konceptov (kot je tehtanje v vozilu) z uporabo arhitekture, opisane tukaj.

DSC_11 Pojasnilo: v skladu z določbami Uredbe (EU) št. 165/2014 (člen 7) se podatki o vozniku ne bodo prenašali preko *komunikacije*.

2 PODROČJE UPORABE

Področje tega dodatka je določitev načina, na katerega predstavniki pristojnih nadzornih organov uporabljajo posebno brezžično komunikacijo 5,8 GHz DSRC za pridobivanje podatkov (*podatki*) na daljavo od

▼B

ciljnega vozila, s katerimi se ugotovi, da ciljno vozilo morebiti krši Uredbo št. 165/2014 in bi ga bilo treba ustaviti za nadaljnje preverjanje.

Uredba (EU) št. 165/2014 določa, da pridejo v poštev za zbiranje samo podatki, s katerimi je mogoče ugotoviti morebitno kršitev, ali podatki, povezani z njimi, kot je opredeljeno v členu 9 Uredbe (EU) št. 165/2014.

V tem scenariju je čas, ki je na razpolago za komunikacijo, omejen, ker je komunikacija ciljno usmerjena in je po svoji zasnovi kratkega dosega. Poleg tega lahko pristojni nadzorni organi ista komunikacijska sredstva, ki se uporabljajo za nadzor tahografov na daljavo (RTM), uporabljajo tudi za druge namene (kot je največja teža in dimenzije težkih tovornih vozil, opredeljene v Direktivi 2015/719/ES), take operacije pa so lahko po presoji pristojnih nadzornih organov ločene ali zaporedne.

Ta dodatek določa:

— komunikacijsko opremo, postopke in protokole, ki se uporabljajo za *komunikacijo*,

— standarde in pravila, s katerimi mora biti skladna radijska oprema,

— predstavitev *podatkov* opremi za *komunikacijo.*,

— postopek zahteve in nalaganja ter zaporedje operacij,

— *podatke* za prenos,

— možno interpretacijo *podatkov,* ki se prenašajo v *komunikaciji*,

— določbe za zaščitne podatke, povezane s *komunikacijo*,

— razpoložljivost *podatkov* pristojnim nadzornim organom,

— način, na katerega lahko *bralnik komunikacije za zgodnje odkrivanje na daljavo* zahteva različne podatkovne koncepte glede tovora in voznega parka.

Pojasnilo: ta dodatek ne določa:

— operacije zbiranja *podatkov* in upravljanja z njimi znotraj VU (ki je odvisna od zasnove proizvoda, razen če je v Uredbi (EU) št. 165/2014) določeno drugače;

— oblike predstavitve zbranih podatkov predstavniku pristojnih nadzornih organov, niti meril, po katerih bodo pristojni nadzorni organi odločali, katera vozila bodo ustavili (to bo odvisno od zasnove proizvoda, razen če je drugje v Uredbi (EU) št. 165/2014 določeno drugače, ali od odločitve pristojnih nadzornih organov glede politike). Pojasnilo: *komunikacija* zgolj daje pristojnim nadzornim organom na razpolago *podatke*, da bodo lahko oni sami odločali na njihovi podlagi;

▼B

— določb o zaščiti podatkov (kot je šifriranje) glede vsebine *podatkov* (te bodo navedene v Dodatku 11, Skupni varnostni mehanizmi);

— podrobnosti drugih podatkovnih konceptov, razen RTM, ki jih je mogoče pridobiti z uporabo iste arhitekture in opreme;

— podrobnosti o obnašanju in upravljanju med VU in DSRC-VU, prav tako ne o obnašanju znotraj DSRC-VU (razen posredovanja *podatkov*, če je tako zahteval REDCR).

3 KRATICE, OPREDELITVE IN OZNAKE

Kratice in opredelitve, specifične za ta dodatek, ki se uporabljajo v tem dodatku:

antena	električna naprava, ki pretvarja električno energijo v radijske valove in obratno, ter se uporablja v kombinaciji z radijskim oddajnikom ali sprejemnikom. Radijski sprejemnik pri delovanju napaja terminale antene z električnim tokom, ki niha na radijski frekvenci, antena pa oddaja energijo iz električnega toka kot elektromagnetne valove (radijske valove). Pri sprejemanju antena prestreže nekaj energije elektromagnetnega vala in tako na svojih terminalih ustvari zelo nizko napetost, ki jo sprejemnik ojača;
Komunikacija	izmenjava informacij/podatkov med DSRC-REDCR in a DSRC-VU v skladu z oddelkom 5 v razmerju nadrejenega in podrejenega udeleženca z namenom pridobivanja podatkov.
Podatki	zaščiteni podatki opredeljenega formata (glej 5.4.4), ki jih zahteva enota *DSRC-REDCR* in ki jih enoti *DSRC-REDCR* posreduje enota *DSRC-VU* preko povezave 5,8 GHz DSRC, ko je opredeljeno v oddelku 5;
Uredba (ES) št. 165/2014	Uredba (EU) št. 165/2014 Evropskega parlamenta in Sveta z dne 4. februarja 2014 o tahografih v cestnem prometu, razveljavitvi Uredbe Sveta (EGS) št. 3821/85 o tahografu (nadzorni napravi) v

▼B

	cestnem prometu in spremembi Uredbe (ES) št. 561/2006 Evropskega parlamenta in Sveta o usklajevanju določene socialne zakonodaje v zvezi s cestnim prometom.
AID	identifikator aplikacije
BLE	nizkoenergijski Bluetooth
BST	tabela storitev signala oddajnika
CIWD	vstavitev kartice med vožnjo
CRC	ciklično preverjanje redundance
DSC (n)	identifikator zahteve za poseben dodatek DSRC
DSRC	Dedicated Short Range Communication (posebna komunikacija kratkega dosega)
DSRC-REDCR	DSRC – bralnik komunikacije za zgodnje odkrivanje na daljavo
DSRC-VU	DSRC – enota v vozilu To je „oprema za zgodnje odkrivanje na daljavo“, opredeljena v Prilogi 1C.
DWVC	vožnja brez veljavne kartice
EID	identifikator elementa
LLC	logično upravljanje povezave
LPDU	podatkovna enota protokola LLC
OWS	sistem za tehtanje v vozilu
PDU	podatkovna enota protokola
REDCR	bralnik komunikacije za zgodnje odkrivanje na daljavo To je „oprema bralnika komunikacije za zgodnje odkrivanje na daljavo“, opredeljena v Prilogi 1C.
RTM	nadzor tahografa na daljavo
SM-REDCR	varnostni modul – bralnik komunikacije za zgodnje odkrivanje na daljavo
TARV	telematične aplikacije za vozila, urejena s predpisi (serija standardov ISO 15638)

▼B

VU	enota v vozilu
VUPM	pomnilnik enote v vozilu za koristne podatke
VUSM	varnostni modul enote v vozilu
VST	tabela storitev vozila
WIM	tehtanje med premikanjem
WOB	tehtanje v vozilu

Specifikacija, opredeljena v tem dodatku, se navezuje na vse dele navedenih uredb in standardov in je odvisna od njih. V določbah tega dodatka so določeni upoštevni standardi ali upoštevne določbe standardov. V primeru neskladja veljajo določbe tega dodatka. Če pride do neskladja, pri katerem v tem dodatku ni jasno določena specifikacija, ima prednost delovanje v mejah ERC 70-03 (in preskušeno glede na ustrezne parametre standarda EN 300 674-1) nato pa v padajočem prednostnem redu EN 12795, EN 12253 EN 12834 in EN 13372, 6.2, 6.3, 6.4 in 7.1.

Ta priloga se sklicuje na naslednje uredbe in standarde:

[1] Uredba (EU) št. 165/2014 Evropskega parlamenta in Sveta z dne 4. februarja 2014 o tahografih v cestnem prometu, razveljavitvi Uredbe Sveta (EGS) št. 3821/85 o tahografu (nadzorni napravi) v cestnem prometu in spremembi Uredbe (ES) št. 561/2006 Evropskega parlamenta in Sveta o usklajevanju določene socialne zakonodaje v zvezi s cestnim prometom.

[2] Uredba (EU) št. 561/2006 Evropskega parlamenta in Sveta z dne 15. marca 2006 o usklajevanju določene socialne zakonodaje v zvezi s cestnim prometom in spremembi uredb Sveta (EGS) št.3821/85 in (ES) št. 2135/98 ter razveljavitvi Uredbe Sveta (EGS) št. 3820/85 (Besedilo velja za EGP).

[3] ERC 70-03 CEPT: Priporočilo ECC 70-03: glede uporabe naprav kratkega dosega (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); Oddajniška oprema za enouporabniško (osebno) komunikacijo kratkega dosega (DSRC) (s prenosnima hitrostma 500 kbit/s / 250 kbit/s), ki deluje v pasu 5,8 GHz, namenjenem industrijski, znanstveni in medicinski uporabi; Del 1: Splošne značilnosti in metode preskušanja za obcestne enote (RSU) in enote, nameščene v vozilu (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 SCENARIJI DELOVANJA

4.1 **Pregled**

Uredba (EU) št. 165/2014 določa posebne in nadzorovane scenarije, v mejah katerih se uporablja *komunikacija.*

Podprti scenariji:

„komunikacijski profil 1: cestni inšpekcijski pregled z uporabo brezžične komunikacije bralnika komunikacije za zgodnje odkrivanje na daljavo, na podlagi katere se opravi cestni inšpekcijski pregled (nadrejena enota – podrejena enota);

profil bralnika 1a: z bralnikom komunikacije za zgodnje odkrivanje na daljavo, namerjenim z roko ali nameščenim na nosilcu ob cesti;

profil bralnika 1b: z bralnikom komunikacije za zgodnje odkrivanje na daljavo, nameščenim na vozilu in usmerjenim v določeno smer“.

4.1.1 *Predpogoji za prenos podatkov preko vmesnika 5,8 GHz DSRC*

OPOMBA: Kontekst predpogojev je razviden iz slike 14.3.

4.1.1.1 Podatki, ki se hranijo v VU

DSC_12 Naloga VU je posodabljati podatke vsakih 60 sekund jih vzdrževati, da se shranijo v VU brez sodelovanja komunikacijske funkcije DSRC. To se doseže z notranjimi sredstvi VU, ki so določena v Uredbi (EU) št. 165/2014, Priloga 1 C, oddelek 3.19 „*Komunikacija na daljavo za namen ciljnih cestnih preverjanj*“, in niso določena v tem dodatku.

4.1.1.2 Podatki, ki se posredujejo opremi DSRC-VU

DSC_13 Naloga VU je posodabljati podatke tahografa DSRC (*podatki*) ob vsaki posodobitvi podatkov, shranjenih v VU, v presledku, določenem v 4.1.1.1 (DSC_12), brez sodelovanja komunikacijske funkcije DSRC.

DSC_14 Podatki VU se uporabljajo kot podlaga za polnjenje in posodabljanje *podatkov*, sredstva, s katerimi se to doseže, so določena v oddelku 3.19 Priloge 1C *Komunikacija na daljavo za namen ciljnih cestnih preverjanj*, če pa take določbe ni, so odvisna od zasnove proizvoda in niso določena v tem dodatku. Zasnova povezave med opremo DSRC-VU in VU je pojasnjena v oddelku 5.6.

▼B

4.1.1.3 Vsebina podatkov

DSC_15 Vsebina in format *podatkov* sta taka, da bosta po dešifriranju strukturirana in razpoložljiva v obliki in formatu iz oddelka 5.4.4 tega dodatka (podatkovne strukture).

4.1.1.4 Predstavitev podatkov

DSC_16 Potem ko so bili *podatki* večkrat posodobljeni v skladu s postopki, določenimi v 4.1.1.1, se pred predstavitvijo enoti *DSRC-VU* zaščitijo in se predstavijo kot vrednost zaščitenega podatkovnega koncepta, za začasno hrambo v *DSRC-VU* kot tekoča različica *podatkov*. Ti podatki se iz *VUSM* prenesejo v funkcijo DSRC *VUPM*. *VUSM* in *VUPM* sta funkciji in nista nujno fizični enoti. Oblika fizične konkretizacije teh funkcij je odvisna od zasnove proizvoda, razen če je določeno drugače v Uredbi (EU) št. 165/2014.

4.1.1.5 Zaščitni podatki

DSC_17 Zaščitni podatki (*securityData)*, ki vsebujejo podatke, ki jih zahteva *REDCR,* da lahko opravi nalogo dešifriranja *podatkov,* se posredujejo v skladu z opredelitvijo v Dodatku 11 Skupni varnostni mehanizmi in se predstavijo kot vrednost podatkovnega koncepta za začasno hrambo v *DSRC-VU* kot tekoča vrednost *zaščitnih podatkov* v obliki, opredeljeni v oddelku 5.4.4 te priloge.

4.1.1.6 Podatki VUPM, ki so na razpolago za prenos preko vmesnika DSRC

DSC_18 Podatkovni koncept, ki mora biti vedno na razpolago v funkciji DSRC VUPM za takojšen prenos na zahtevek *REDCR*, je opredeljen v oddelku 5.4.4 za celotne specifikacije modula ASN.1.

Splošni pregled komunikacijskega profila 1

Ta profil zajema primer uporabe, pri katerem predstavnik pristojnih nadzornih organov uporablja bralnik komunikacije za zgodnje odkrivanje na daljavo kratkega dosega (vmesniki 5,8 GHz DSRC delujejo v mejah standarda ERC 70-03 in so preskušeni glede na ustrezne parametre standarda EN 300 674-1, kot je opisano v oddelku 5) (*REDCR*), da na daljavo ugotovi, ali vozilo morebiti krši Uredbo (EU) št. 165/2014. Ko je bilo to za vozilo ugotovljeno, predstavnik pristojnih nadzornih organov, ki upravlja poizvedbo, odloči, ali je treba vozilo ustaviti.

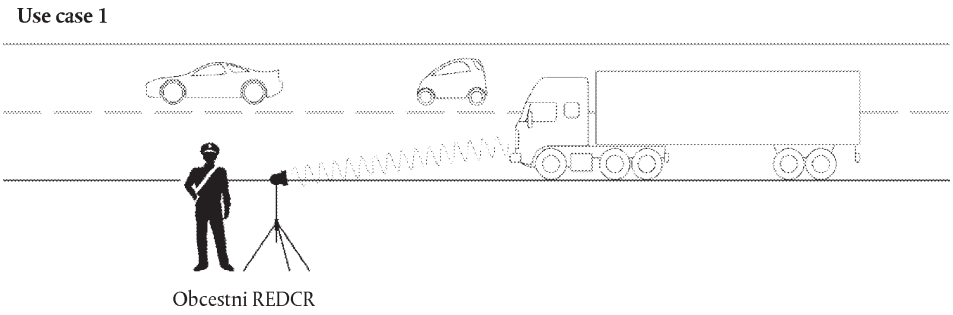
4.1.2 *Profil 1a: z bralnikom komunikacije za zgodnje odkrivanje na daljavo, namerjenim z roko ali začasno nameščenim na nosilcu ob cesti*

V tem primeru uporabe se predstavnik pristojnih nadzornih organov nahaja ob cesti in nameri *REDCR*, ki ga drži v roki ali ki je nameščen na trinožniku ali podobnem stojalu, z mesta ob cesti proti središču vetrobranskega stekla ciljnega vozila. Poizvedba se izvede z uporabo vmesnikov 5,8 GHz DSRC, ki delujejo v mejah standarda ERC 70-03 in so preskušeni glede na ustrezne parametre standarda EN 300 674-1, kot je opisano v oddelku 5. Glej sliko 14.1 (primer uporabe 1).

▼B

Slika 14.1

Obcestna poizvedba z uporabo 5,8 GHz DSRC

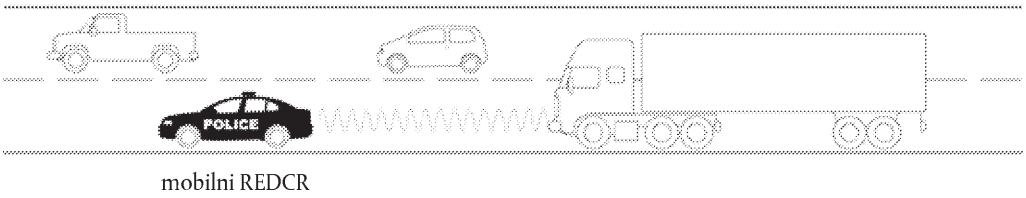


4.1.3 *Profil 1b: z bralnikom komunikacije za zgodnje odkrivanje na daljavo (REDCR), nameščenim na vozilu in usmerjenim v določeno smer*

V tem primeru uporabe se predstavnik pristojnega nadzornega organa nahaja v premikajočem se vozilu in nameri prenosni *REDCR*, ki ga drži v roki, iz vozila proti središču vetrobranskega stekla ciljnega vozila, ali pa je *REDCR* nameščen v vozilu ali na njem tako, da meri proti središču vetrobranskega stekla ciljnega vozila, ko je vozilo z bralnikom komunikacije za zgodnje odkrivanje na daljavo v določenem položaju glede na ciljno vozilo (npr. neposredno pred njim v tekočem prometu). Poizvedba se izvede z uporabo vmesnikov 5,8 GHz DSRC, ki delujejo v mejah ERC 70-03 in so preskušeni glede na ustrezne parametre standarda EN 300 674-1, kot je opisano v oddelku 5. Glej sliko 14.2 (primer uporabe 2).

Slika 14.2

Poizvedba iz vozila z uporabo 5,8 GHz DSRC



4.2 **Varnost/celovitost**

Da bi bilo mogoče preveriti avtentičnost in celovitost podatkov, prenesenih s komunikacijo na daljavo, se zaščiteni *podatki* preverijo in dešifrirajo v skladu z določbami dodatka 11, Skupni varnostni mehanizmi.

