Denne tekst tjener udelukkende som dokumentationsværktøj og har ingen retsvirkning. EU's institutioner påtager sig intet ansvar for dens indhold. De autentiske udgaver af de relevante retsakter, inklusive deres betragtninger, er offentliggjort i den Europæiske Unions Tidende og kan findes i EUR-Lex. Disse officielle tekster er tilgængelige direkte via linkene i dette dokument

►B

KOMMISSIONENS GENNEMFØRELSESFORORDNING (EU) 2016/799

af 18. marts 2016

om gennemførelse af Europa-Parlamentets og Rådets forordning (EU) nr. 165/2014 om fastsættelse af forskrifter for konstruktion, afprøvning, installering, brug og reparation af takografer og deres komponenter

(EØS-relevant tekst)

(EUT L 139 af 26.5.2016, s. 1)

Berigtiget ved:

►C1 Berigtigelse, EUT L 146 af 3.6.2016, s. 31 (2016/799)
►C2 Berigtigelse, EUT L 27 af 1.2.2017, s. 169 (2016/799)
►C3 Berigtigelse, EUT L 166 af 29.6.2017, s. 82 (2016/799)

▼B

KOMMISSIONENS GENNEMFØRELSESFORORDNING (EU) 2016/799

af 18. marts 2016

om gennemførelse af Europa-Parlamentets og Rådets forordning (EU) nr. 165/2014 om fastsættelse af forskrifter for konstruktion, afprøvning, installering, brug og reparation af takografer og deres komponenter

(EØS-relevant tekst)

Artikel 1

Genstand og anvendelsesområde

1. I denne forordning fastsættes de nødvendige bestemmelser for en ensartet anvendelse af følgende aspekter vedrørende takografer:

a) registrering af køretøjets position på visse punkter i løbet af førerens daglige arbejdsperiode

b) tidlig fjernafsløring af mulig manipulation eller misbrug af intelligente takografer

c) interface med intelligente transportsystemer

d) de administrative og tekniske krav til typegodkendelsesprocedurerne for takografer, herunder sikkerhedsmekanismerne.

2. Konstruktion, afprøvning, installering, eftersyn, brug og reparation af intelligente takografer og deres komponenter skal ske i henhold til de tekniske krav i bilag 1C til denne forordning.

3. Andre takografer end intelligente takografer skal, for så vidt angår konstruktion, afprøvning, installering, eftersyn, brug og reparation, fortsat overholde kravene i enten bilag 1 eller bilag 1B til Rådets forordning (EØF) nr. 3821/85 ([1]), alt efter hvad der er relevant.

4. I henhold til artikel 10d i direktiv 96/53/EF skal udstyret til tidlig fjernafsløring ligeledes transmittere vægtdata fra et internt vejesystem i lastbilerne med henblik på tidlig fjernafsløring af svig.

Artikel 2

Definitioner

I denne forordning anvendes definitionerne i artikel 2 i forordning (EU) nr. 165/2014.

Desuden forstås ved:

1) »digital takograf« eller »takograf af første generation«: digital takograf, som ikke er en intelligent takograf

2) »eksternt GNSS-udstyr«: udstyr, der indeholder GNSS-modtageren, når køretøjsenheden ikke er en enkelt enhed, samt andre komponenter, der er nødvendige for at beskytte transmission af positionsdata til resten af køretøjsenheden

([1]) Rådets forordning (EØF) nr. 3821/85 af 20. december 1985 om kontrolapparatet inden for vejtransport (EFT L 370 af 31.12.1985, s. 8).

▼B

3) »informationsmappe«: hele mappen, i elektronisk form eller papirform, der indeholder alle oplysninger, som fabrikanten eller dennes repræsentant har indgivet til typegodkendelsesmyndigheden med henblik på typegodkendelse af en takograf eller en komponent i denne, inklusive de i artikel 12, stk. 3, i forordning (EU) nr. 165/2014 nævnte certifikater, resultaterne af de afprøvninger, der defineres i bilag 1C til denne forordning samt tegninger, fotografier og andre relevante dokumenter