5 ZASNOVA KOMUNIKACIJE NA DALJAVO IN PROTOKOLI ZANJO

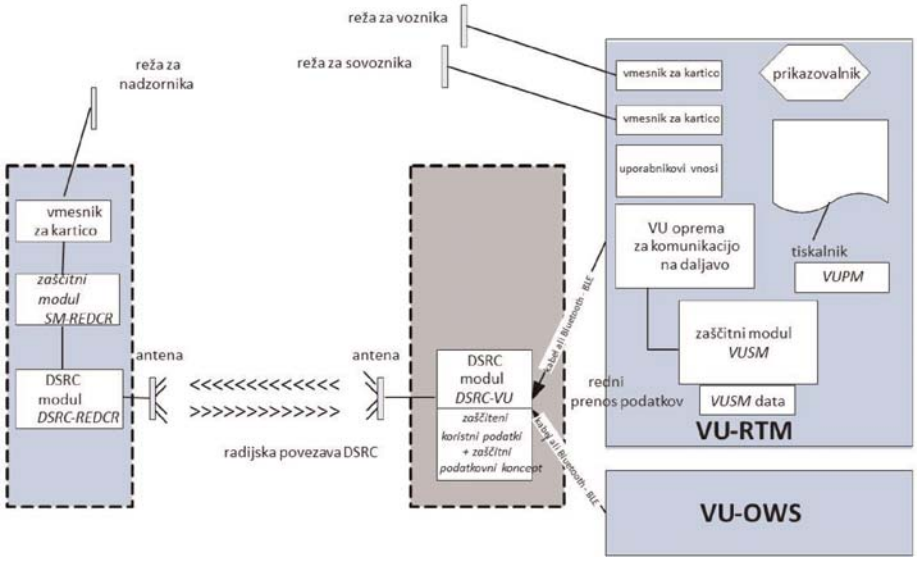
5.1 **Zasnova**

Zasnova funkcije komunikacije na daljavo v pametnem tahografu je prikazana na sliki 14.3.

▼B

Slika 14.3

Zasnova funkcije komunikacije na daljavo



DSC_19 Funkcije, ki se nahajajo v VU:

— Varnostni modul (*VUSM*). Naloga te funkcije v VU je zaščita *podatkov* za prenos iz *DSRC-VU* do predstavnika pristojnih nadzornih organov s komunikacijo na daljavo.

— Zaščiteni podatki so shranjeni v pomnilniku VUSM. VU v presledkih, določenih v 4.1.1.1 (DSC_12), šifrira in ponovno naloži podatkovni koncept RTM (ki zajema koristne podatke in vrednosti koncepta zaščitnih podatkov, določene spodaj v tem dodatku), ki je shranjen v pomnilniku DSRC-VU Delovanje varnostnega modula je opredeljeno v Dodatku 11, Skupni varnostni mehanizmi, in je zunaj področja tega dodatka, razen da je potrebna za zagotavljanje posodobitev komunikacijske opreme VU ob vsaki spremembi podatkov VUSM.

— Komunikacija med VU in DSRC-VU je lahko žična ali kot nizkoenergijski Bluetooth (BLE), fizično pa je DRSC-VU lahko integriran z anteno na vetrobranskem steklu vozila, lahko je v notranjosti VU ali kje vmes med njima.

— DSRC-VU mora imeti ves čas na razpolago zanesljiv vir napajanja. Način zagotavljanja napajanja je odvisen od zasnove.

— Pomnilnik DSRC-VU ne sme biti neobstojen, tako da lahko ohranja podatke v DSRC-VU tudi, kadar je stikalo vozila za vžig izklopljeno.

— Če komunikacija med VU in DSRC-VU poteka preko BLE, vir napajanja pa je baterija, ki je ni mogoče ponovno napolniti, je treba vir napajanja DSRC-VU zamenjati ob vsakem rednem kontrolnem pregledu, proizvajalec opreme

▼B

DSRC-VU pa mora zagotoviti, da bo napajanje zadostovalo do naslednjega rednega kontrolnega pregleda, s čimer bo REDCR omogočen normalen dostop do podatkov skozi celotno obdobje brez prenehanja ali prekinitve.

— Oprema VU RTM „pomnilnik za koristne podatke“ (*VUPM*). Naloga te funkcije, ki se nahaja v VU, je zagotavljanje in posodabljanje *podatkov*. Vsebina *podatkov*. („TachographPayload“) je opredeljena v oddelkih 5.4.4/5.4.5 in se posodablja v presledkih, določenih v oddelku 4.1.1.1 (DSC_12).

— DSRC-VU. Ta funkcija, ki je znotraj antene ali je povezana z njo in komunicira z VU preko žične ali brezžične (BLE) povezave, hrani tekoče podatke (*podatke VUPM*) in upravlja odgovor na poizvedbo preko medija 5,8 GHz DSRC. Odklop opreme DSRC ali motenje delovanja opreme DSRC med normalnim obratovanjem vozila se šteje za kršitev Uredbe (EU) št. 165/2014.

— Varnostni modul (REDCR) (*SM-REDCR*) je funkcija za dešifriranje in preverjanje celovitosti podatkov, ki izvirajo iz VU. Sredstva, s katerimi se to doseže, so določena v Dodatku 11, Skupni varnostni mehanizmi, in ni opredeljena v tem dodatku.

— Funkcija opreme DSRC (REDCR) (*DSRC-REDCR*) vsebuje oddajnik-sprejemnik 5,8 GHz ter povezano strojno-programsko opremo in programsko opremo, ki upravlja *komunikacijo* z *DSRC-VU* v skladu s tem dodatkom.

— *DSRC-REDCR* pošlje poizvedbo *DSRC-VU* ciljnega vozila in pridobi *podatke* (tekoče *podatke VUPM* ciljnega vozila) preko povezave DSRC, prejete podatke obdela in jih shrani v svojem *SM-REDCR*.

— Antena *DSRC-VU* (antena) je nameščena na mestu, na katerem omogoča najboljšo možno komunikacijo DSRC med vozilom in obcestno anteno (na splošno v središču vetrobranskega stekla vozila ali blizu njega). Pri lahkih vozilih je primerna namestitev, ki ustreza zgornjemu delu vetrobranskega stekla.

— Pred anteno ali blizu nje ne sme biti kovinskih predmetov (npr. ploščice z imeni, nalepke, trakovi antirefleksne folije (zatemnjevanje), ščitniki proti soncu, brisalci v mirujočem položaju), ki bi lahko motili komunikacijo.

— Antena mora biti nameščena tako, da je njena smer snopa vzporedna s površino ceste.

▼B

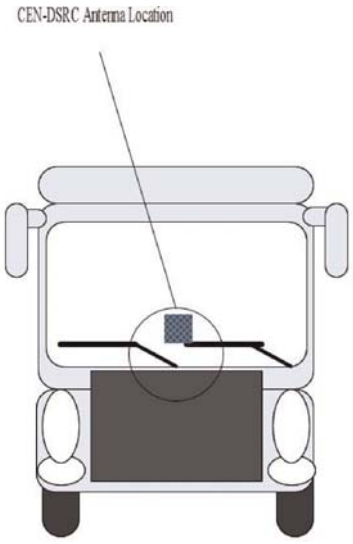
DSC_20 Antena in komunikacija delujeta v mejah standarda ERC 70-03 in sta preskušeni glede na ustrezne parametre standarda EN 300 674-1, kot je opisano v oddelku 5. Antena in komunikacija lahko izvedeta tehnike za ublažitev tveganja brezžičnih motenj, kot je opisano v poročilu ECC 228, npr. z uporabo filtrov v komunikaciji CEN DSRC 5,8 GHz.

DSC_21 Antena DSRC je z opremo DSRC-VU povezana neposredno znotraj modula, nameščenega na vetrobranskem steklu ali blizu njega, ali pa po posebnem kablu, ki je zasnovan tako, da otežuje prepovedan odklop. Odklop ali motenje delovanja antene pomeni kršitev Uredbe (EU) št. 165/2014. Namerno prikrivanje delovanja antene ali kakšna koli drugačna slabitev zmogljivosti antene se šteje za kršitev Uredbe št. 165/2014.

DSC_22 Faktor oblike antene ni opredeljen in je poslovna odločitev, vendar mora nameščeni DSRC-VU izpolnjevati zahteve o skladnosti, opredeljene v oddelku 5. Antena mora biti nameščena na položaju, ki je določen v DSC_19 in prikazan na sliki 14.4 (ovalno polje) ter mora učinkovito podpirati primere uporabe iz 4.1.2 in 4.1.3.

Slika 14.4

Primer namestitve antene 5,8 GHz DSRC na vetrobranskem steklu za vozila, urejena s predpisi



Faktor oblike *REDCR* in njegove antene je lahko različen glede na namestitev bralnika (nameščen na trinožniku, ročni, nameščen na vozilu itd.) in način delovanja, ko ga uporablja predstavnik pristojnih nadzornih organov.

Rezultati funkcije komunikacije na daljavo se predstavniku pristojnih nadzornih organov predstavijo preko prikaza in/ali funkcije obveščanja. Prikaz je možen na zaslonu, kot izpis na papirju, zvočni signal ali kombinacija navedenega. Oblika takega prikaza in/ali obvestila je odvisna od zahtev predstavnikov pristojnih nadzornih organov in zasnove opreme ter ni določena v tem dodatku.

▼B

DSC_23 Zasnova in faktor oblike *REDCR* sta odvisna od komercialne zasnove, ki mora omogočati delovanje v mejah ERC 70-03, ter zasnove in specifikacij zmogljivosti, opredeljenih v tem dodatku (oddelek 5.3.2), s čimer bo trgu omogočena čim večja prilagodljivost v zasnovi in zagotavljanju opreme za uporabo v posebnih scenarijih poizvedbe katerega koli pristojnega nadzornega organa.

DSC_24 Zasnova in faktor oblike *DSRC-VU* in njena namestitev v VU ali zunaj nje so odvisni od komercialne zasnove, ki mora omogočati delovanje v mejah ERC 70-03, ter zasnove in specifikacij zmogljivosti, opredeljenih v tem dodatku (oddelek 5.3.2) in v tem odstavku (5.1).

DSC_25 Vendar mora biti *DSRC-VU* v razumnih mejah sposobna prejemati vrednosti podatkovnih konceptov od druge pametne opreme vozila s pomočjo povezave in protokolov v skladu z odprtimi industrijskimi standardi (npr. od opreme za tehtanje v vozilu), če so podatkovni koncepti identificirani z edinstvenimi in znanimi identifikatorji/imeni datotek, navodila za delo s takimi protokoli pa so na razpolago Evropski komisiji in so brezplačno na razpolago proizvajalcem zadevne opreme.

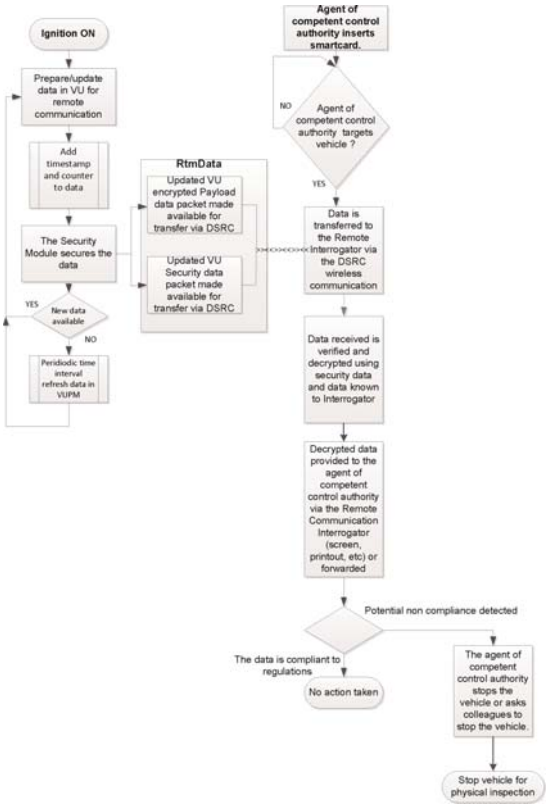
5.2 **Postopek dela**

5.2.1 *Operacije*

Postopek dela za operacije je opisan na sliki 14.5.

Slika 14.5

Postopek dela funkcije komunikacije na daljavo



▼B

Opis korakov:

a. kadar vozilo deluje (stikalo za vžig v položaju ON), tahograf posreduje podatke funkciji VU. Funkcija VU pripravi *podatke* za funkcijo komunikacije na daljavo (šifrirano) in posodobi *VUPM*, shranjen v pomnilniku *DSRC-VU* (kot je opredeljeno v oddelkih 4.1.1.1–4.1.1.2). Zbrani *podatki* se formatirajo, kot je opredeljeno v oddelkih 5.4.4.–5.4.5;

b. ob vsaki posodobitvi *podatkov* se posodobi časovni žig, opredeljen v konceptu zaščitnih podatkov;

c. funkcija *VUSM* zaščiti podatke v skladu s postopki, določenimi v Dodatku 11;

d. Ob vsaki posodobitvi *podatkov* (glej 4.1.1.1–4.1.1.2) se *podatki* prenesejo v *DSRC-VU*, kjer zamenjajo prejšnje podatke, tako da so posodobljeni tekoči podatki (*podatki*) vedno na voljo za posredovanje v primeru poizvedbe s strani *REDCR*. Ko VU *podatke* posreduje DSRC-VU, morajo biti ti podatki razpoznavni s pomočjo imena datoteke, *RTMData*, ali identifikacijske oznake aplikacije in identifikatorjev atributov.

e. Če želi predstavnik pristojnih nadzornih organov izbrati vozilo in od njega pridobiti *podatke*, najprej vstavi svojo pametno kartico v *REDCR*, da vzpostavi *komunikacijo* in omogoči. da *SM-REDCR* preveri njeno avtentičnost in dešifrira podatke.

f. Predstavnik pristojnega nadzornega organa nato izbere vozilo in poda zahtevek za podatke preko komunikacije na daljavo. *REDCR* odpre sejo vmesnika 5,8 GHz DSRC z *DSRC-VU* ciljnega vozila in zahteva *podatke*. *Podatki* se v *REDCR* prenesejo preko brezžičnega komunikacijskega sistema kot atribut DSRC s pomočjo aplikacijske storitve GET, kot je opredeljeno v oddelku 5.4. Atribut vsebuje šifrirane vrednosti koristnih podatkov in zaščitne podatke DSRC.

g. Potem ko podatke analizira oprema *REDCR*, se posredujejo predstavniku pristojnega nadzornega organa.

h. Predstavnik pristojnega nadzornega organa se s pomočjo teh podatkov odloči, ali bo vozilo ustavil za temeljitejši pregled ali pa bo zaprosil drugega predstavnika pristojnega nadzornega organa, da ustavi vozilo.

5.2.2 *Razlaga podatkov, prejetih preko komunikacije DSRC*

DSC_26 Podatki, prejeti preko vmesnika 5,8 GHz, imajo pomen in format, opredeljen v oddelkih 5.4.4 in 5.4.5, in samo tak pomen in format, razumeti pa jih je treba v okviru ciljev, opredeljenih v teh oddelkih. V skladu z določbami Uredbe

▼B

(EU) št. 165/2014 se *podatki* uporabljajo samo za posredovanje pomembnih informacij pristojnemu nadzornemu organu v pomoč pri določanju vozila, ki ga je treba ustaviti za fizični pregled, pozneje pa se uničijo v skladu s členom 9 Uredbe (EU) št. 165/2014.

5.3 **Parametri fizičnega vmesnika DSRC za komunikacijo na daljavo**

5.3.1 *Omejitve glede kraja namestitve*

DSC_27 Pridobivanje podatkov na daljavo pri vozilih z uporabo vmesnika 5,8 GHz DSRC se ne sme uporabljati na razdalji manj kot 200 m od delujočega portala 5,8 GHz DSRC.

5.3.2 *Parametri za navzdolnjo in navzgornjo povezavo*

DSC_28 Oprema, ki se uporablja za nadzor tahografa na daljavo, mora biti skladna s standardom ERC70-03 in parametri, opredeljenimi v tabelah 14.1 in 14.2, ter delovati v njihovih mejah.

DSC_29 Poleg tega mora biti oprema za nadzor tahografa na daljavo za zagotovitev skladnosti s parametri delovanja drugih standardiziranih sistemov 5,8 GHz DSRC skladna s parametri iz standardov EN 12253 in EN 13372.