4) »informationspakke«: informationsmappen i elektronisk form eller papirform, ledsaget af alle andre dokumenter, som typegodkendelsesmyndigheden har tilføjet til informationsmappen i forbindelse med udøvelsen af sine funktioner, herunder ved afslutningen af typegodkendelsesprocessen, EC-typegodkendelsesattesten for takografen eller en komponent i denne

5) »indeks til informationspakken«: dokument med en nummereret liste over indholdet i informationspakken, hvori alle de relevante dele af denne pakke identificeres. Formatet af dette dokument skal skelne mellem de forskellige trin i EC-typegodkendelsesprocessen, herunder datoer for eventuelle revisioner og ajourføringer af pakken

6) »udstyr til tidlig fjernafsløring«: udstyr i køretøjsenheden, der anvendes til at udføre målrettede vejkontroller

7) »intelligent takograf« eller »takograf af anden generation«: digital takograf, der er i overensstemmelse med artikel 8, 9 og 10 i forordning (EU) nr. 165/2014 samt med bilag I C til nærværende forordning

8) »takografkomponent« eller »komponent«: enhver af følgende elementer: køretøjsenheden, bevægelsessensoren, takografkortet, diagramarket, det eksterne GNSS-udstyr og udstyret til tidlig fjernafsløring

9) »typegodkendelsesmyndighed«: myndighed i en medlemsstat, der er kompetent til at foretage typegodkendelse af takografen eller af dennes komponenter, godkendelsesprocessen, udstedelse og i givet fald tilbagekaldelse af typegodkendelsesattester, at fungere som kontaktpunkt for typegodkendelsesmyndigheder i andre medlemsstater og at sikre, at fabrikanterne opfylder deres forpligtelser vedrørende overholdelsen af kravene i denne forordning.

Artikel 3

Lokaliseringsbaserede tjenester

1. Fabrikanterne sikrer, at intelligente takografer er kompatible med de lokaliseringstjenester, der tilbydes af systemerne Galileo og den europæiske geostationære navigations-overlay-tjeneste (»EGNOS«).

2. Ud over de i stk. 1 omtalte systemer kan fabrikanterne også vælge at sikre kompatibilitet med andre satellitnavigationssystemer.

▼B

Artikel 4

Procedure for typegodkendelse af en takograf og takografkomponenter

1. En fabrikant eller dennes repræsentant indgiver en ansøgning om typegodkendelse af en takograf eller en af dennes komponenter eller en gruppe af komponenter til typegodkendelsesmyndighederne, som udpeges af hver medlemsstat. Den skal bestå af en informationsmappe, der indeholder oplysninger om hver af de pågældende komponenter, herunder i givet fald typegodkendelsesattester for andre komponenter, der er nødvendige for at færdigbygge takografen samt alle andre relevante dokumenter.

2. En medlemsstat meddeler typegodkendelse af enhver takograf, komponent eller gruppe af komponenter, der er i overensstemmelse med de administrative og tekniske krav i artikel 1, stk. 2 eller 3. I dette tilfælde udsteder typegodkendelsesmyndigheden en typegodkendelsesattest til ansøgeren, der er i overensstemmelse med modellen i bilag II til denne forordning.

3. Typegodkendelsesmyndigheden kan anmode fabrikanten eller dennes repræsentant om at indsende eventuelle supplerende oplysninger.

4. Fabrikanten eller dennes repræsentant stiller det nødvendige antal takografer eller takografkomponenter til rådighed for typegodkendelsesmyndighederne og for de organer, der er ansvarlige for at udstede de i artikel 12, stk. 3, i forordning (EU) nr. 165/2014 omhandlede attester, med henblik på at muliggøre en tilfredsstillende afvikling af typegodkendelsesproceduren.

5. Når fabrikanten eller dennes repræsentant søger typegodkendelse af bestemte komponenter eller grupper af komponenter i en takograf, skal de stille de øvrige komponenter, som allerede er typegodkendt, samt andre dele, der er nødvendige for konstruktionen af den komplette takograf til rådighed for typegodkendelsesmyndighederne, således at disse myndigheder kan foretage de nødvendige afprøvninger.

Artikel 5

Ændringer af typegodkendelser

1. Fabrikanten eller dennes repræsentant underretter straks de typegodkendelsesmyndigheder, der har meddelt den oprindelige typegodkendelse, om eventuelle ændringer i software eller hardware til takografen eller i arten af materialer brugt til dens fremstilling, der er registreret i informationspakken, og fremsender en ansøgning om ændring af typegodkendelsen.

2. Typegodkendelsesmyndighederne kan revidere eller forlænge den eksisterende typegodkendelse eller udstede en ny typegodkendelse afhængigt af ændringernes art og kendetegn.

Der foretages en »revision«, hvis typegodkendelsesmyndigheden finder, at ændringerne i takografens software eller hardware eller arten af de materialer, der er anvendt til fremstillingen, er uvæsentlige. I så fald udsteder typegodkendelsesmyndigheden de reviderede dokumenter i informationspakken med angivelse af de foretagne ændringer og datoen for deres godkendelse. En ajourført udgave af informationspakken i konsolideret form ledsaget af en detaljeret beskrivelse af de foretagne ændringer er tilstrækkeligt til at opfylde dette krav.

▼B

En »forlængelse« foretages, hvis typegodkendelsesmyndigheden finder, at ændringerne i takografens software eller hardware eller arten af de materialer, der er anvendt til fremstillingen, er væsentlige. I så fald kan den anmode om, at der foretages yderligere afprøvninger, og underretter fabrikanten eller dennes repræsentant herom. Hvis disse afprøvninger er tilfredsstillende, udsteder typegodkendelsesmyndigheden en revideret typegodkendelsesattest, hvorpå angives et nummer, der henviser til den meddelte forlængelse. På typegodkendelsesattesten angives årsagen til forlængelsen og datoen for dens udstedelse.

3. I indholdsfortegnelsen i informationspakken anføres datoen for den seneste forlængelse eller revision af typegodkendelsen eller datoen for den seneste konsolidering af den ajourførte udgave af typegodkendelsen.

4. En typegodkendelse er nødvendig, hvis de ønskede ændringer af en typegodkendt takograf eller dens komponenter ville medføre, at der udstedes en ny sikkerheds- eller interoperabilitetsattest.

Artikel 6

Ikrafttræden

Denne forordning træder i kraft på tyvendedagen efter offentliggørelsen i *Den Europæiske Unions Tidende*.

Den anvendes fra den 2. marts 2016.

Bilagene gælder imidlertid fra den 2. marts 2019 med undtagelse af tillæg 16, der anvendes fra den 2. marts 2016.

Denne forordning er bindende i alle enkeltheder og gælder umiddelbart i hver medlemsstat.