Torej velja:

Tabela 14.1

Parametri za navzdolnjo povezavo

Točka št.	Parameter	Vrednosti	Opomba
D1	Nosilne frekvence navzdolnje povezave	REDCR lahko uporablja štiri alternativne možnosti: 5,7975 GHz 5,8025 GHz 5,8075 GHz 5,8125 GHz	V mejah standarda ERC 70-03. Nosilne frekvence lahko izbere izvajalec obcestnega sistema, ni potrebno, da bi jih poznal DSRC-VU. (skladno s standardi EN 12253, EN 13372)
D1a (*)	Toleranca nosilnih frekvenc	v območju ± 5 ppm	(skladno s standardom EN 12253)
D2 (*)	RSU (REDCR) maska spektra oddajnika	V mejah standarda ERC 70-03. REDCR je v skladu z razredom B,C, kot je opredeljen v EN 12253. Brez drugih posebnih zahtev v tej prilogi.	Parameter, ki se uporablja za nadzor interference med poizvedovalniki v bližini (kot je opredeljeno v standardih EN 12253 in EN 13372).
D3	OBU(DSRC-VU) najnižji frekvenčni razpon	5,795 – 5,815 GHz	(skladno s standardom EN 12253)
D4 (*)	Največji E.I.R.P.	v mejah standarda ERC 70-03 (nelicenciran) in nacionalne ureditve največ + 33 dBm	(skladno s standardom EN 12253)

▼B

Točka št.	Parameter	Vrednosti	Opomba
D4a	Maska kotne E.I.R.P.	v skladu s prijavljeno in objavljeno specifikacijo oblikovalca poizvedovalnika	(skladno s standardom EN 12253)
D5	Polarizacija	levosučna krožna	(skladno s standardom EN 12253)
D5a	Navzkrižna polarizacija	XPD: v smeri snopa: (REDCR) RSU t ≥ 15 dB (DSRC-VU) OBU r ≥ 10 dB v območju –3 dB: (REDCR) RSU t ≥ 10 dB (DSRC-VU) OBU r ≥ 6 dB	(skladno s standardom EN 12253)
D6 (*)	Modulacija	dvonivojska amplitudna modulacija	(skladno s standardom EN 12253)
D6a (*)	Indeks modulacije	0,5 … 0,9	(skladno s standardom EN 12253)
D6b	Očesni vzorec	≥ 90 % (čas) / ≥ 85 % (amplituda)	
D7 (*)	Kodiranje podatkov	FM0 Bit ‘1’ ima prehode samo na začetku in koncu bitnega intervala. Bit ‘0’ ima dodaten prehod sredi bitnega intervala v primerjavi z bitom ‘1’.	(skladno s standardom EN 12253)
D8 (*)	Bitna hitrost	500 kBit/s	(skladno s standardom EN 12253)
D8a	Toleranca ure za serijski premik podatkov	boljša od ± 100 ppm	(skladno s standardom EN 12253)
D9 (*)	Delež napačnih bitov (B.E.R.) za komunikacijo	$\leq 10^{-6}$, če je pripadajoča moč na OBU (DSRC-VU) v razponu, danem od [D11a to D11b].	(skladno s standardom EN 12253)
D10	Prožilec bujenja za OBU (DSRC-VU)	OBU (DSRC-VU) se prebudi ob prejemu okvira z 11 ali več okteti (vključno s preambulo).	Ni potreben poseben budilni vzorec. DSRC-VU se lahko prebudi ob prejemu okvira z manj kot 11 okteti. (skladno s standardom EN 12253)
D10a	najdaljši zagonski čas	≤ 5 ms	(skladno s standardom EN 12253)
D11	Cona komunikacije	prostorsko območje, v katerem se sprejema B.E.R. v skladu z D9a	(skladno s standardom EN 12253)
D11a (*)	Meja moči za komunikacijo (zgornja)	– 24dBm	(skladno s standardom EN 12253)

▼B

Točka št.	Parameter	Vrednosti	Opomba
D11b (*)	Meja moči za komunikacijo (spodnja)	pripadajoča moč: – 43 dBm (smer snopa) – 41 dBm (v razponu – 45° – + 45°, ustreza ploskvi, vzporedni s cestiščem, če je DSRC-VU pozneje nameščen v vozilu (azimut))	(skladno s standardom EN 12253) razširjena zahteva za vodoravne kote do ± 45° zaradi primerov uporabe, opredeljenih v tem dodatku
D12 (*)	Minimalna raven moči za (DSRC-VU)	– 60 dBm	(skladno s standardom EN 12253)
D13	Preambula	Preambula je obvezna.	(skladno s standardom EN 12253)
D13a	Dolžina in vzorec preambule	16 bitov ± 1 bit FM0 kodirano kot ‘1’ bit	(skladno s standardom EN 12253)
D13b	Valovna oblika preambule	izmenjujoče se zaporedje nizke in visoke ravni s trajanjem impulza 2 μs Toleranca je podana z D8a.	(skladno s standardom EN 12253)
D13c	Zaključni biti	RSU (REDCR) lahko odpošlje največ 8 bitov po zaključni zastavici. Od OBU (DSRC-VU) se ne zahteva, da bi te dodatne bite upoštevala.	(skladno s standardom EN 12253)

(*) – Za parametre navzdolnje povezave je potreben preskus skladnosti v skladu z ustreznim preskusom parametra iz standarda EN 300 674-1.

Tabela 14.2

Parametri za navzgornjo povezavo

Točka št.	Parameter	Vrednosti	Opomba
U1 (*)	Podnosilne frekvence	OBU (DSRC-VU) podpira 1,5 MHz in 2,0 MHz. RSU (REDCR) podpira 1,5 MHz ali 2,0 MHz ali obe. U1-0: 1,5 MHz U1-1: 2,0 MHz	Izbira podnosilne frekvence (1,5 MHz ali 2,0 MHz) je odvisna od izbranega profila iz standarda EN 13372.
U1a (*)	Toleranca podnosilnih frekvenc	v razponu ± 0,1 %	(skladno s standardom EN 12253)
U1b	Uporaba bočnih pasov	isti podatki na obeh straneh	(skladno s standardom EN 12253)
U2 (*)	OBU (DSRC-VU) maska spektra oddajnika	V skladu z EN12253: 1) moč izhodnega pasu: glej ETSI EN 300674-1;	(skladno s standardom EN 12253)

▼B

Točka št.	Parameter	Vrednosti	Opomba
		2) moč vhodnega pasu: [U4a] dBm v 500 kHz; 3) oddajanje v drug kanal za navzgornjo povezavo: U2(3)-1 = –35 dBm v 500 kHz.	
U4a (*)	Največji enobočni E.I.R.P. (smer snopa)	Dve možnosti: U4a-0: –14 dBm U4a-1: –21 dBm	v skladu s prijavljeno in objavljeno specifikacijo oblikovalca opreme
U4b (*)	Največji enobočni E.I.R.P. (35°)	Dve možnosti: — ni relevantno; — – 17dBm.	v skladu s prijavljeno in objavljeno specifikacijo oblikovalca opreme
U5	Polarizacija	levosučna krožna	(skladno s standardom EN 12253)
U5a	Navzkrižna polarizacija	XPD: v smeri snopa: (REDCR) RSU r ≥ 15 dB (DSRC-VU) OBU t ≥ 10 dB v območju –3 dB: (REDCR) RSU r ≥ 10 dB (DSRC-VU) OBU t ≥ 6 dB	(skladno s standardom EN 12253)
U6	podnosilna modulacija	2-PSK Šifrirani podatki sinhronizirani s podnosilcem: prehodi šifriranih podatkov sovpadajo s prehodi podnosilca.	(skladno s standardom EN 12253)
U6b	Obratovalni cikel	obratovalni cikel: 50 % ± α, α ≤ 5 %	(skladno s standardom EN 12253)
U6c	modulacija na nosilcu	množenje moduliranega podnosilca z nosilcem	(skladno s standardom EN 12253)
U7 (*)	Kodiranje podatkov	NRZI (brez prehoda na začetku bita ‘1’, prehod na začetku bita ‘0’, brez prehoda znotraj bita)	(skladno s standardom EN 12253)
U8 (*)	Bitna hitrost	250 kbit/s	(skladno s standardom EN 12253)
U8a	Toleranca ure za serijski premik podatkov	v območju ± 1 000 ppm	(skladno s standardom EN 12253)
U9	Delež napačnih bitov (B.E.R.) za komunikacijo	$\leq 10^{-6}$	(skladno s standardom EN 12253)

▼B

Točka št.	Parameter	Vrednosti	Opomba
U11	Cona komunikacije	prostorsko območje, v katerem se nahaja DSRC-VU, in sicer tako, da njegove prenose sprejema REDCR z B.E.R., ki je nižji od tistega, ki je naveden v U9a.	(skladno s standardom EN 12253)
U12a (*)	Ojačitev pri pretvorbi (spodnja meja)	1 dB za vsak bočni pas Kotni razpon: krožno simetričen med smerjo snopa in ± 35° ter	
		med – 45° – + 45°, ustreza ploskvi, vzporedni s cestiščem, če je DSRC-VU pozneje nameščen v vozilu (azimut).	večji od razpona vrednosti, določenega za vodoravne kote do ± 45°, zaradi primerov uporabe, opredeljenih v tem dodatku
U12b (*)	Ojačitev pri pretvorbi (zgornja meja)	10 dB za vsak bočni pas	manjša od vrednosti, določene za vsak bočni pas znotraj krožnega stožca okrog smeri snopa s kotom odpiranja ± 45°
U13	Preambula	Preambula je obvezna.	(skladno s standardom EN 12253)
U13a	Preambula dolžina in vzorec	od 32 do 36 μs, modulirana samo s podnosilcem, nato 8 bitov ‘0’, kodiranih NRZI.	(skladno s standardom EN 12253)
U13b	Zaključni biti	DSRC-VU lahko odpošlje največ 8 bitov po zaključni zastavici. Od RSU (REDCR) se ne zahteva, da bi te dodatne bite upoštevala.	(skladno s standardom EN 12253)

(*) – Za parametre navzgornje povezave je potreben preskus skladnosti v skladu z ustreznim preskusom parametra iz standarda EN 300 674-1.

5.3.3 *Zasnova antene*

5.3.3.1 Antena REDCR

DSC_30 Zasnova antene *REDCR* je odvisna od komercialne zasnove, ki omogoča delovanje v mejah, opredeljenih v oddelku 5.3.2 in ki je prilagojena za najboljšo možno zmogljivost branja *DSRC-REDCR* za poseben namen in za okoliščine branja, za kakršne je bil zasnovan *REDCR*.

5.3.3.2 Antena VU

DSC_31 Zasnova antene *DSRC-VU* je odvisna od komercialne zasnove, ki omogoča delovanje v mejah, opredeljenih v oddelku 5.3.2 in ki je prilagojena za najboljšo možno zmogljivost branja *DSRC-REDCR* za poseben namen in za okoliščine branja, za kakršne je bil zasnovan *REDCR*.

▼B

DSC_32 Antena VU mora biti pritrjena na sprednje vetrobransko steklo vozila ali blizu njega, kakor je navedeno v oddelku 5.1.

DSC_33 V preskusnem okolju v servisni delavnici (glej oddelek 6.3) se mora antena DSRC-VU, pritrjena, kot je navedeno v oddelku 5.1, uspešno povezati s standardno preskusno komunikacijo in uspešno posredovati transakcijo RTM, kot je opredeljena v tej prilogi, na razdalji 2–10 m, nad 99 % časa, izračunano kot povprečje na podlagi 1 000 poizvedb.

5.4 **Zahteve protokola DSRC za RTM**

5.4.1 *Pregled*

DSC_34 Protokol transakcije za prenos *podatkov* preko povezave vmesnika 5,8 GHz DSRC poteka po spodaj navedenem postopku. V tem oddelku je opisan potek transakcije v idealnih pogojih brez ponovnega oddajanja ali prekinitev komunikacije.

Opomba: namen faze inicializacije (korak 1) je vzpostaviti komunikacijo med *REDCR* in tistimi DSRC-VU, ki so vstopile v transakcijsko cono 5,8 GHz DSRC (nadrejeni in podrejeni udeleženec), vendar še niso vzpostavile komunikacije z *REDCR*, in obvestiti procese aplikacije.

— **Korak 1** Inicializacija. *REDCR* pošlje okvir s „tabelo storitev signala oddajnika“ (BST), ki v seznamu storitev, ki jih podpira, zajema identifikatorje aplikacije (AIDs). V aplikaciji RTM bo to samo storitev z vrednostjo AID = 2 („tovor in vozni park“, Freight&Fleet). *DSRC-VU* ovrednoti prejeto BST in odgovori (glej spodaj) s seznamom podprtih aplikacij v domeni Freight&Fleet oziroma ne odgovori, če nobena ni podprta. Če *REDCR* ne ponudi AID=2, DSRC-VU ne odgovori REDCR.

— **Korak 2** *DSRC-VU* pošlje okvir z zahtevo za dodelitev zasebnega okna.

— **Korak 3** *REDCR* pošlje okvir z dodelitvijo zasebnega okna.

— **Korak 4** *DSRC-VU* uporabi dodeljeno zasebno okno za pošiljanje okvira s svojo tabelo storitev vozila (VST). Ta VST vsebuje seznam vseh različnih konkretizacij aplikacije, ki jih *DSRC-VU* podpira v okviru AID=2. Različne konkretizacije so določene s pomočjo edinstvene ustvarjene EID, vsaka je povezana z vrednostjo parametra Application Context Mark, ki označuje podprto aplikacijo in standard.

— **Korak 5** *REDCR* nato analizira ponujeno VST, nato pa ali prekine zvezo (RELEASE), ker ga ne zanima nič od tistega, kar nudi VST (tj. prejema VST od *DSRC-VU*, ki ne podpira transakcije RTM), ali, če prejme ustrezno VST, začne konkretizacijo aplikacije.

▼B

— **Korak 6** REDCR v ta namen pošlje okvir z ukazom za pridobitev podatkov RTM, pri čemer identificira konkretizacijo aplikacije RTM tako, da navede identifikator, ki ustreza konkretizaciji aplikacije RTM (kot jo je določila DSRC-VU v VST), in dodeli zasebno okno.

— **Korak 7** *DSRC-VU* na novo dodeljeno zasebno okno uporabi za pošiljanje okvira z naslovljenim identifikatorjem, ki ustreza konkretizaciji aplikacije, kot je navedena v VST, sledi pa ji atribut *RtmData* (element koristnih podatkov + zaščitni element).

— **Korak 8** Če se zahteva več storitev, se vrednost ‘n’ spremeni v referenčno številko naslednje storitve in postopek se ponovi.

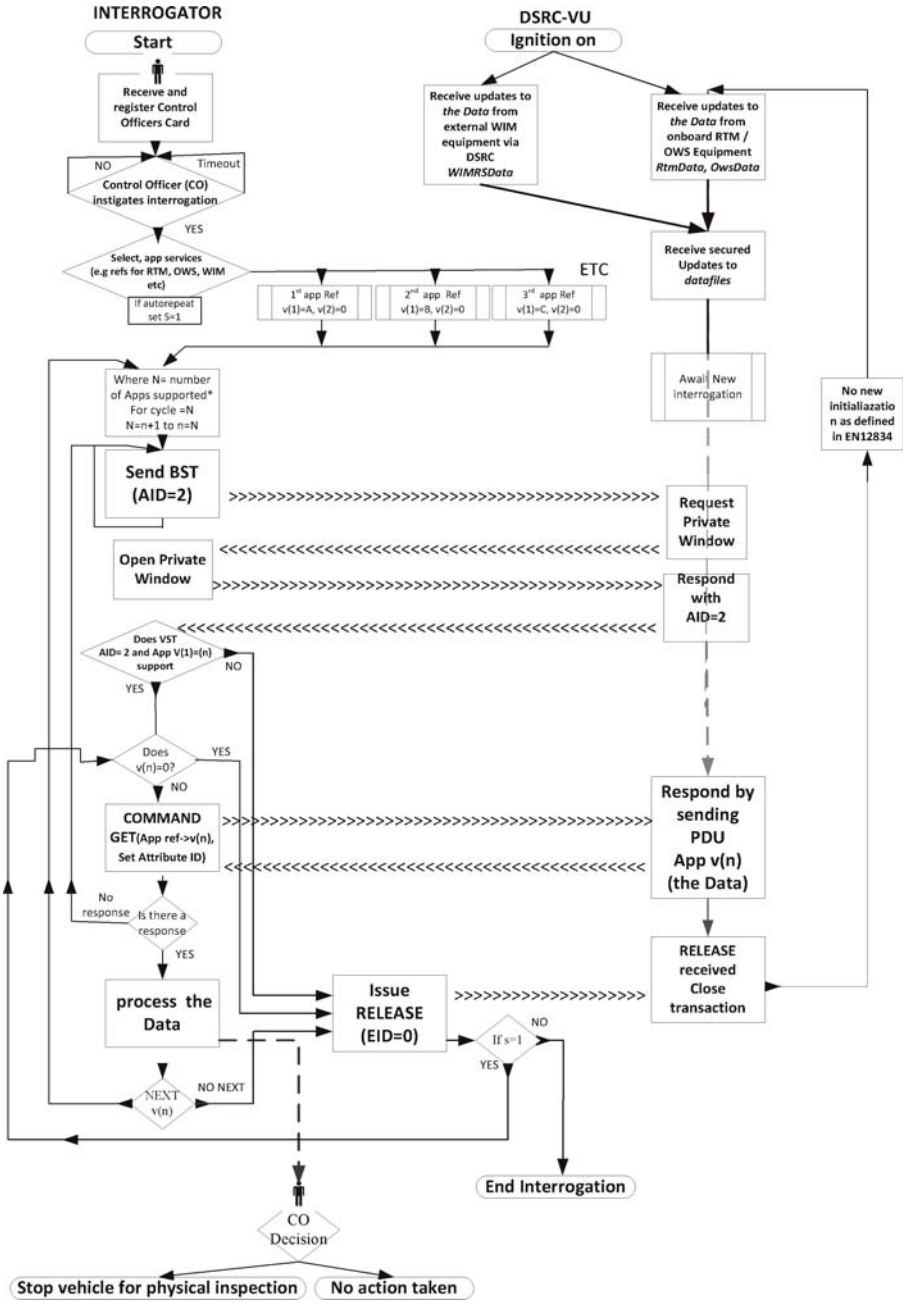
— **Korak 9** *REDCR* potrdi prejem podatkov tako, da pošlje *DSRC-VU* okvir z ukazom RELEASE, s katerim slednji prekine sejo ali, če ni potrdil uspešnega prejema LDPU, se vrne na korak 6.

Slikovna ponazoritev transakcijskega protokola je na sliki 14.6.

▼B

Slika 14.6

Potek procesa RTM preko 5,8 GHz DSRC



5.4.2 *Ukazi*

DSC_35 Edine funkcije, ki se uporabljajo v fazi transakcije RTM, so naslednji ukazi:

— **INITIALISATION.request**: Ukaz, ki ga REDCR pošlje v obliki oddajanja z opredelitvijo aplikacij, ki jih podpira

— **INITIALISATION.response**: Odgovor, s katerim DSRC-VU potrjuje zvezo in ki vsebuje seznam podprtih konkretizacij aplikacij z značilnostmi in informacijami o njihovem naslavljanju (EID).

▼B

— **GET.request**: Ukaz, ki ga *REDCR*pošlje v *DSRC-VU* in ki določa konkretizacijo aplikacije, ki bo naslovljena s pomočjo opredeljenega EID, kot je bil prejet v VST; s tem ukazom pa se *DSRC-VU* ukaže, da pošlje izbrane atribute s *podatki*. Cilj ukaza GET je, da *REDCR* dobi *podatke* od *DSRC-VU*.

— **GET.response**: Odgovor DSRC-VU, ki vsebuje zahtevane *podatke*.

— **ACTION.request ECHO**: Ukaz, s katerim se *DSRC-VU* ukaže, da povratne podatke *DSRC-VU* pošlje *REDCR*. Cilj ukaza ECHO je omogočiti servisnim delavnicam ali objektom za homologacijske preskuse, da preskusijo delovanje povezave DSRC, ne da bi potrebovali dostop do varnostnih poverilnic.

— **ACTION**.response ECHO: Odgovor DSRC VU na ukaz ECHO.

— **EVENT_REPORT.request** RELEASE: Ukaz, s katerim se *DSRC-VU* sporoči, da je transakcija končana. Cilj ukaza RELEASE je končati sejo z *DSRC-VU*. *DSRC-VU* po prejemu ukaza RELEASE ne odgovarja več na poizvedbe med tekočo povezavo. Opozorilo: v skladu s standardom EN 12834 se DSRC-VU ne bo povezala dvakrat z istim poizvedovalnikom, razen če je bila izven cone komunikacije 255 sekund ali če se je spremenila identifikacijska številka signala antene poizvedovalnika.