▼B

BILAG I C

Forskrifter for konstruktion, afprøvning, montering og eftersyn

INDLEDNING

1 DEFINITIONER

2 KONTROLAPPARATETS GENERELLE EGENSKABER OG FUNKTIONER

2.1 Generelle egenskaber

2.2 Funktioner

2.3 Funktionstilstande

2.4 Sikkerhed

3 KONSTRUKTIONS- OG FUNKTIONSKRAV TIL KONTROLAPPARAT

3.1 Overvågning af isætning og udtagning af kort

3.2 Måling af hastighed, position og afstand

3.2.1 Måling af den tilbagelagte vejstrækning

3.2.2 Måling af hastigheden

3.2.3 Måling af position

3.3 Tidsmåling

3.4 Overvågning af føreraktiviteter

3.5 Overvågning af kørestatus

3.6 Indlæsning foretaget af fører

3.6.1 Indlæsning af de steder, hvor den daglige arbejdstid begynder og/eller slutter

3.6.2 Manuel indlæsning af føreraktiviteter og førerens samtykke til brug af ITS-grænsefladen

3.6.3 Indlæsning af særlige omstændigheder

3.7 Forvaltning af virksomhedslåse

3.8 Overvågning af kontrolaktiviteter

3.9 Detektion af hændelser og/eller fejl

3.9.1 Hændelsen »isætning af ugyldigt kort«

3.9.2 Hændelsen »kortkonflikt«

3.9.3 Hændelsen »tidsoverlapning«

3.9.4 Hændelsen »kørsel uden behørigt kort«

3.9.5 Hændelsen »isætning af kort under kørslen«

3.9.6 Hændelsen »sidste kortsession ikke korrekt afsluttet«

3.9.7 Hændelsen »overskridelse af tilladt hastighed«

3.9.8 Hændelsen »afbrydelse af strømforsyning«

3.9.9 Hændelsen »fejl ved kommunikation med faciliteten til fjernkommunikation«

3.9.10 Hændelsen »manglende positionsoplysninger fra GNSS-modtager«

▼B

3.9.11	Hændelsen »fejl ved kommunikation med det eksterne GNSS-udstyr«
3.9.12	Hændelsen »fejl ved køredata«
3.9.13	Hændelsen »køretøjsbevægelseskonflikt«
3.9.14	Hændelsen »forsøg på sikkerhedsbrud«
3.9.15	Hændelsen »tidskonflikt«
3.9.16	Fejlen »kort«
3.9.17	Fejlen »kontrolapparat«
3.10	Indbyggede tester og selvtester
3.11	Læsning fra datalager
3.12	Registrering og lagring i datalageret
3.12.1	Identifikationsdata for apparat
3.12.1.1	Identifikationsdata for køretøjsenhed
3.12.1.2	Identifikationsdata for bevægelsessensor
3.12.1.3	Identifikationsdata for globale satellitnavigationssystemer (GNSS)
3.12.2	Nøgler og certifikater
3.12.3	Data vedrørende isætning og udtagning af førerkort eller værkstedskort
3.12.4	Føreraktivitetsdata
3.12.5	Steder og positioner, hvor daglige arbejdsperioder starter og slutter og/eller hvor tre timers sammenhængende køretid nås
3.12.6	Kilometertællerdata
3.12.7	Detaljerede hastighedsdata
3.12.8	Data vedrørende hændelser
3.12.9	Data vedrørende fejl
3.12.10	Kalibreringsdata
3.12.11	Tidsjusteringsdata
3.12.12	Kontrolaktivitetsdata
3.12.13	Data vedrørende virksomhedslåse
3.12.14	Data vedrørende dataoverførselsaktivitet
3.12.15	Data vedrørende særlige omstændigheder
3.12.16	Data vedrørende takografkort
3.13	Læsning fra takografkort
3.14	Registrering og lagring på takografkort
3.14.1	Registrering og lagring på takografkort af første generation
3.14.2	Registrering og lagring på takografkort af anden generation
3.15	Visning på skærm
3.15.1	Standardskærmbillede
3.15.2	Visning af advarsel

▼B

3.15.3	Adgang via menu
3.15.4	Andre skærmbilleder
3.16	Udskrivning
3.17	Advarsler
3.18	Dataoverførsel til eksterne medier
3.19	Fjernkommunikation i forbindelse med målrettede vejsidekontroller
3.20	Udlæsning af data til supplerende eksterne enheder
3.21	Kalibrering
3.22	Kalibreringskontrol ved vejsiden
3.23	Tidsjustering
3.24	Funktionsspecifikationer
3.25	Materialer
3.26	Mærkning
4	KONSTRUKTIONS- OG FUNKTIONSKRAV TIL TAKOGRAF-KORT
4.1	Synlige data
4.2	Sikkerhed
4.3	Standarder
4.4	Miljømæssige og elektriske specifikationer
4.5	Lagring af oplysninger
4.5.1	Elementærfiler til identifikation og kortstyring
4.5.2	Identifikation af IC-kort
4.5.2.1	Identifikation af chip
4.5.2.2	DIR (findes kun i takografkort af anden generation)
4.5.2.3	ATR-oplysninger (betingede, findes kun i takografkort af anden generation)
4.5.2.4	Oplysninger med udvidet længde (betingede, findes kun i takograf-kort af anden generation)
4.5.3	Førerkort
4.5.3.1	Takografapplikation (tilgængelig for køretøjsenheder af første og anden generation)
4.5.3.1.1	Identifikation af applikation
4.5.3.1.2	Nøgler og certifikater
4.5.3.1.3	Identifikation af kort
4.5.3.1.4	Identifikation af kortindehaver
4.5.3.1.5	Dataoverførsel på kort
4.5.3.1.6	Oplysninger om førerbevis
4.5.3.1.7	Data vedrørende hændelser
4.5.3.1.8	Data vedrørende fejl
4.5.3.1.9	Føreraktivitetsdata

▼B

4.5.3.1.10	Data vedrørende anvendte køretøjer
4.5.3.1.11	Steder, hvor den daglige arbejdstid begynder og/eller slutter
4.5.3.1.12	Kortsessionsdata
4.5.3.1.13	Kontrolaktivitetsdata
4.5.3.1.14	Data vedrørende særlige omstændigheder
4.5.3.2	Takografapplikation af anden generation (ikke tilgængelig for køretøjsenheder af første generation)
4.5.3.2.1	Identifikation af applikation
4.5.3.2.2	Nøgler og certifikater
4.5.3.2.3	Identifikation af kort
4.5.3.2.4	Identifikation af kortindehaver
4.5.3.2.5	Dataoverførsel på kort
4.5.3.2.6	Oplysninger om førerbevis
4.5.3.2.7	Data vedrørende hændelser
4.5.3.2.8	Data vedrørende fejl
4.5.3.2.9	Føreraktivitetsdata
4.5.3.2.10	Data vedrørende anvendte køretøjer
4.5.3.2.11	Steder og positioner, hvor den daglige arbejdstid begynder og/eller slutter
4.5.3.2.12	Kortsessionsdata
4.5.3.2.13	Kontrolaktivitetsdata
4.5.3.2.14	Data vedrørende særlige omstændigheder
4.5.3.2.15	Data vedrørende anvendte køretøjsenheder
4.5.3.2.16	Data vedrørende den position, hvor tre timers sammenhængende køretid nås
4.5.4	Værkstedskort
4.5.4.1	Takografapplikation (tilgængelig for køretøjsenheder af første og anden generation)
4.5.4.1.1	Identifikation af applikation
4.5.4.1.2	Nøgler og certifikater
4.5.4.1.3	Identifikation af kort
4.5.4.1.4	Identifikation af kortindehaver
4.5.4.1.5	Dataoverførsel på kort
4.5.4.1.6	Kalibrerings- og tidsjusteringsdata
4.5.4.1.7	Data vedrørende hændelser og fejl
4.5.4.1.8	Føreraktivitetsdata
4.5.4.1.9	Data vedrørende anvendte køretøjer
4.5.4.1.10	Data vedrørende steder, hvor den daglige arbejdstid begynder og/eller slutter
4.5.4.1.11	Kortsessionsdata
4.5.4.1.12	Kontrolaktivitetsdata

▼B

4.5.4.1.13	Data vedrørende særlige omstændigheder
4.5.4.2	Takografapplikation af anden generation (ikke tilgængelig for køretøjsenheder af første generation)
4.5.4.2.1	Identifikation af applikation
4.5.4.2.2	Nøgler og certifikater
4.5.4.2.3	Identifikation af kort
4.5.4.2.4	Identifikation af kortindehaver
4.5.4.2.5	Dataoverførsel på kort
4.5.4.2.6	Kalibrerings- og tidsjusteringsdata
4.5.4.2.7	Data vedrørende hændelser og fejl
4.5.4.2.8	Føreraktivitetsdata
4.5.4.2.9	Data vedrørende anvendte køretøjer
4.5.4.2.10	Data vedrørende steder, hvor den daglige arbejdstid begynder og/eller slutter
4.5.4.2.11	Kortsessionsdata
4.5.4.2.12	Kontrolaktivitetsdata
4.5.4.2.13	Data vedrørende anvendte køretøjsenheder
4.5.4.2.14	Data vedrørende den position, hvor tre timers sammenhængende køretid nås
4.5.4.2.15	Data vedrørende særlige omstændigheder
4.5.5	Kontrolkort
4.5.5.1	Takografapplikation (tilgængelig for køretøjsenheder af første og anden generation)
4.5.5.1.1	Identifikation af applikation
4.5.5.1.2	Nøgler og certifikater
4.5.5.1.3	Identifikation af kort
4.5.5.1.4	Identifikation af kortindehaver
4.5.5.1.5	Kontrolaktivitetsdata
4.5.5.2	Takografapplikation af anden generation (ikke tilgængelig for køretøjsenheder af første generation)
4.5.5.2.1	Identifikation af applikation
4.5.5.2.2	Nøgler og certifikater
4.5.5.2.3	Identifikation af kort
4.5.5.2.4	Identifikation af kortindehaver
4.5.5.2.5	Kontrolaktivitetsdata
4.5.6	Virksomhedskort
4.5.6.1	Takografapplikation (tilgængelig for køretøjsenheder af første og anden generation)
4.5.6.1.1	Identifikation af applikation
4.5.6.1.2	Nøgler og certifikater
4.5.6.1.3	Identifikation af kort