5.4.3 *Zaporedje ukazov pri poizvedbi*

DSC_36 Opis transakcije z vidika zaporedja ukaza in odgovora:

Zaporedje	Pošiljatelj		Prejemnik	Opis	Dejanje
1	REDCR	>	DSRC-VU	Inicializacija komunikacije povezava – zahteva	REDCR oddaja BST
2	*DSRC-VU*	>	*REDCR*	*Inicializacija komunikacije povezava – odgovor*	*Če BST podpira AID=2, potem DSRC-VU zahteva privatno okno.*
3	REDCR	>	DSRC-VU	Dodeli zasebno okno.	Pošlje okvir, ki vsebuje dodelitev zasebnega okna.
4	*DSRC-VU*	>	*REDCR*	*Pošlje VST.*	*Pošlje okvir, ki vsebuje VST.*
5	REDCR	>	DSRC-VU	Pošlje GET.request za podatke v atributu za določen EID.	
6	*DSRC-VU*	>	*REDCR*	*Pošlje GET.response z zahtevanim atributom za določen EID.*	*Pošlje atribut (RTMData, OWSData ...) s podatki za določen EID.*

▼B

Zaporedje	Pošiljatelj		Prejemnik	Opis	Dejanje
7	REDCR	>	DSRC-VU	Pošlje GET.request za podatke drugega atributa (če je primerno).	
8	*DSRC-VU*	>	*REDCR*	*Pošlje GET.response z zahtevanim atributom.*	*Pošlje atribut s podatki za določen EID.*
9	REDCR	>	DSRC-VU	Potrdi uspešen prejem podatkov	Pošlje ukaz RELEASE, ki zaključi transakcijo.
10	*DSRC-VU*			*Zaključi transakcijo.*	

Primer zaporedja transakcije in vsebine izmenjanih okvirov je opredeljen v oddelkih 5.4.7 in 5.4.8.

5.4.4 *Strukture podatkov*

DSC_37 Semantična struktura *podatkov* med prenosom preko vmesnika 5,8 GHz DSRC mora biti skladna s tistim, kar je opisano v tem dodatku. V tem oddelku je določeno, kako so ti podatki strukturirani.

DSC_38 Koristni podatki (podatki RTM) so sestavljeni iz združitve

1. podatkov EncryptedTachographPayload, ki so šifrirani podatki TachographPayload, opredeljeni v ASN.1 v oddelku 5.4.5. Metoda šifriranja je opisana v Dodatku 11.

2. DSRCSecurityData, navedeni v Dodatku 11.

DSC_39 Podatki RTM so naslovljeni kot atribut RTM = 1 in se prenesejo v RTM vsebnik = 10.

DSC_40 Oznaka konteksta RTM identificira podprti standard v seriji standardov TARV (RTM ustreza delu 9).

Modul ASN.1 za podatke DSRC znotraj aplikacije RTM se opredeli:

▼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 RtmData, izvedena dejanja in opredelitve*

DSC_41 Podatkovne vrednosti, ki jih izračuna VU in s katerimi se posodobijo zaščiteni podatki v DSRC-VU, se izračunajo v skladu s pravili,opredeljenimi v tabeli 14.3:

Tabela 14.3

Elementi RtmData, izvedena dejanja in opredelitve

(1) Element podatkov RTM	(2) Dejanje, ki ga izvede VU		(3) opredelitev podatkov ASN.1
RTM1 **registracijska tablica vozila**	VU nastavi vrednost podatkovnega elementa RTM1 *tp15638VehicleRegistrationPlate* iz zapisane vrednosti podatkovnega tipa *Vehicle-RegistrationIdentification*, kot je opredeljen v Dodatku 1 *VehicleRegistrationIdentification*	registracijska tablica vozila (Vehicle Registration Plate) izražena kot zaporedje znakov	tp15638VehicleRegstrationPlate LPN, --registracijska tablica vozila, uvožena iz ISO 14906 z omejitvijo iz EN 15509, ki je ZAPOREDJE, ki vsebuje kodo države, ki ji sledi abecedna oznaka, ki ji sledi številka tablice, ki je vedno 14 oktetov (zapolnjena z ničlami), tako da je dolžina tipa EN 15509 LPN vedno 17 oktetov, od katerih 14 predstavlja „dejansko“ številko tablice.
RTM2 **Dogodek prekoračitve hitrosti (Speeding Event)**	VU ustvari Boolovo vrednost za podatkovni element RTM2 tp15638SpeedingEvent. VU izračuna vrednost tp15638SpeedingEvent iz števila dogodkov prekoračitve hitrosti (Over Speeding Event), zapisanih v VU v zadnjih 10 dneh nastopov dogodkov, kot je opredeljeno v Prilogi 1C.	1 (TRUE) – Označuje nepravilnosti glede hitrosti v zadnjih 10 dneh nastopov dogodkov.	tp15638speedingEvent BOOLEAN,

▼B

(1) Element podatkov RTM	(2) Dejanje, ki ga izvede VU		(3) opredelitev podatkov ASN.1
	Če je v zadnjih 10 dneh nastopov dogodkov vsaj en tp15638SpeedingEvent, se vrednost tp15638SpeedingEvent nastavi na TRUE. ELSE če v zadnjih 10 dneh nastopov dogodkov ni dogodkov, se vrednost tp15638SpeedingEvent nastavi na FALSE.		
RTM3 **Vožnja brez veljavne kartice (Driving without Valid Card)**	VU ustvari Boolovo vrednost za podatkovni element RTM3 tp15638DrivingWithoutValidCard. VU spremenljivki tp15638DrivingWithoutValidCard dodeli vrednost TRUE, če je v podatkih VU v zadnjih 10 dneh nastopov dogodkov zapisan vsaj en dogodek tipa „vožnja brez ustrezne kartice“, kot je opredeljen v Prilogi 1C. ELSE če v zadnjih 10 dneh nastopov dogodkov ni dogodkov, se spremenljivka tp15638DrivingWithoutValidCard nastavi na FALSE.	1 (TRUE) = Označuje uporabo neveljavne kartice	`tp15638DrivingWithoutValidCard` `BOOLEAN,`
RTM4 **Veljavna vozniška kartica (Valid Driver Card)**	VU ustvari Boolovo vrednost za podatkovni element RTM4 tp15638DriverCard na podlagi podatkov, shranjenih v VU in opredeljenih v Dodatku 1. Če ne obstaja veljavna vozniška kartica, VU spremenljivko nastavi na TRUE. ELSE če vozniška kartica obstaja, VU spremenljivko nastavi na FALSE.	0 (FALSE) = Označuje veljavno vozniško kartico.	`tp15638DriverCard` `BOOLEAN,`
RTM5 **Vstavitev kartice med vožnjo (Card Insertion while Driving)**	VU ustvari Boolovo vrednost za podatkovni element RTM5. VU spremenljivki tp15638CardInsertion dodeli vrednost TRUE, če je v podatkih VU v zadnjih 10 dneh nastopov dogodkov zapisan vsaj en dogodek tipa „vstavitev kartice med vožnjo“, kot je opredeljen v Prilogi 1C. ELSE če v zadnjih 10 dneh nastopov dogodkov ni takih dogodkov, se spremenljivka tp15638CardInsertion nastavi na FALSE.	1 (TRUE) = Označuje vstavitev kartice med vožnjo v zadnjih 10 dneh nastopov dogodkov.	`tp15638CardInsertion` `BOOLEAN,`
RTM6 **Napaka v podatkih o gibanju (Motion Data Error)**	VU ustvari Boolovo vrednost za element RTM6. VU spremenljivki tp15638MotionDataError dodeli vrednost TRUE, če je v podatkih VU v zadnjih 10 dneh nastopov dogodkov zapisan vsaj en dogodek tipa „napaka v podatkih o gibanju“, kot je opredeljen v Prilogi 1C. ELSE če v zadnjih 10 dneh nastopov dogodkov ni takih dogodkov, se spremenljivka tp15638MotionDataError nastavi na FALSE.	1 (TRUE) = Označuje napako v podatkih o gibanju v zadnjih 10 dneh nastopov dogodkov.	`tp15638motionDataError` `BOOLEAN,`

▼B

(1) Element podatkov RTM	(2) Dejanje, ki ga izvede VU		(3) opredelitev podatkov ASN.1
RTM7 **Navzkrižje glede gibanja vozila (Vehicle Motion Conflict)**	VU ustvari Boolovo vrednost za podatkovni element RTM7. VU spremenljivki tp15638vehicleMotionConflict dodeli vrednost TRUE, če je v podatkih VU v zadnjih 10 dneh nastopov zapisan vsaj en dogodek tipa „navzkrižje glede gibanja vozila“ (vrednost ‘0A’H). ELSE če v zadnjih 10 dneh nastopov dogodkov ni dogodkov, se spremenljivka tp15638VehicleMotionConflict nastavi na FALSE.	1 (TRUE) = Označuje navzkrižje glede gibanja vozila v zadnjih 10 dneh nastopov dogodkov.	`tp15638vehicleMotionConflict` `BOOLEAN,`
RTM8 **Druga vozniška kartica (2nd Driver Card)**	VU ustvari Boolovo vrednost za podatkovni element RTM8 na podlagi Priloge 1C („podatki o voznikovi dejavnosti“ CREW in CO-DRIVER). Če v VU obstaja druga veljavna vozniška kartica, VU vrednost nastavi na TRUE. ELSE če druga vozniška kartica ne obstaja, VU spremenljivko nastavi na FALSE.	1 (TRUE) = Označuje, da je vstavljena druga vozniška kartica.	`tp156382ndDriverCard BOOLEAN,`
RTM9 **Tekoča dejavnost (Current Activity)**	VU ustvari Boolovo vrednost za podatkovni element RTM9. Če je tekoča dejavnost v VU zapisana kot dejavnost, ki ni „DRIVING“, kot je opredeljeno v Prilogi 1C, VU spremenljivko nastavi na TRUE. ELSE če je tekoča dejavnost v VU zapisana kot „DRIVING“, VU spremenljivko nastavi na FALSE.	1 (TRUE) = izbrana je druga dejavnost; 0 (FALSE) = izbrana je vožnja.	`tp15638currentActivityDriving` `BOOLEAN`
RTM10 **Zadnja seja zaključena (Last Session Closed)**	VU ustvari Boolovo vrednost za podatkovni element RTM10. Če zadnja seja s kartico ni bila pravilno zaključena, kot je opredeljeno v Prilogi 1C, VU spremenljivko nastavi na TRUE. ELSE če je bila zadnja seja s kartico pravilno zaključena, VU spremenljivko nastavi na FALSE.	1 (TRUE) = nepravilno zaključena, 0 (FALSE) = pravilno zaključena.	`tp15638lastSessionClosed` `BOOLEAN`
RTM11 **Izpad napajanja**	VU ustvari celoštevilsko vrednost za podatkovni element RTM11. VU spremenljivki tp15638PowerSupplyInterruption dodeli vrednost, ki je enaka najdaljši prekinitvi napajanja v skladu s členom 9 Uredbe (EU) št. 165/2014 tipa „izpad napajanja“, kot je opredeljena v Prilogi 1C.	— Število izpadov napajanja v zadnjih 10 dneh nastopov dogodkov.	`tp15638powerSupplyInterruption` `INTEGER (0..127),`

▼B

(1) Element podatkov RTM	(2) Dejanje, ki ga izvede VU		(3) opredelitev podatkov ASN.1
	ELSE če v zadnjih 10 dneh nastopov dogodkov ni bilo dogodkov izpada napajanja, se celoštevilčna vrednost nastavi na 0.		
RTM12 **Napaka na tipalu**	VU ustvari celoštevilčno vrednost za podatkovni element RTM12. VU spremenljivki sensorFault dodeli vrednost: — 1 če je bil v zadnjih 10 dneh zabeležen dogodek tipa napaka na tipalu ‘35’ H; — 2 če je bil v zadnjih 10 dneh zabeležen dogodek tipa „napaka na GNSS sprejemniku“ (notranja ali zunanja z vrednostjo enum ‘51’H ali ‘52’H; — 3 če je bil v zadnjih 10 dneh nastopov dogodkov zapisan dogodek tipa ‘53’H „napaka v zunanji komunikaciji GNSS“; — 4 če sta bila v zadnjih 10 dneh nastopov dogodkov zapisana „napaka na tipalu“ in „napaka GNSS sprejemnika“; — 5 če sta bila v zadnjih 10 dneh nastopov dogodkov zapisana „napaka na tipalu“ in „napaka v zunanji komunikaciji GNSS“; — 6 če sta bila v zadnjih 10 dneh nastopov dogodkov zapisana „napaka GNSS sprejemnika“ in „napaka v zunanji komunikaciji GNSS“; — 7 če so bile v zadnjih 10 dneh nastopov dogodkov zapisane vse tri napake na tipalu. ELSE dodeli vrednost 0, če v zadnjih 10 dneh nastopov dogodkov ni bilo zapisanih nobenih dogodkov.	— – Napaka na tipalu, en oktet v skladu s slovarjem podatkov.	`tp15638SensorFault INTEGER (0..255),`
RTM13 **Nastavljanje časa (Time Adjustment)**	VU ustvari celoštevilsko vrednost (timeReal iz Dodatka 1) za podatkovni element RTM13 na podlagi obstoja podatkov „nastavitev časa“, kot so opredeljeni v Prilogi 1C. VU dodeli vrednost časa, v katerem je nastopil zadnji dogodek nastavljanja časa. ELSE če v podatkih VU ne obstaja dogodek „nastavitev časa“, kot je opredeljen v Prilogi 1C, VU nastavi vrednost na 0.	Čas zadnjega nastavljanja časa.	`tp15638TimeAdjustment INTEGER(0..4294967295),`
RTM14 **Poskus kršenja varnosti (Security Breach Attempt)**	VU ustvari celoštevilsko vrednost (timeReal iz Dodatka 1) za podatkovni element RTM14 na podlagi obstoja dogodka „poskus kršenja varnosti“, kot je opredeljen v Prilogi 1C. VU nastavi vrednost časa zadnjega dogodka poskusa kršenja varnosti, zapisanega v VU.	Čas zadnjega poskusa kršenja varnosti. — privzeta vrednost = 0x00FF	`tp15638LatestBreachAttempt INTEGER(0..4294967295),`

▼B

(1) Element podatkov RTM	(2) Dejanje, ki ga izvede VU		(3) opredelitev podatkov ASN.1
	ELSE če v podatkih VU ne obstaja dogodek „poskus kršenja varnosti“, kot je opredeljen v Prilogi 1C, VU nastavi vrednost na 0x00FF.		
RTM15 **Zadnja kalibracija (Last Calibration)**	VU ustvari celoštevilsko vrednost (timeReal iz Dodatka 1) za podatkovni element RTM15 na podlagi obstoja podatkov „zadnja kalibracija“, kot so opredeljeni v Prilogi 1C. VU nastavi vrednost časa zadnjih dveh kalibracij (RTM15 in RTM16), ki sta nastavljeni v VuCalibrationData, kot je opredeljena v Dodatku 1. VU nastavi vrednost za RTM15 na timeReal zadnjega kalibracijskega zapisa.	Čas zadnjih podatkov o kalibraciji.	`tp15638LastCalibrationData` `INTEGER(0..4294967295),`
RTM16 **Prejšnja kalibracija (Previous Calibration)**	VU ustvari celoštevilčno vrednost (timeReal iz Dodatka 1) za podatkovni element RTM16 kalibracijskega zapisa, ki je bil izveden pred zadnjo kalibracijo. ELSE če prej ni bilo nobene kalibracije, VU vrednost RTM16 nastavi na 0.	Čas podatkov prejšnje kalibracije.	`tp15638PrevCalibrationData` `INTEGER(0..4294967295),`
RTM17 **Datum povezave tahografa (Date Tachograph Connected).**	VU za podatkovni element RTM17 ustvari celoštevilčno vrednost (timeReal iz dodatka 1). VU nastavi vrednost časa začetne namestitve VU. VU te podatke pridobi iz VuCalibrationData (Dodatek 1) iz vuCalibrationRecords, pri čemer je CalibrationPurpose enaka ‘03’H.	Datum povezave tahografa.	`tp15638DateTachoConnected` `INTEGER(0..4294967295),`
RTM18 **Trenutna hitrost (Current Speed)**	VU ustvari celoštevilsko vrednost za podatkovni element RTM18. VU nastavi vrednost za RTM16 na zadnjo zapisano trenutno hitrost v času zadnje posodobitve RtmData.	Zadnja zapisana trenutna hitrost.	`tp15638CurrentSpeed` `INTEGER (0..255),`
RTM19 **Časovni žig (Timestamp)**	VU za podatkovni element RTM19 ustvari celoštevilčno vrednost (timeReal iz Dodatka 1). VU nastavi vrednost za RTM19 na čas zadnje posodobitve RtmData.	Časovni žig tekočega zapisa TachographPayload.	`tp15638Timestamp` `INTEGER(0..4294967295),`

5.4.6 *Mehanizem za prenos podatkov*

DSC_42 REDCR zahteva predhodno opredeljene koristne podatke po fazi inicializacije, nato pa jih *DSRC-VU* posreduje v dodeljenem oknu. REDCR za pridobivanje podatkov uporabi ukaz GET.

▼B

DSC_43 Pri vseh izmenjavah DSRC se podatki kodirajo z uporabo PER (Packed Encoding Rules).

5.4.7 *Podroben opis transakcije DSRC*

DSC_44 Inicializacija se izvede v skladu z DSC_44 – DSC_48 in tabelami 14.4 – 14.9. V fazi inicializacije REDCR začne tako, da pošlje okvir z BST („tabela storitev signala oddajnika“, Beacon Service Table) v skladu s standardom EN 12834 in oddelki 6.2, 6.3, 6.4 ter 7.1 standarda EN 13372, z nastavitvami, kot so navedene v tabeli 14.4.

Tabela 14.4

Inicializacija – nastavitve okvira BST

Polje	Nastavitve
Identifikator povezave	naslov pošiljanja
BeaconId	v skladu z EN 12834
Čas	v skladu z EN 12834
Profil	Brez razširitve, uporabi se 0 ali 1.
MandApplications	Brez razširitve, EID ne obstaja, parameter ne obstaja, AID= 2 Freight&Fleet
NonMandApplications	ne obstajajo
ProfileList	brez razširitve, število profilov na seznamu = 0
Fragmentacijska glava	brez fragmentiranja
nastavitve plasti 2	ukazna PDU, ukaz UI

Praktičen primer nastavitev iz tabele 14.4 z navedbo bitnega kodiranja je v tabeli 14.5.

Tabela 14.5

Inicializacija – primer vsebine okvira BST

Oktet #	Atribut/polje	Biti v oktetu	Opis
1	FLAG	0111 1110	začetna zastavica
2	Broadcast ID	1111 1111	naslov pošiljanja
3	MAC Control Field	1010 0000	ukazna PDU
4	LLC Control field	0000 0011	ukaz UI

▼B

Oktet #	Atribut/polje	Biti v oktetu	Opis
5	Fragmentation header	1xxx x001	brez fragmentiranja
6	BST	1000	zahtevek za inicializacijo
	SEQUENCE {		
	OPTION indicator BeaconID SEQUENCE { ManufacturerId INTEGER (0..65535)	0	NonMand aplikacije ne obstajajo
		xxx	Indentifikator proizvajalca
7		xxxx xxxx	
8		xxxx x	
	IndividualID INTEGER (0..134217727)	xxx	27 bit ID na razpolago za proizvajalca
9		xxxx xxxx	
10		xxxx xxxx	
11	}	xxxx xxxx	
12	Time INTEGER (0..4294967295)	xxxx xxxx	32 bitni realni čas UNIX
13		xxxx xxxx	
14		xxxx xxxx	
15		xxxx xxxx	
16	Profile INTEGER (0..127,...)	0000 0000	brez razširitve primer profila 0
17	MandApplications SEQUENCE (SIZE(0..127,...)) OF {	0000 0001	brez razširitve, število mandApplications = 1
18	SEQUENCE {		
	OPTION indicator	0	EID ne obstaja.
	OPTION indicator	0	Parameter ne obstaja.
	AID DSRCApplicationEntityID } }	00 0010	brez razširitve AID= 2 Freight&Fleet

▼B

Oktet #	Atribut/polje	Biti v oktetu	Opis
19	ProfileList SEQUENCE (0..127,...) OF Profile }	0000 0000	Brez razširitve, število profilov na seznamu = 0.
20	FCS	xxxx xxxx	zaporedje preveritve okvira
21		xxxx xxxx	
22	Flag	0111 1110	zaključna zastavica

DSC_45 *DSRC-VU* med prejemom BST zahteva dodelitev zasebnega okna v skladu s standardom EN 12795 in oddelkom 7.1.1 standarda EN 13372, brez posebnih nastavitev RTM. V tabeli 14.6 je primer bitnega kodiranja.

Tabela 14.6

Inicializacija – vsebina okvira zahtevka za dodelitev zasebnega okna

Oktet #	Atribut/polje	Biti v oktetu	Opis
1	FLAG	0111 1110	začetna zastavica
2	Private LID	xxxx xxxx	naslov povezave posebne DSRC-VU
3		xxxx xxxx	
4		xxxx xxxx	
5		xxxx xxxx	
6	MAC Control field	0110 0000	zahtevek za zasebno okno
7	FCS	xxxx xxxx	zaporedje preveritve okvira
8		xxxx xxxx	
9	Flag	0111 1110	zaključna zastavica

DSC_46 REDCR nato odgovori z dodelitvijo zasebnega okna v skladu s standardom EN 12795 in oddelkom 7.1.1 standarda EN 13372 brez posebnih nastavitev RTM.

V tabeli 14.7 je primer bitnega kodiranja.

Tabela 14.7

Inicializacija – Vsebina okvira dodelitve zasebnega okna

Oktet #	Atribut/polje	Biti v oktetu	Opis
1	FLAG	0111 1110	začetna zastavica
2	Private LID	xxxx xxxx	naslov povezave določene DSRC-VU
3		xxxx xxxx	

▼B

Oktet #	Atribut/polje	Biti v oktetu	Opis
4		xxxx xxxx	
5		xxxx xxxx	
6	MAC Control field	0010 s000	dodelitev zasebnega okna
7	FCS	xxxx xxxx	zaporedje preveritve okvira
8		xxxx xxxx	
9	Flag	0111 1110	End Flag

DSC_47 *DSRC-VU*, ob prejemu dodelitve zasebnega okna pošlje svojo VST („tabelo storitev vozila“, Vehicle Service Table) v skladu s standardom EN 12834 in oddelki 6.2, 6.3, 6.4 in 7.1 standarda EN 13372, z nastavitvami, kot so navedene v tabeli 14.8, ob uporabi dodeljenega okna za prenos.

Tabela 14.8

Inicializacija – nastavitve okvira VST

Polje	Nastavitve
Private LID	v skladu s standardom EN 12834
Parametri VST	Fill=0, nato za vsako podprto aplikacijo: EID obstaja, parameter obstaja, AID=2, EID, kot ga je ustvarila OBU
Parameter	brez razširitve, vsebuje oznako konteksta RTM
Konfiguracija Obe	Lahko obstaja neobvezno polje ObeStatus, vendar ga REDCR ne uporablja.
Fragmentacijska glava	brez fragmentiranja
Nastavitve plasti 2	ukazna PDU, ukaz UI

DSC_48 *DSRC-VU* podpira aplikacijo „Freight and Fleet“, ki se identificira z identifikatorjem aplikacije ‘2’. Lahko so podprti tudi drugi identifikatorji aplikacije, vendar v tej VST ne obstajajo, saj BST zahteva samo AID = 2. Polje „Aplikacije“ vsebuje seznam podprtih konkretizacij aplikacije v *DSRC-VU* Za vsako podprto konkretizacijo aplikacije je naveden sklic na ustrezni standard, narejen iz oznake Rtm Context, ki je sestavljena iz identifikatorja objekta, ki predstavlja povezani standard, njegov del (9 za RTM) in morebitno verzijo, ter EID, ki ga ustvari DSRC-VU in je povezan s to konkretizacijo aplikacije.

Praktičen primer nastavitev iz tabele 14.8 z navedbo bitnega kodiranja je v tabeli 14.9.

▼B

Tabela 14.9

Inicializacija – primer vsebine okvira VST

Oktet #	Atribut/polje	Biti v oktetu	Opis
1	FLAG	0111 1110	začetna zastavica
2	Private LID	xxxx xxxx	naslov povezave določene DSRC-VU
3		xxxx xxxx	
4		xxxx xxxx	
5		xxxx xxxx	
6	MAC Control field	1100 0000	ukazna PDU
7	LLC Control field	0000 0011	ukaz UI
8	Fragmentation header	1xxx x001	brez fragmentiranja
9	VST SEQUENCE {	1001	odgovor na inicializacijo
	Fill BIT STRING (SIZE(4))	0000	neuporabljeno in nastavljeno na 0
10	Profile INTEGER (0..127,…) Applications SEQUENCE OF {	0000 0000	Brez razširitve. Primer profila 0.
11		0000 0001	Brez razširitve, 1 aplikacija.
12	SEQUENCE {		
	OPTION indicator	1	EID obstaja.
	OPTION indicator	1	Parameter obstaja.
	AID DSRCApplicationEntityID	00 0010	Brez razširitve. AID= 2 Freight&Fleet
13	EID Dsrc-EID	xxxx xxxx	Opredeljen v OBU in določa instanco aplikacije.
14	Parameter Container {	0000 0010	Brez razširitve, izbira vsebnika = 02, Oktetni niz.
15		0000 1000	Brez razširitve, dolžina oznake konteksta RTM = 8.

▼B

Oktet #	Atribut/polje	Biti v oktetu	Opis
16	Rtm-ContextMark::= SEQUENCE {	0000 0110	identifikator objekta podprtega standarda, dela in različice Primer: ISO (1) standard (0) TARV (15638) del9(9) različica1 (1). Prvi oktet je 06H, to je identifikator objekta; drugi oktet je 06H, to je njegova dolžina. V naslednjih 6 oktetih je kodiran identifikator objekta iz primera. Opozorilo: obstaja samo en element zaporedja (neobvezni element RtmCommProfile je izpuščen).
17	StandardIdentifier standardIdentifier	0000 0110	
18		0010 1000	
19		1000 0000	
20		1111 1010	
21		0001 0110	
22		0000 1001	
23		0000 0001	
24	ObeConfiguration Sequence {		
	OPTION indicator	0	ObeStatus ne obstaja
	EquipmentClass INTEGER (0..32767)	xxx xxxx	
25		xxxx xxxx	
26	ManufacturerId INTEGER (0..65535)	xxxx xxxx	identifikator proizvajalca za DSRC-VU, kot je opisan v registru standarda ISO 14816
27		xxxx xxxx	
28	FCS	xxxx xxxx	zaporedje preveritve okvira
29		xxxx xxxx	
30	Flag	0111 1110	zaključna zastavica

DCS_49 REDCR nato prebere podatke z ukazom GET, ki je skladen z ukazom GET, opredeljenim v oddelkih 6.2, 6.3 in 6.4 standarda EN 13372 ter standardu EN 12834, z nastavitvami, kot so navedene v tabeli 14.10.

Tabela 14.10

Predstavitev – nastavitve okvira zahtevka GET

Polje	Nastavitve
Invoker Identifier (IID)	ne obstaja
Link Identifier (LID)	naslov povezave določene DSRC-VU
Chaining	ne
Element Identifier (EID)	kot je naveden v VST Brez razširitve.

▼B

Polje	Nastavitve
Access Credentials	ne
AttributeIdList	Brez razširitve, 1 atribut, AttributeID = 1 (RtmData).
Fragmentation	ne
Layer2 settings	ukazna PDU, pozivni ukaz ACn

V Tabeli 14.11 je prikazan primer branja podatkov RTM.

Tabela 14.11

Predstavitev – primer okvira Get Request

Oktet #	Atribut/polje	Biti v oktetu	Opis
1	FLAG	0111 1110	začetna zastavica
2	Private LID	xxxx xxxx	naslov povezave določene DSRC-VU
3		xxxx xxxx	
4		xxxx xxxx	
5		xxxx xxxx	
6	MAC Control field	1010 s000	ukazna PDU
7	LLC Control field	n111 0111	pozivni ukaz ACn, n bitni
8	Fragmentation header	1xxx x001	brez fragmentiranja
9	Get.request SEQUENCE {	0110	Pridobi zahtevo.
	OPTION indicator	0	Poverilnice za dostop ne obstajajo.
	OPTION indicator	0	IID ne obstaja.
	OPTION indicator	1	AttributeIdList obstaja.
	Fill BIT STRING(SIZE(1))	0	Nastavi na 0.
10	EID INTEGER(0..127,…)	xxxx xxxx	EID konkretizacije aplikacije RTM, kot je naveden v VST Brez razširitve.
11	AttributeIdList SEQUENCE OF { AttributeId }}	0000 0001	Brez razširitve, število atributov = 1.
12		0000 0001	AttributeId=1, RtmData. Brez razširitve.
13	FCS	xxxx xxxx	zaporedje preveritve okvira
14		xxxx xxxx	
15	Flag	0111 1110	zaključna zastavica

▼B

DSC_50 *DSRC-VU* ob prejemu zahtevka GET pošlje odgovor GET z zahtevanimi podatki, ki so v skladu z odgovorom GET, opredeljenim v oddelkih 6.2, 6.3 in 6.4 standarda EN 13372 ter standardu EN 12834, z nastavitvami, kot so navedene v tabeli 14.12.

Tabela 14.12

Predstavitev – nastavitve okvira odgovora GET

Polje	Nastavitve
Invoker Identifier (IID)	ne obstaja
Link Identifier (LID)	v skladu z EN 12834
Chaining	ne
Element Identifier (EID)	kot je naveden v VST
Access Credentials	ne
Fragmentation	ne
Layer2 settings	PDU za odgovor, odgovor na razpolago in ukaz sprejet, ukaz ACn.

V Tabeli 14.13 je prikazan primer branja podatkov RTM.

Tabela 14.13

Predstavitev – primer vsebine okvira odgovora

Oktet #	Atribut/polje	Biti v oktetu	Opis
1	FLAG	0111 1110	začetna zastavica
2	Private LID	xxxx xxxx	naslov povezave določene DSRC-VU
3		xxxx xxxx	
4		xxxx xxxx	
5		xxxx xxxx	
6	MAC Control field	1101 0000	PDU za odgovor
7	LLC Control field	n111 0111	odgovor na razpolago, ukaz ACn n-bitni
8	LLC Status field	0000 0000	odgovor na razpolago in ukaz sprejet
9	Fragmentation header	1xxx x001	brez fragmentiranja
10	Get.response SEQUENCE {	0111	Pridobi odgovor.

▼B

Oktet #	Atribut/polje	Biti v oktetu	Opis
	OPTION indicator	0	IID ne obstaja.
	OPTION indicator	1	Seznam atributov obstaja.
	OPTION indicator	0	Povratni status ne obstaja.
	Fill BIT STRING(SIZE(1))	0	Ni uporabljeno.
11	EID INTEGER(0..127,…)	xxxx xxxx	Odgovor konkretizacije aplikacije RTM. Brez razširitve.
12	AttributeList SEQUENCE OF {	0000 0001	Brez razširitve, število atributov = 1.
13	Attributes SEQUENCE { AttributeId	0000 0001	Brez razširitve, AttributeId=1 (RtmData).
14	AttributeValue CONTAINER {	0000 1010	Brez razširitve, izbira vsebnika = 10_{10}.
15		kkkk kkkk	RtmData
16		kkkk kkkk	
17		kkkk kkkk	
…		…	
n	}}}}	kkkk kkkk	
n+1	FCS	xxxx xxxx	zaporedje preveritve okvira
n+2		xxxx xxxx	
n+3	Flag	0111 1110	zaključna zastavica

DSC_51 REDCR nato zaključi povezavo z ukazom EVENT_REPORT, RELEASE, ki je v skladu s točkami 6.2, 6.3 in 6.4 standardaEN 13372 ter oddelek 7.3.8 standarda EN 12834, brez posebnih nastavitev RTM. V tabeli 14.14 je prikazan primer bitnega kodiranja primera ukaza RELEASE.

Tabela 14.14

Prekinitev. Vsebina okvira EVENT_REPORT RELEASE

Oktet #	Atribut/polje	Biti v oktetu	Opis
1	FLAG	0111 1110	začetna zastavica
2	Private LID	xxxx xxxx	naslov povezave določene DSRC-VU
3		xxxx xxxx	
4		xxxx xxxx	

▼B

Oktet #	Atribut/polje	Biti v oktetu	Opis
5		xxxx xxxx	
6	MAC Control field	1000 s000	Okvir vsebuje ukazno LPDU.
7	LLC Control field	0000 0011	ukaz UI
8	Fragmentation header	1xxx x001	brez fragmentiranja
9	EVENT_REPORT.request SEQUENCE {	0010	EVENT_REPORT (Release)
	OPTION indicator	0	Poverilnice za dostop ne obstajajo.
	OPTION indicator	0	Parameter dogodka ne obstaja.
	OPTION indicator	0	IID ne obstaja.
	Mode BOOLEAN	0	Ne pričakuje se odgovor.
10	EID INTEGER (0..127,…)	0000 0000	Brez razširitve, EID = 0 (sistem).
11	EventType INTEGER (0..127,…) }	0000 0000	Tip dogodka 0 = Release
12	FCS	xxxx xxxx	zaporedje preveritve okvira
13		xxxx xxxx	
14	Flag	0111 1110	zaključna zastavica

DSC_52 Ni predvideno, da bi *DSRC-VU* odgovoril na ukaz Release. Komunikacija je zaključena.

5.4.8 *Opis preskusne transakcije DSRC*

DSC_53 Opraviti je treba celotne preskuse, vključno z zaščito podatkov, kot je opredeljeno v Dodatku 11, Skupni varnostni mehanizmi, in sicer jih morajo opraviti pooblaščene osebe, ki imajo dostop do postopkov zaščite, z običajnim ukazom GET, kot je opredeljeno zgoraj.

DSC_54 Naročanje in redni kontrolni pregledi, pri katerih je potrebno dešifriranje in razumevanje dešifriranih podatkov, se izvede, kot je navedeno v Dodatku 11, Skupni varnostni mehanizmi, in dodatku 9, Homologacijski seznam minimalnih potrebnih preskusov.

Vendar pa je osnovno komunikacijo DSRC mogoče preizkusiti z ukazom ECHO. Taki preskusi se lahko zahtevajo pri naročilu, ob rednem kontrolnem pregledu ali tudi sicer, če tako zahteva pristojni nadzorni organ ali Uredba (EU) št. 165/2014 (glej oddelek 6).

▼B

DSC_55 Za izvedbo osnovnega preskusa komunikacije REDCR da ukaz ECHO med sejo, t.j. po uspešno končani fazi inicializacije. Zaporedje interakcij je podobno zaporedju pri poizvedbi:

— Korak 1 *REDCR* pošlje „tabelo storitev signala oddajnika“ (BST), ki vsebuje tudi identifikatorje aplikacije (AID) v seznamu storitev, ki ga podpira. V aplikacijah RTM bo to preprosto storitev z vrednostjo AID = 2.

DSRC-VU preveri prejeto BST in, kjer ugotovi, da BST zahteva Freight&Fleet (AID = 2), *DSRC-VU* odgovori. Če *REDCR* ne ponudi AID = 2, *DSRC-VU* zaključi transakcijo z *REDCR*.

— Korak 2 *DSRC-VU* pošlje zahtevek za dodelitev zasebnega okna.

— Korak 3 *REDCR* pošlje dodelitev zasebnega okna.

— Korak 4 *DSRC-VU* v dodeljenem zasebnem oknu pošlje svojo tabelo storitev vozila (VST). Ta VST vsebuje seznam vseh različnih konkretizacij aplikacije, ki jih ta *DSRC-VU* podpira v sklopu AID=2. Različne konkretizacije so določene s pomočjo edinstvenih EID, vsaka je povezana z vrednostjo parametra, ki označuje podprto konkretizacijo aplikacije in standard.

— Korak 5 *REDCR* nato analizira ponujeno VST, nato pa ali prekine zvezo (RELEASE), ker ga ne zanima nič od tistega, kar nudi VST (tj. prejema VST od *DSRC-VU*, ki ni RTM VU), ali, če prejme ustrezno VST, začne konkretizacijo aplikacije.

— Korak 6 *REDCR* da ukaz (ECHO) določeni *DSRC-VU* in dodeli zasebno okno.

— Korak 7 *DSRC-VU* v pravkar dodeljenem zasebnem oknu pošlje okvir odgovora ECHO.

V tabelah spodaj je praktično prikazana seja izmenjave zahtevka ECHO.

DSC_56 Inicializacija se izvede v skladu z oddelkkom 5.4.7 DSC_44 – DSC_48 in tabelami 14.4 – 14.9.

DSC_57 REDCR nato da ukaz ACTION, ECHO v skladu s standardom ISO 14906, ki vsebuje 100 oktetov podatkov brez posebnih nastavitev za RTM. V tabeli 14.15 je prikazana vsebina okvira, ki ga pošlje REDCR.

▼B

Tabela 14.15

Primer okvira z ukazom ACTION, ECHO

Oktet #	Atribut/polje	Biti v oktetu	Opis
1	FLAG	0111 1110	začetna zastavica
2	Private LID	xxxx xxxx	naslov povezave določene DSRC-VU
3		xxxx xxxx	
4		xxxx xxxx	
5		xxxx xxxx	
6	MAC Control field	1010 s000	ukazna PDU
7	LLC Control field	n111 0111	pozivni ukaz ACn, n bitni
8	Fragmentation header	1xxx x001	brez fragmentiranja
9	ACTION.request SEQUENCE {	0000	zahtevek za dejanje (ECHO)
	OPTION indicator	0	Poverilnice za dostop ne obstajajo.
	OPTION indicator	1	Parameter dejanja obstaja.
	OPTION indicator	0	IID ne obstaja.
	Mode BOOLEAN	1	Pričakuje se odgovor.
10	EID INTEGER (0..127,…)	0000 0000	Brez razširitve, EID = 0 (sistem).
11	ActionType INTEGER (0..127,…)	0000 1111	Brez razširitve, tip dejanja je zahtevek ECHO.
12	ActionParameter CONTAINER {	0000 0010	Brez razširitve, izbor vsebnika = 2.
13		0110 0100	Brez razširitve. Dolžina niza = 100 oktetov.
14		xxxx xxxx	podatki za prikaz
…		…	
113	}}	xxxx xxxx	
114	FCS	xxxx xxxx	zaporedje preveritve okvira
115		xxxx xxxx	
116	Flag	0111 1110	zaključna zastavica

▼B

DSC_58 *DSRC-VU* ob prejemu zahtevka ECHO pošlje odgovor ECHO v obsegu 100 oktetov podatkov kot odraz prejetega ukaza v skladu s standardom ISO 14906 brez posebnih nastavitev za RTM. V tabeli 14.16 je prikazan primer kodiranja na bitni ravni.

Tabela 14.16

Primer okvira z odgovorom ACTION, ECHO

Oktet #	Atribut/polje	Biti v oktetu	Opis
1	FLAG	0111 1110	začetna zastavica
2	Private LID	xxxx xxxx	naslov povezave določene VU
3		xxxx xxxx	
4		xxxx xxxx	
5		xxxx xxxx	
6	MAC Control field	1101 0000	PDU za odgovor
7	LLC Control field	n111 0111	ukaz ACn, n-bitni
8	LLC status field	0000 0000	Na razpolago je odgovor.
9	Fragmentation header	1xxx x001	brez fragmentiranja
10	ACTION.response SEQUENCE {	0001	odgovor ACTION (ECHO)
	OPTION indicator	0	IID ne obstaja.
	OPTION indicator	1	Parameter za odgovor obstaja.
	OPTION indicator	0	Povratni status ne obstaja.
	Fill BIT STRING (SIZE (1))	0	Ni uporabljeno.
11	EID INTEGER (0..127,…)	0000 0000	Brez razširitve, EID = 0 (sistem)
12	ResponseParameter CONTAINER {	0000 0010	Brez razširitve, izbor vsebnika = 2.
13		0110 0100	Brez razširitve. Dolžina niza = 100 oktetov.
14		xxxx xxxx	prikazani podatki
…		…	
113	}}	xxxx xxxx	
114	FCS	xxxx xxxx	zaporedje preveritve okvira
115		xxxx xxxx	
116	Flag	0111 1110	zaključna zastavica

▼B

5.5 **Podpora za Direktivo 2015/71/EU**

5.5.1 *Pregled*

DSC_59 Za podporo za Direktivo 2015/719/ES o največji teži in dimenzijah težkih tovornih vozil bo protokol transakcije za prenos podatkov OWS preko povezave z vmesnikom 5,8 GHz DSRC enak kot protokol za podatke RTM (glej 5.4.1) z edino razliko, da se bo z identifikatorjem objekta, ki se nanaša na standard TARV, naslavljal del 20 standarda ISO 15638 (TARV), ki se nanaša na WOB/OWS.

5.5.2 *Ukazi*

DSC_60 Ukazi za transakcijo OWS bodo enaki kot ukazi za transakcijo RTM.

5.5.3 *Zaporedje ukazov pri poizvedbi*

DSC_61 Zaporedje ukazov pri poizvedbi bo za podatke OWS enako kot za podatke RTM.

5.5.4 *Strukture podatkov*

DSC_62 Koristni podatki (podatki OWS) so sestavljeni iz združitve

1. podatkov EncryptedOwsPayload, ki so šifrirani podatki OwsPayload, opredeljeni v ASN.1 v oddelku 5.5.5. Metoda šifriranja je enaka kot metoda za RtmData, ki je navedena v Dodatku 11.

2. DSRCSecurityData, izračunano z istimi algoritmi kot so algoritmi za RtmData, ki so navedeni v Dodatku 11.

▼B

5.5.5 *Modul ASN.1 za transakcijo OWS DSRC*

DSC_63 Opredelitev modula ASN.1 za podatke DSRC znotraj aplikacije RTM se opredeli:

```
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 OwsData, izvedena dejanja in opredelitve*

Elementi OwsData so opredeljeni tako, da podpirajo Direktivo 2015/719/ES o največji teži in dimenzijah težkih tovornih vozil. Njihov pomen:

— recordedWeight pomeni celotno izmerjeno težo težkega tovornega vozila z natančnostjo 10 kg, kot je opredeljeno v standardu EN ISO 14906. Npr. vrednost 2 500 pomeni težo 25 ton;

— axlesConfiguration pomeni konfiguracijo težkega tovornega vozila glede števila osi. Konfiguracija je opredeljena z bitno masko dolžine 20 bitov (razširjeno iz standarda EN ISO 14906).

Bitna maska 2 bitov predstavlja konfiguracijo osi z naslednjim formatom::

— Vrednost 00B pomeni, da vrednost „ni na razpolago“, ker vozilo nima opreme za zbiranje podatkov o teži na osi.

— Vrednost 01B pomeni, da os ne obstaja.

— Vrednost 10B pomeni, da os obstaja, da je bil podatek o teži izračunan in zbran ter je naveden v polju axlesRecordedWeight.

— Vrednost 11B je rezervirana za prihodnje možnosti uporabe.

Zadnji 4 biti so rezervirani za prihodnje možnosti uporabe.

Število osi										
Število osi na vlačilcu			Število osi na priklopniku							
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 biti)

— axlesRecordedWeight predstavlja določeno težo, zapisano za vsako os, z natančnostjo 10 kg. Za vsako os se uporabljata dva okteta. Npr. vrednost 150 pomeni težo 1 500 kg;

Drugi podatkovni tipi so opredeljeni v 5.4.5.

5.5.7 *Mehanizem za prenos podatkov*

DSC_64 Mehanizem za prenos podatkov za podatke OWS med poizvedovalnikom in napravo DSRC v vozilu je isti kot za podatke RTM (glej 5.4.6).

DSC_65 Prenos podatkov med platformo, ki zbira podatke o največji teži, in napravo DSRC v vozilu temelji na fizični povezavi, vmesnikih in protokolih, opredeljenih v oddelku 5.6.

5.6 **Prenos podatkov med DSRC-VU in VU**

5.6.1 *Fizična povezava in vmesniki*

DSC_66 *VU* in *DSRC-VU* sta lahko povezani s fizičnim kablom ali brezžično komunikacijo kratkega dosega, ki temelji na Bluetooth v4.0 BLE.

▼B

DSC_67 Ne glede ne izbiro fizične povezave in vmesnika morajo biti izpolnjeni naslednji elementi:

DSC_68 a) da bi bilo mogoče naročilo za dobavo VU in DSRC-VU, pa tudi različnih serij DSRC-VU, mora biti povezava med VU in DSRC-VU v skladu z odprtimi standardi. Povezava med VU in DSRC-VU mora biti

i) fiksna kabelska povezava dolžine najmanj 2 metrov z ravnim priključkom DIN 41612 H11 – 11 polni odobreni moški priključek iz DSRC-VU z ustreznim podobnim ženskim priključkom na napravi VU;

ii) z uporabo Bluetooth Low Energy (BLE);

iii) s povezavo v skladu s standardom ISO 11898 ali SAE J1939;

DSC_69 b) opredelitev vmesnikov in povezave med VU in DSRC-VU mora podpirati ukaze protokola aplikacije iz oddelka 5.6.2 in

DSC_70 c) VU in DSRC-VU morata podpirati delovanje prenosa podatkov preko povezave glede zmogljivosti in napajanja.

5.6.2 *Protokol aplikacije*

DSC_71 Naloga protokola aplikacije med opremo za komunikacijo na daljavo VU in DSRC-VU je redno prenašanje komunikacije na daljavo od VU do DSRC.

DSC_72 Določeni so naslednji glavni ukazi:

1. inicializacija komunikacijske povezave – zahtevek;

2. inicializacija komunikacijske povezave – odgovor;

3. Send Data („pošlji podatke“) z identifikatorjem aplikacije RTM in koristnimi podatki, opredeljenimi v podatkih RTM;

4. potrditev podatkov;

5. prekinitev komunikacijske povezave – zahtevek;

6. prekinitev komunikacijske povezave – odgovor;

DSC_73 Navedene ukaze je mogoče v ASN1.0 opredeliti kot:

▼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 Opis ukazov in parametrov:

— RCDT-Communication Link Initialization – Request

RCDT-Communication Link Initialization – Request se uporablja za inicializacijo komunikacijske povezave. Ta ukaz VU pošlje DSRC-VU. VU nastavi LinkIdentifier, ki se nato sporoči DSRC-VU, da lahko sledi določeni komunikacijski povezavi.

(Opomba: to je namenjeno podpori bodočih povezav in drugih aplikacij/modulov, kot je „tehtanje v vozilu“.

— RCDT-Communication Link Initialization – Response

RCDT-Communication Link Initialization – Response uporablja DSRC-VU za odgovor na zahtevek za inicializacijo komunikacijske povezave. Ta ukaz DSRC-VU pošlje VU. Ukaz poda izid inicializacije kot odgovor = 1 (uspešna) ali =0 (neuspešna).

DSC_75 Inicializacija komunikacijske povezave se izvede šele po namestitvi, kalibraciji in zagonu motorja / vklopu VU.

▼B

— RCDT-Send Data Z VU pošlje DSRC-VU podpisane podatke RCDTData (tj. *podatke, poslane na daljavo*). Podatki bodo poslani vsakih 60 sekund. Parameter DataTransactionId označuje določen prenos podatkov. Pravilnost ustrezne povezave se zagotavlja tudi z LinkIdentifier.

— RCDT-Data Acknowledgment pošlje DSRC-VU kot povratno informacijo za VU o prejemu podatkov od ukaza RCDT-Send Data, ki ga določi parameter DataTransactionId. Parameter za odgovor je 1 (uspešen) ali =0 (neuspešen). Če VU prejeme več kot tri odgovore, ki so enaki 0, ali če VU ne prejme potrditve podatkov RCDT za določen RCDTR – Send Data, ki je bili poslan s posebno DataTransactionId, VU ustvari dogodek in zapis o njem.

— RCDT-Communication Link Termination request VU pošlje DSRC-VU, da prekine povezavo z določenim LinkIdentifier.

DSC_76 Po ponovnem zagonu DSRC-VU ali VU je treba odstraniti vse obstoječe komunikacijske povezave, saj bi lahko obstajale „obvisele povezave“ zaradi nenadne zaustavitve VU.

— RCDT-Communication Link Termination – Response DSRC-VU pošlje VU kot potrditev zahtevka za prekinitev povezave, ki ga je podala VU za določen LinkIdentifier.

5.7 **Obravnava napak**

5.7.1 *Beleženje in sporočanje podatkov v DSRC-VU*

DSC_77 Funkcija *VUSM podatke*, ki so že zaščiteni, posreduje *DSRC-VU*. *VUSM* preveri, da so bili podatki, ki so bili zapisani v *DSRC-VU*, zapisani pravilno. Zapis napak v prenosu podatkov od *VU* v pomnilnik *DSRC-VU* in poročanje o njih se zapisuje s tipom EventFaultType in nastavitvijo vrednosti enum na ‘62’H, napaka v komunikaciji opreme za komunikacijo na daljavo, skupaj s časovnim žigom.

DSC_78 *VU* za zapis „napak v notranji komunikaciji VU“ vzdržuje datoteko, označeno z edinstvenim imenom, ki ga inšpektorji brez težav ugotovijo.

DSC_79 Če VUPM poskusi pridobiti podatke VU od varnostnega modula (da bi jih posredoval VU-DSRC), vendar ne uspe, ta neuspeh zapiše s tipom EventFaultType in nastavitvijo vrednosti enum na *‘62’H Remote Communication Facility*, napaka v

▼B

komunikaciji, skupaj s časovnim žigom. Neuspešna komunikacija se zazna, če sporočilo `RCDT Data Acknowledgment` več kot trikrat zaporedoma ni prejeto za ustrezne (tj. z isto DataTransactionId v sporočilih `Send Data and Acknowledgment`) `RCDT Send Data`.

5.7.2 *Napake v brezžični komunikaciji*

DSC_80 Obravnava napak v komunikaciji mora biti skladna s povezanimi standardi DSRC, in sicer EN 300 674-1, EN 12253, EN 12795, EN 12834 ter ustreznimi parametri standarda EN 13372.

5.7.2.1 *Napake pri šifriranju in podpisovanju*

DSC_81 Napake pri šifriranju in podpisovanju se obravnavajo, kot je opredeljeno v Dodatku 11, Skupni varnostni mehanizmi, in niso prisotne v sporočilih o napakah, povezanih s prenosom podatkom preko DSRC.

5.7.2.2 *Beleženje napak*

Medij DSRC je dinamična brezžična komunikacija v okolju, ki je negotovo glede atmosferskih pogojev in interferenc, zlasti v kombinacijah „prenosnega REDCR“ in „premikajočega se vozila“, ki nastopajo v tej aplikaciji. Zato je treba ugotoviti razliko med „nebranjem“ in stanjem „napake“. Pri transakciji preko brezžičnega vmesnika je nebranje pogosto, navadno mu sledi ponoven poskus, tj. ponovno oddajanje BST in ponoven poskus vzpostavitve zaporedja, kar večinoma pripelje do uspešne komunikacijske povezave in prenosa podatkov, razen če se ciljno vozilo v času, potrebnem za ponovno oddajanje, premakne iz dosega. (Za „uspešen“ primer branja je bilo morda potrebnih več ponovnih poskusov.)

Vzrok za nebranje je lahko, da anteni nista bili pravilno povezani (napaka pri „nameritvi“); ker je ena od anten zakrita pred signalom – morda namenoma, lahko pa tudi zaradi fizične prisotnosti drugega vozila; radijska interferenca, zlasti od WIFI okrog 5,8 GHz ali drugih javno dostopnih brezžičnih komunikacij, povzroči pa jo lahko tudi radarska interferenca ali težavni atmosferski pogoji (npr. med nevihto); ali preprosto zato, ker se je vozilo premaknilo iz dosega komunikacije z DSRC. Posameznih primerov nebranja zaradi njihove narave ni mogoče zapisati, pač zato, ker komunikacije preprosto ni bilo.

Če pa predstavnik pristojnega nadzornega organa izbere vozilo in poskusi opraviti poizvedbo njegovega *DSRC-VU*, a ne pride do uspešnega prenosa podatkov, je do te napake morda prišlo zaradi namernega posega, zato mora biti predstavniku pristojnega nadzornega organa omogočeno, da napako zabeleži in opozori kolege, ki so naprej ob cesti, da je morda prišlo do kršitve. Kolegi lahko nato ustavijo vozilo in opravijo fizični pregled. Vendar pa uspešne komunikacije ni bilo, zato DSRC-VU ne more posredovati podatkov o napaki. Tako poročanje mora biti torej odvisno od zasnove opreme REDCR.

„Nebranje“ se tehnično razlikuje od „napake“. V tej zvezi „napaka“ pomeni pridobitev napačne vrednosti.

▼B

Podatki, ki se posredujejo *DSRC-VU*, so ob posredovanju še zaščiteni, zato jih je moral preveriti posredovalec podatkov (glej oddelek 5.4).

Podatki, ki se nato prenesejo skozi vmesnik po zraku, se preverjajo s cikličnimi preverjanji redundance (CRC) na ravni komunikacij. Če jih CRC potrdi, so podatki pravilni. Če jih CRC ne potrdi, se podatki pošljejo ponovno. Verjetnost, da bi podatki nepravilno prišli skozi CRC, je statistično tako majhna, da jo je mogoče zanemariti.

Če CRC ne potrdi podatkov in ni časa za ponoven prenos in prejem pravilnih podatkov, izid ne bo napaka, temveč konkretizacija določenega tipa napake pri branju.

Edini pomemben podatek o „napaki“, ki se lahko zapiše, je število uspešnih konkretizacij transakcij, ki so se odvile, ne da bi pri njih prišlo do uspešnega prenosa podatkov v REDCR.

DSC_82 *REDCR* zato zapiše, skupaj s časovnim žigom, število primerov, v katerih je bila faza „inicializacije“ poizvedbe preko DSRC sicer uspešna, vendar je bila transakcija prekinjena, preden je REDCR uspešno prejel *podatke*. Podatki so na razpolago predstavniku pristojnega nadzornega organa in so shranjeni v pomnilniku opreme REDCR. Sredstva, s katerimi se to doseže, so odvisna od zasnove proizvoda ali specifikacije pristojnega nadzornega organa.

Edini pomembni podatek o „napaki“, ki ga je mogoče zapisati, je, kolikokrat REDCR ni uspelo dešifrirati prejetih *podatkov*. Vendar bo to odvisno zgolj od učinkovitosti programske opreme REDCR. Lahko se zgodi, da so podatki tehnično dešifrirani, vendar semantično nimajo nobenega pomena.

DSC_83 Zato *REDCR* zapiše, skupaj s časovnim žigom, kolikokrat je neuspešno poskusil dešifrirati podatke, ki jih je prejel preko vmesnika DSRC.

6 NAROČANJE IN REDNI KONTROLNI PREGLEDI ZA FUNKCIJO KOMUNIKACIJE NA DALJAVO

6.1 **Splošno**

DSC_84 Za funkcijo komunikacije na daljavo sta predvideni dve vrsti preskusov:

1) preskus ECHO za preverjanje brezžičnega komunikacijskega kanala *DSRC-REDCR >>-:-<DSRC-VU*;

2) varnostni preskus celotnega postopka, s katerim se zagotovi, da kartica servisne delavnice lahko dostopa do šifrirane in podpisane podatkovne vsebine, ki jo je ustvarila VU in ki je bila prenesena preko brezžičnega komunikacijskega kanala.

6.2 **ECHO**

Določbe tega odstavka se nanašajo posebej na preskus, s katerim se ugotavlja, ali je povezava *DSRC-REDCR >>-:-<DSRC-VU* funkcionalno aktivna.

▼B

Cilj ukaza ECHO je omogočiti servisnim delavnicam ali objektom za homologacijske preskuse, da preskusijo delovanje povezave DSRC, ne da bi potrebovali dostop do varnostnih poverilnic. Zato je dovolj, da preskuševalčeva oprema inicializira komunikacijo preko DSRC (tako, da pošlje BST z AID = 2), nato pa pošlje ukaz ECHO in bo, če DSRC deluje, prejela odgovor ECHO. Podrobnosti so navedene voddelku 5.4.8. Če povezava DSRC (*DSRC-REDCR* >>-:-<*DSRC-VU*) ta odgovor prejme pravilno, je mogoče potrditi, da deluje pravilno.

6.3 **Preskus za preveritev vsebine zaščitenih podatkov**

DSC_85 S tem testom se preverja zaščiteni pretok podatkov od začetka do konca. Za tak preskus je potreben preskusni bralnik DSRC. Preskusni bralnik DSRC opravlja enako funkcijo in se uporablja z enakimi specifikacijami kot bralnik, ki ga uporabljajo organi javnega reda, edina razlika je, da se za avtentikacijo uporabnika preskusnega bralnika DSRC ne uporablja nadzorna kartica, temveč kartica servisne delavnice. Preskus se lahko izvede po začetni aktivaciji pametnega tahografa ali po končanem postopku kalibracije. Po aktivaciji enota v vozilu ustvari in sporoči DSRC-VU zaščitene podatke o zgodnjem odkrivanju.

DSC_86 Osebje servisne delavnice mora postaviti preskusni bralnik na razdalji 2–10 metrov pred vozilom.

DSC_87 Nato osebje servisne delavnice vstavi kartico servisne delavnice v preskusni bralnik, da lahko zahteva poizvedbo podatkov o zgodnjem odkrivanju v enoti v vozilu. Po uspešni poizvedbi si osebje servisne delavnice ogleda prejete podatke, da bi zagotovilo, da je bila njihova celovitost uspešno potrjena in da so bili uspešno dešifrirani.

▼B

Dodatek 15

MIGRACIJA: UPRAVLJANJE SOOBSTOJA NAPRAV RAZLIČNIH GENERACIJ

KAZALO

1. OPREDELITVE POJMOV

2. SPLOŠNE DOLOČBE

2.1. Pregled prehoda

2.2. Interoperabilnost med VU in karticami

2.3. Interoperabilnost med VU in tipali gibanja

2.4. Interoperabilnost med enotami v vozilu, tahografskimi karticami in opremo za prenos podatkov

2.4.1 Neposredni prenos podatkov s strani IDE

2.4.2 Prenos podatkov s kartice prek enote v vozilu

2.4.3 Prenos podatkov iz enote v vozilu

2.5. Interoperabilnost med vu in kalibracijsko opremo

3. GLAVNI KORAKI V OBDOBJU PRED DATUMOM UVEDBE

4. DOLOČBE ZA OBDOBJE PO DATUMU UVEDBE

1. OPREDELITVE POJMOV

Za namen tega dodatka se uporabljajo naslednje opredelitve:

sistem pametnih tahografov*:* kot je opredeljen v tej prilogi (poglavje 1: opredelitev bbb));

tahografski sistem prve generacije*:* kot je opredeljen v tej uredbi (člen 2: opredelitev 1);

tahografski sistem druge generacije*:* kot je opredeljen v tej uredbi (člen 2: opredelitev 7);

datum uvedbe*:* kot je opredeljen v tej prilogi (poglavje 1: opredelitev ccc));

inteligentna namenska oprema (IDE)*:* oprema, ki se uporablja za prenos podatkov, kot je opredeljeno v Dodatku 7 k tej prilogi.

2. SPLOŠNE DOLOČBE

2.1. **Pregled prehoda**

Uvodne izjave te priloge vsebujejo pregled prehoda med tahografskima sistemoma prve in druge generacije.

Poleg določb iz teh uvodnih izjav:

— tipala gibanja prve generacije ne bodo interoperabilna z enotami v vozilu druge generacije,

— se bodo tipala gibanja druge generacije začela nameščati v vozila hkrati z enotami v vozilu druge generacije,

▼B

— bo potreben nadaljnji razvoj opreme za prenos podatkov in kalibracijo, da bo podpirala uporabo z zapisovalnimi napravami in tahografskimi karticami obeh generacij.

2.2. **Interoperabilnost med VU in karticami**

Razume se, da so tahografske kartice prve generacije interoperabilne z enotami v vozilu prve generacije (v skladu s Prilogo 1B k tej uredbi) ter da so tahografske kartice druge generacije interoperabilne z enotami v vozilu druge generacije (v skladu s Prilogo 1C k tej uredbi). Poleg tega veljajo tudi spodnje zahteve.

MIG_001 Razen kot je določeno v zahtevah MIG_004 in MIG_005, se tahografske kartice prve generacije lahko še naprej uporabljajo v enotah v vozilu druge generacije do datuma izteka njihove veljavnosti. Vendar njihovi imetniki lahko zaprosijo za nadomestitev teh kartic s tahografskimi karticami druge generacije, takoj ko bodo te na voljo.

MIG_002 Enote v vozilu druge generacije lahko uporabljajo katero koli vstavljeno veljavno vozniško in nadzorno kartico in kartico podjetja prve generacije.

MIG_003 To zmožnost takšnih enot v vozilu lahko enkrat za vselej odpravijo servisne delavnice, tako da enote v vozilu tahografskih kartic prve generacije ne sprejemajo več. To lahko storijo samo potem, ko Evropska komisija sproži postopek, s katerim od servisnih delavnic to namerava zahtevati, na primer med rednimi kontrolnimi pregledi tahografov.

MIG_004 Enote v vozilu druge generacije lahko uporabljajo samo kartice servisne delavnice druge generacije.

MIG_005 Za določitev načina delovanja enote v vozilu druge generacije upoštevajo samo vrsto veljavnih vstavljenih kartic, ne glede na njihovo generacijo.

MIG_006 Vsaka veljavna tahografska kartica druge generacije se lahko uporabi v enotah v vozilu prve generacije na točno enak način kot tahografske kartice iste vrste prve generacije.

2.3. **Interoperabilnost med VU in tipali gibanja**

Razume se, da so tipala gibanja prve generacije interoperabilna z enotami v vozilu prve generacije ter da so tipala gibanja druge generacije interoperabilna z enotami v vozilu druge generacije. Poleg tega veljajo tudi spodnje zahteve.

MIG_007 Enote v vozilu druge generacije se ne morejo povezati in uporabljati s tipali gibanja prve generacije.

MIG_008 tipala gibanja druge generacije se lahko povežejo in uporabljajo bodisi samo z enotami v vozilu druge generacije bodisi z enotami v vozilu obeh generacij.

2.4. **Interoperabilnost med enotami v vozilu, tahografskimi karticami in opremo za prenos podatkov**

MIG_009 Oprema za prenos podatkov se lahko uporablja bodisi samo z eno generacijo enot v vozilu in tahografskih kartic bodisi z obema.

▼B

2.4.1 *Neposredni prenos podatkov s strani IDE*

MIG_010 Podatke s tahografskih kartic ene generacije, vstavljene v njihove bralnike kartic, IDE prenese ob uporabi varnostnih mehanizmov in protokola za prenos podatkov za ustrezno generacijo, preneseni podatki pa so v formatu, določenem za to generacijo.

MIG_011 Da se nadzor nad vozniki omogoči tudi nadzornim organom zunaj EU, je mogoče z vozniških kartic (in kartic servisne delavnice) druge generacije podatke prenesti na povsem enak način, kot z vozniških kartic (in kartic servisne delavnice) prve generacije. Tak prenos podatkov vključuje:

— nepodpisani EF `IC`in `ICC`,

— nepodpisani EF (prve generacije) `Card_Certificate` in `CA_Certificate`,

— druge EF z aplikativnimi podatki (v DF `TACHO`), ki se zahtevajo v protokolu za prenos podatkov s kartice prve generacije. Ti podatki so v skladu z varnostnimi mehanizmi prve generacije zaščiteni z digitalnim podpisom.

Tak prenos ne vključuje EF z aplikativnimi podatki, prisotnih na vozniških karticah (in karticah servisnih delavnic) druge generacije (EF z aplikativnimi podatki znotraj DF `TACHO_G2`).

2.4.2 *Prenos podatkov s kartice prek enote v vozilu*

MIG_012 Podatki s kartice druge generacije, vstavljene v enoto v vozilu prve generacije, se prenesejo ob uporabi protokola za prenos podatkov prve generacije. Kartica na ukaze enote v vozilu odgovori na točno enak način kot kartica prve generacije in preneseni podatki so v enakem formatu kot podatki, preneseni s kartice prve generacije.

MIG_013 S kartice prve generacije, vstavljene v enoto v vozilu druge generacije, se podatki prenesejo ob uporabi protokola za prenos podatkov, kot je opredeljen v Dodatku 7 k tej prilogi. Enota v vozilu pošilja ukaze kartici na točno enak način kot enota v vozilu prve generacije in preneseni podatki ustrezajo formatu, določenemu za kartice prve generacije.

2.4.3 *Prenos podatkov iz enote v vozilu*

MIG_014 Iz enot v vozilu druge generacije se podatki prenesejo ob uporabi varnostnih mehanizmov druge generacije in protokola za prenos podatkov, kot je določen v Dodatku 7 k tej prilogi.

MIG_015 Da se omogočita nadzor nad vozniki tudi nadzornim organom zunaj EU in prenos podatkov s strani servisnih delavnic zunaj EU, je neobvezno lahko omogočen tudi prenos podatkov iz enot v vozilu druge generacije ob uporabi varnostnih mehanizmov prve generacije in protokola za prenos podatkov prve generacije. Preneseni podatki so v enakem formatu kot podatki, preneseni iz enote v vozilu prve generacije. Ta funkcija se lahko izbere prek ukazov v meniju.

▼B

2.5. **Interoperabilnost med VU in kalibracijsko opremo**

MIG_016 Kalibracijska oprema je zmožna opraviti kalibracijo katere koli generacije tahografov s pomočjo kalibracijskega protokola ustrezne generacije. Kalibracijska oprema se lahko uporablja bodisi samo z eno generacijo tahografov bodisi z obema.

3. GLAVNI KORAKI V OBDOBJU PRED DATUMOM UVEDBE

MIG_017 Preskusni ključi in certifikati so proizvajalcem na voljo najpozneje **30 mesecev** pred datumom uvedbe.

MIG_018 Preskusi interoperabilnosti, če jih zahtevajo proizvajalci, so pripravljeni za izvedbo najpozneje **15 mesecev** pred datumom uvedbe.

MIG_019 Uradni ključi in certifikati so proizvajalcem na voljo najpozneje **12 mesecev** pred datumom uvedbe.

MIG_020 Države članice so zmožne izdati kartice servisne delavnice druge generacije najpozneje **3 mesece** pred datumom uvedbe.

MIG_021 Države članice so zmožne izdati vse vrste tahografskih kartic druge generacije najpozneje **1 mesec pred datumom uvedbe**.

4. DOLOČBE ZA OBDOBJE PO DATUMU UVEDBE

MIG_022 Po datumu uvedbe države članice izdajajo samo tahografske kartice druge generacije.

MIG_023 Proizvajalcem enot v vozilu/tipal gibanja je dovoljena proizvodnja enot v vozilu/tipal gibanja prve generacije, dokler se uporabljajo v praksi, tako da se lahko nadomestijo okvarjeni deli.

MIG_024 Proizvajalcem enot v vozilu/tipal gibanja je dovoljeno, da zaprosijo za obnovitev homologacije in jo pridobijo za že homologirane vrste enot v vozilu/tipal gibanja prve generacije.

▼B

Dodatek 16

PRETVORNIK ZA VOZILA KATEGORIJ M1 IN N1

KAZALO

1. KRATICE IN REFERENČNI DOKUMENTI

1.1. Kratice

1.2. Referenčni standardi

2. SPLOŠNE ZNAČILNOSTI IN FUNKCIJE PRETVORNIKA

2.1. Splošni opis pretvornika

2.2. Funkcije

2.3. Varnost

3. ZAHTEVE ZA ZAPISOVALNO NAPRAVO V PRIMERU NAMEŠČENEGA PRETVORNIKA

4. KONSTRUKCIJSKE IN FUNKCIONALNE ZAHTEVE ZA PRETVORNIK

4.1. Povezovanje in prilagajanje vhodnih impulzov hitrosti

4.2. Prenašanje vhodnih impulzov v vgrajeno tipalo gibanja

4.3. Vgrajeno tipalo gibanja

4.4. Varnostne zahteve

4.5. Delovne karakteristike

4.6. Materiali

4.7. Oznake

5. NAMESTITEV ZAPISOVALNE NAPRAVE V PRIMERU UPORABE PRETVORNIKA

5.1. Namestitev

5.2. Zapečatenje

6. PREVERJANJA, KONTROLNI PREGLEDI IN POPRAVILA

6.1. Redni kontrolni pregledi

7. HOMOLOGACIJA ZAPISOVALNE NAPRAVE V PRIMERU UPORABE PRETVORNIKA

7.1. Splošne točke

7.2. Potrdilo o funkcionalnosti

1. KRATICE IN REFERENČNI DOKUMENTI

1.1. **Kratice**

TBD Bo določeno naknadno

VU Enota v vozilu

1.2. **Referenčni standardi**

ISO16844-3 Road vehicles – Tachograph systems – Part 3: Motion sensor interface

2. SPLOŠNE ZNAČILNOSTI IN FUNKCIJE PRETVORNIKA

2.1. **Splošni opis pretvornika**

ADA_001 Pretvornik povezani enoti v vozilu zagotavlja zaščitene podatke o gibanju vozila, ki stalno kažejo hitrost in prevoženo pot vozila.

Pretvornik je namenjen le tistim vozilom, za katere se zahteva, da so opremljena z zapisovalno opremo v skladu s to uredbo.

▼B

Pretvornik se namesti in uporablja samo v tipih vozil, opredeljenih v opredelitvi yy) „pretvornik“ Priloge IC, če namestitev druge vrste obstoječega tipala gibanja, ki sicer je v skladu z določbami te priloge in njenih dodatkov 1 do 16, mehansko ni mogoča,

Pretvornik ni mehansko povezan s premikajočim se delom vozila, temveč je povezan z impulzi hitrosti/razdalje, ki jih ustvarjajo vgrajena tipala ali alternativni vmesniki.

ADA_002 Homologirano tipalo gibanja (v skladu z določbami iz oddelka 8 Priloge IC „Homologacija zapisovalne naprave in tahografskih kartic“) se namesti v ohišje pretvornika, v katerem je tudi naprava za pretvarjanje impulzov, ki posreduje vhodne impulze v vgrajeno tipalo gibanja. Vgrajeno tipalo gibanja je povezano z enoto v vozilu, tako da je vmesnik med to enoto in pretvornikom v skladu z zahtevami iz standarda ISO 16844-3.

2.2. **Funkcije**

ADA_003 Pretvornik ima tudi naslednje funkcije:

— vmesniško povezovanje in prilagajanje vhodnih impulzov hitrosti,

— prenašanje vhodnih impulzov v vgrajeno tipalo gibanja,

— vse funkcije vgrajenega tipala gibanja, ki enoti v vozilu zagotavljajo zaščitene podatke o gibanju.

2.3. **Varnost**

ADA_004 V skladu s splošnim varnostnim ciljem v zvezi s tipalom gibanja, opredeljenim v Dodatku 10 k tej prilogi, pretvornik ni varnostno certificiran. Namesto tega se uporabljajo varnostne zahteve iz oddelka 4.4 tega dodatka.

3. ZAHTEVE ZA ZAPISOVALNO NAPRAVO V PRIMERU NAMEŠČENEGA PRETVORNIKA

Zahteve v tem oddelku in naslednjih oddelkih pojasnjujejo zahteve iz te priloge v primeru uporabe pretvornika. Zadevne številke zahtev iz Priloge IC so navedene v oklepajih.

ADA_005 Zapisovalna naprava mora v vsakem vozilu, ki je opremljeno s pretvornikom, izpolnjevati vse določbe iz te priloge, razen če je v tem dodatku določeno drugače.

ADA_006 V primeru nameščenega pretvornika je zapisovalna naprava sestavljena iz kablov, pretvornika (vključno s tipalom gibanja) in enote v vozilu [01].

ADA_007 Funkcija zaznavanja dogodkov in/ali napak zapisovalne naprave se spremeni, kot sledi:

— dogodek „izpad napajanja“ sproži enota v vozilu, kadar naprava ni v kalibracijskem načinu in izpad napajanja vgrajenega tipala gibanja traja dlje kot 200 milisekund [79];

▼B

— dogodek „napaka v podatkih o gibanju“ sproži enota v vozilu, kadar je prekinjen normalen pretok podatkov med vgrajenim tipalom gibanja in enoto v vozilu in/ali ob napaki v zvezi s celovitostjo ali avtentikacijo podatkov pri prenosu podatkov med vgrajenim tipalom gibanja in enoto v vozilu [83];

— dogodek „poskus kršenja varnosti“ sproži enota v vozilu ob vsakem drugem dogodku, ki vpliva na zaščito vgrajenega tipala gibanja, kadar naprava ni v kalibracijskem načinu [85];

— napako „zapisovalna naprava“ sproži enota v vozilu za vsako napako vgrajenega tipala gibanja, kadar naprava ni v kalibracijskem načinu [88].

ADA_008 Zapisovalna naprava zazna napake pretvornika, povezane z vgrajenim tipalom gibanja [88].

ADA_009 Funkcija kalibracije enote v vozilu omogoča samodejno povezovanje vgrajenega tipala gibanja z enoto v vozilu [202, 204].

4. KONSTRUKCIJSKE IN FUNKCIONALNE ZAHTEVE ZA PRETVORNIK

4.1. **Povezovanje in prilagajanje vhodnih impulzov hitrosti**

ADA_011 Vhodni vmesnik pretvornika sprejema frekvenčne impulze, ki kažejo hitrost in prevoženo pot vozila. Električne značilnosti vhodnih impulzov so: *naknadno določi proizvajalec*. Po potrebi se s prilagoditvami, ki so dostopne le proizvajalcu pretvornika in pooblaščeni servisni delavnici, ki pretvornike namešča, omogoči pravilno vmesniško povezovanje vhoda pretvornika z vozilom, če je ustrezno.

ADA_012 Vhodni vmesnik pretvornika, če je ustrezno, lahko s fiksnim faktorjem množi ali deli frekvenčne impulze vhodnih impulzov hitrosti, da se signal prilagodi vrednosti v območju faktorja k, ki je določeno v tej prilogi (4 000 do 25 000 impulzov/km). Fiksni faktor lahko določita le proizvajalec pretvornika in pooblaščena servisna delavnica, ki opravlja namestitev pretvornika.

4.2. **Prenašanje vhodnih impulzov v vgrajeno tipalo gibanja**

ADA_013 Vhodni impulzi, ki se po potrebi prilagodijo, kot je predpisano zgoraj, se prenesejo v vgrajeno tipalo gibanja, tako da to zazna vsak vhodni impulz.

4.3. **Vgrajeno tipalo gibanja**

ADA_014 Vgrajeno tipalo gibanja stimulirajo preneseni impulzi, s čimer se omogoča pridobivanje podatkov o gibanju, ki točno prikazujejo gibanje vozila, kot če bi bilo tipalo mehansko povezano s premikajočim se delom vozila.

ADA_015 Enota v vozilu za identifikacijo pretvornika uporablja identifikacijske podatke vgrajenega tipala gibanja [95].

▼B

ADA_016 Podatki o vgradnji, ki jih hrani vgrajeno tipalo gibanja, se štejejo kot podatki o namestitvi pretvornika [122].

4.4. **Varnostne zahteve**

ADA_017 Ohišje pretvornika je zasnovano tako, da ga ni mogoče odpreti. Ohišje je zapečateno, tako da je poskuse nepooblaščenih fizičnih posegov mogoče enostavno odkriti (npr. na podlagi vizualnega pregleda, glej ADA_035). Za pečate veljajo enake zahteve kot za pečate tipala gibanja [398 do 406].

ADA_018 Vgrajenega tipala gibanja ni mogoče odstraniti iz pretvornika brez preloma pečata(-ov) na ohišju pretvornika ali brez preloma pečata med tipalom in ohišjem pretvornika (glej ADA_034).

ADA_019 Pretvornik zagotavlja, da je podatke o gibanju mogoče obdelovati in pridobivati le prek vhoda pretvornika.

4.5. **Delovne karakteristike**

ADA_020 Pretvornik je v celoti funkcionalen v temperaturnem območju, ki ga določi proizvajalec.

ADA_021 Pretvornik je v celoti funkcionalen v območju vlažnosti od 10 % do 90 % [214].

ADA_022 Pretvornik je zaščiten pred prenapetostjo, zamenjavo polarnosti napajanja in kratkimi stiki [216].

ADA_023 Pretvornik:

— bodisi reagira na magnetna polja, ki motijo zaznavanje gibanja vozila. V takšnih okoliščinah enota v vozilu zapiše in shrani napako na tipalu [88];

— bodisi ima tipalni element, ki je zaščiten pred magnetnimi polji ali je zanje neobčutljiv [217].

ADA_024 Pretvornik je skladen z mednarodnim predpisom UN ECE R10 o elektromagnetni združljivosti ter zaščiten pred elektrostatičnimi razelektritvami in prehodnimi pojavi [218].

4.6. **Materiali**

ADA_025 Pretvornik ima stopnjo zaščite *(naknadno določi proizvajalec, odvisno od položaja namestitve)* [220, 221].

ADA_026 Ohišje pretvornika je rumene barve.

4.7. **Oznake**

ADA_027 Na pretvornik je pritrjena označevalna ploščica, na kateri so navedeni naslednji podatki:

— ime in naslov proizvajalca pretvornika,

— kataloška številka proizvajalca in leto proizvodnje pretvornika,

— homologacijska oznaka tipa pretvornika ali tipa zapisovalne naprave, vključno z vgrajenim pretvornikom,

— datum vgradnje pretvornika,

▼B

— identifikacijska številka vozila, v katero je pretvornik nameščen.

ADA_028 Označevalna ploščica vsebuje tudi naslednje podatke (če jih ni mogoče prebrati neposredno na zunanji strani vgrajenega tipala gibanja):

— ime proizvajalca vgrajenega tipala gibanja,

— kataloška številka proizvajalca in leto proizvodnje vgrajenega tipala gibanja,

— homologacijska oznaka vgrajenega tipala gibanja.

5. NAMESTITEV ZAPISOVALNE NAPRAVE V PRIMERU UPORABE PRETVORNIKA

5.1. **Namestitev**

ADA_029 Pretvornike za namestitev v vozila lahko namestijo samo proizvajalci vozil ali servisne delavnice, pooblaščene za namestitev, aktivacijo in kalibracijo digitalnih in pametnih tahografov.

ADA_030 Pooblaščena servisna delavnica, ki vgradi pretvornik, prilagodi vhodni vmesnik in izbere razmerje za izračun vhodnega signala (če je ustrezno).

ADA_031 Pooblaščena servisna delavnica, ki vgradi pretvornik, zapečati ohišje pretvornika.

ADA_032 Pretvornik se namesti čim bližje delu vozila, ki zagotavlja vhodne impulze.

ADA_033 Kabli, prek katerih se pretvornik napaja, so rdeče (faza) in črne barve (ozemljitev).

5.2. **Zapečatenje**

ADA_034 Pri zapečatenju veljajo naslednje zahteve:

— ohišje pretvornika je zapečateno (glej ADA_017),

— ohišje vgrajenega tipala je pripečateno na ohišje pretvornika, razen če tipala ni mogoče odstraniti od ohišja pretvornika, ne da bi pri tem poškodovali pečat na ohišju pretvornika (glej ADA_018),

— ohišje pretvornika je zapečateno na vozilo,

— povezava med pretvornikom in opremo, ki zagotavlja vhodne impulze, je zapečatena na obeh straneh (kolikor je to v razumnih mejah mogoče).

6. PREVERJANJA, KONTROLNI PREGLEDI IN POPRAVILA

6.1. **Redni kontrolni pregledi**

ADA_035 Pri uporabi pretvornika se pri vsakem rednem inšpekcijskem pregledu (redni inšpekcijski pregled pomeni pregled v skladu z zahtevami [409] do [413] iz Priloge 1C) zapisovalne naprave preveri naslednje:

— ali ima pretvornik ustrezne homologacijske oznake,

— ali so pečati na pretvorniku in njegovih priključkih nepoškodovani,

▼B

— ali je pretvornik nameščen, kot je navedeno na namestitveni ploščici,

— ali je pretvornik nameščen, kot določa proizvajalec pretvornika in/ali vozila,

— ali je vgradnja pretvornika dovoljena za vozilo, ki se pregleduje.

ADA_036 Ti kontrolni pregledi vključujejo kalibracijo in nadomestitev vseh pečatov, ne glede na to, v kakšnem stanju so.

7. HOMOLOGACIJA ZAPISOVALNE NAPRAVE V PRIMERU UPORABE PRETVORNIKA

7.1. **Splošne točke**

ADA_037 Za homologacijo je treba zapisovalno napravo predložiti skupaj s pretvornikom [425].

ADA_038 Vsak pretvornik se lahko predloži v homologacijo kot samostojna naprava ali kot sestavni del zapisovalne naprave.

ADA_039 Taka homologacija vključuje preskuse delovanja pretvornika. Pozitiven rezultat vsakega od teh preskusov se navede v ustreznem potrdilu [426].

7.2. **Potrdilo o funkcionalnosti**

ADA_040 Potrdilo o funkcionalnosti pretvornika ali zapisovalne naprave s pretvornikom se predloži proizvajalcu pretvornika šele potem, ko so bili uspešno opravljeni vsi minimalni preskusi delovanja, navedeni v nadaljevanju.

Št.	Preskus	Opis	Povezane zahteve
1.	**Administrativni pregled**		
1.1	Dokumentacija	Pravilnost dokumentacije o pretvorniku	
2.	**Vizualni pregled**		
2.1	Skladnost pretvornika z dokumentacijo		
2.2	Identifikacija/oznake pretvornika		ADA_027, ADA_028
2.3	Material pretvornika		od [219] do [223] ADA_026
2.4	Zapečatenje		ADA_017, ADA_018, ADA_034
3.	**Preskusi delovanja**		
3.1	Prenašanje impulzov hitrosti v vgrajeno tipalo gibanja		ADA_013

▼B

Št.	Preskus	Opis	Povezane zahteve
3.2	Povezovanje in prilagajanje vhodnih impulzov hitrosti		ADA_011, ADA_012
3.3	Točnost meritve gibanja		od [30] do [35], [217]
4.	**Okoljski preskusi**		
4.1	Rezultati preskusa proizvajalca	Rezultati okoljskih preskusov proizvajalca	ADA_020, ADA_021, ADA_022, ADA_024
5.	**Elektromagnetna združljivost**		
5.1	Sevane emisije in dovzetnost	Preveri se skladnost z Direktivo 2006/28/ES	ADA_024
5.2	Rezultati preskusa proizvajalca	Rezultati okoljskih preskusov proizvajalca	ADA_024

▼C1

PRILOGA II

HOMOLOGACIJSKA OZNAKA IN CERTIFIKAT O HOMOLOGACIJI

I. HOMOLOGACIJSKA OZNAKA

1. Homologacijska oznaka je sestavljena iz:

(a) pravokotnika, znotraj katerega je majhna črka „e“, ki ji sledi oznaka države (številska ali črkovna), ki je izdala homologacijo, skladno z naslednjimi dogovorjenimi oznakami:

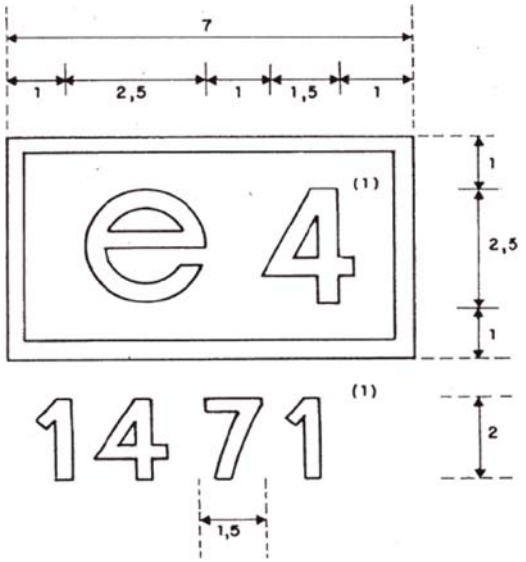
Belgija	6,
Bolgarija	34,
Češka	8,
Danska	18,
Nemčija	1,
Estonija	29,
Irska	24,
Grčija	23,
Španija	9,
Francija	2,
Hrvaška	25,
Italija	3,
Ciper	CY,
Latvija	32,
Litva	36,
Luksemburg	13,
Madžarska	7,
Malta	MT,
Nizozemska	4,
Avstrija	12,
Poljska	20,
Portugalska	21,
Romunija	19,
Slovenija	26,
Slovaška	27,
Finska	17,
Švedska	5,
Združeno kraljestvo ter	11,

(b) homologacijske številke, ki ustreza številki certifikata o homologaciji za prototip zapisovalne naprave ali tahografskega vložka ali številki tahografske kartice in je nameščena v neposredni bližini tega pravokotnika.

▼C1

2. Homologacijska oznaka je prikazana na označevalni ploščici na vsakem kosu opreme, na vsakem tahografskem vložku in na vsaki tahografski kartici. Oznaka mora biti neizbrisna in trajno jasno čitljiva.

3. Mere homologacijske oznake ([1]), ki so na spodnji sliki navedene v milimetrih, so najmanjše možne mere. Razmerja med merami je treba ohraniti.



([1]) Te številke so le smernice.

▼C1

II. CERTIFIKAT O HOMOLOGACIJI ZA ANALOGNE TAHOGRAFE

Država članica, ki je podelila homologacijo, prosilcu izda certifikat o homologaciji, katerega vzorec je v nadaljevanju. Za obveščanje drugih držav članic o izdanih certifikatih ali o njihovem morebitnem odvzemu vsaka država članica uporablja kopije tega certifikata.

CERTIFIKAT O HOMOLOGACIJI

Naziv pristojnega upravnega organa .....

Obvestilo o ([1]):

— homologaciji vrste zapisovalne naprave

— odvzemu homologacije vrste zapisovalne naprave

— homologaciji vzorca tahografskega vložka

— odvzemu homologacije vzorca tahografskega vložka

Homologacijska št.:

.....

1. Trgovska znamka ali ime .....

2. Ime tipa ali vzorca .....

3. Ime proizvajalca .....

4. Naslov proizvajalca .....

5. Predloženo v homologacijo dne .....

6. Preskušeno v laboratoriju .....

7. Datum in številka preskusov .....

8. Datum homologacije .....

9. Datum odvzema homologacije .....

10. Vrsta ali vrste zapisovalne naprave, v kateri(-h) se vložek lahko uporablja

11. Kraj .....

12. Datum .....

13. Priloženi opisni dokumenti .....

14. Pripombe (po potrebi tudi z navedbo mest pečatov)

(Podpis)

([1]) Neustrezno črtati.

▼C1

III. CERTIFIKAT O HOMOLOGACIJI ZA DIGITALNE TAHOGRAFE

Država članica, ki je podelila homologacijo, prosilcu izda certifikat o homologaciji, katerega vzorec je v nadaljevanju. Za obveščanje drugih držav članic o izdanih certifikatih ali o njihovem morebitnem odvzemu vsaka država članica uporablja kopije tega certifikata.

CERTIFIKAT O HOMOLOGACIJI ZA DIGITALNE TAHOGRAFE

Naziv pristojnega upravnega organa .....

Obvestilo o ([1]):

☐ homologaciji: ☐ odvzemu homologacije:

☐ vzorca zapisovalne naprave

☐ sestavnega dela zapisovalne naprave ([2])

☐ vozniške kartice

☐ kartice servisne delavnice

☐ kartice podjetja

☐ kartice nadzornika

Homologacijska št.:

.....

1. Trgovska ali blagovna znamka .....
2. Ime vzorca .....
3. Ime proizvajalca .....
4. Naslov proizvajalca .....
5. Predloženo v homologacijo za .....
6. Laboratorij(-i) .....
7. Datum in številka poročila o preskusu .....
8. Datum homologacije .....
9. Datum odvzema homologacije .....
10. Vzorec zapisovalne naprave/zapisovalnih naprav, s katero(-imi) se sestavni del lahko uporablja
11. Kraj .....
12. Datum .....
13. Priloženi opisni dokumenti .....
14. Pripombe (po potrebi tudi z navedbo mest pečatov)

(Podpis)

([1]) Označite ustrezna okenca.
([2]) Navedite sestavni del, ki ga obvestilo zadeva.

▼C1

IV. CERTIFIKAT O HOMOLOGACIJI ZA PAMETNE TAHOGRAFE

Država članica, ki je podelila homologacijo, prosilcu izda certifikat o homologaciji, katerega vzorec je v nadaljevanju. Za obveščanje drugih držav članic o izdanih certifikatih ali o njihovem morebitnem odvzemu vsaka država članica uporablja kopije tega certifikata.

CERTIFIKAT O HOMOLOGACIJI ZA PAMETNE TAHOGRAFE

Naziv pristojnega upravnega organa .....

Obvestilo o ([1]):

☐ homologaciji: ☐ odvzemu homologacije:

☐ vzorca zapisovalne naprave

☐ sestavnega dela zapisovalne naprave ([2])

☐ vozniške kartice

☐ kartice servisne delavnice

☐ kartice podjetja

☐ kartice nadzornika

Homologacijska št.:

.....

1. Trgovska ali blagovna znamka .....
2. Ime vzorca .....
3. Ime proizvajalca .....
4. Naslov proizvajalca .....
5. Predloženo v homologacijo za .....
6. a) Preskusni laboratorij za potrdilo o funkcionalnosti .....
   b) Preskusni laboratorij za potrdilo o varnosti .....
   c) Preskusni laboratorij za potrdilo o interoperabilnosti .....
7. a) Datum in številka potrdila o funkcionalnosti .....
   b) Datum in številka potrdila o varnosti .....
   c) Datum in številka potrdila o interoperabilnosti .....
8. Datum homologacije .....
9. Datum odvzema homologacije .....
10. Vzorec zapisovalne naprave/zapisovalnih naprav, s katero(-imi) se sestavni del lahko uporablja
11. Kraj .....
12. Datum .....
13. Priloženi opisni dokumenti .....
14. Pripombe (po potrebi tudi z navedbo mest pečatov)

(Podpis)

([1]) Označite ustrezna okenca.
([2]) Navedite sestavni del, ki ga obvestilo zadeva.