▼B

4.5.6.1.4	Identifikation af kortindehaver
4.5.6.1.5	Virksomhedsaktivitetsdata
4.5.6.2	Takografapplikation af anden generation (ikke tilgængelig for køretøjsenheder af første generation)
4.5.6.2.1	Identifikation af applikation
4.5.6.2.2	Nøgler og certifikater
4.5.6.2.3	Identifikation af kort
4.5.6.2.4	Identifikation af kortindehaver
4.5.6.2.5	Virksomhedsaktivitetsdata
5	MONTERING AF KONTROLAPPARATET
5.1	Montering
5.2	Installationsplade
5.3	Plombering
6	KONTROL, EFTERSYN OG REPARATIONER
6.1	Autorisering af installatører, værksteder og køretøjsfabrikanter
6.2	Kontrol af nye eller reparerede instrumenter
6.3	Monteringsinspektion
6.4	Periodisk kontrol
6.5	Måling af fejl
6.6	Reparationer
7	UDSTEDELSE AF KORT
8	TYPEGODKENDELSE AF KONTROLAPPARATUR OG TAKOGRAFKORT
8.1	Almindelige bestemmelser
8.2	Sikkerhedsattest
8.3	Funktionsattest
8.4	Interoperabilitetsattest
8.5	Typegodkendelsesattest
8.6	Undtagelsesprocedure: første interoperabilitetsattest til kontrolapparater og takografkort af anden generation

INDLEDNING

Den første generation af digitale takografsystemer har været i brug siden den 1. maj 2006. I indenlandsk transport kan de bruges, indtil de er udtjent. I international transport derimod skal alle køretøjer 15 år efter ikrafttræden af denne forordning være udstyret med en intelligent takograf af anden generation, som opfylder bestemmelserne i denne forordning.

Dette bilag indeholder kravene til anden generation af kontrolapparater og takografkort. Fra og med datoen for indførelse skal anden generation af kontrolapparater installeres i køretøjer, der registreres for første gang, og anden generation af takografkort skal udstedes.

For at fremme en gnidningsløs indførelse af anden generation af takografsystemer

▼B

— skal anden generation af takografkort udformes, så de også kan bruges i første generation af køretøjsenheder

— vil udskiftning af gyldige takografkort af første generation ikke blive krævet på datoen for indførelse.

Dette vil gøre det muligt for førere at beholde deres unikke førerkort og bruge begge systemer med det.

Anden generation af kontrolapparater vil dog kun blive kalibreret ved brug af anden generation af værkstedskort.

Dette bilag indeholder samtlige krav til interoperabiliteten mellem første og anden generation af takografsystemer.

Tillæg 15 indeholder nærmere oplysninger om, hvordan de to systemers sameksistens skal administreres.

Liste over tillæg

Tillæg 1: DATAORDLISTE

Tillæg 2: SPECIFIKATION AF TAKOGRAFKORT

Tillæg 3: PIKTOGRAMMER

Tillæg 4: UDSKRIFTER

Tillæg 5: SKÆRM

Tillæg 6: STIK TIL KALIBRERING OG DATAOVERFØRSEL PÅ FRONTPANELET

Tillæg 7: PROTOKOLLER FOR DATAOVERFØRSEL

Tillæg 8: KALIBRERINGSPROTOKOL

Tillæg 9: TYPEGODKENDELSE — LISTE OVER MINDSTEKRAV TIL PRØVER

Tillæg 10: SIKKERHEDSKRAV

Tillæg 11: FÆLLES SIKKERHEDSMEKANISMER

Tillæg 12: LOKALISERING BASERET PÅ ET GLOBALT SATELLITNAVIGATIONSSYSTEM (GNSS)

Tillæg 13: ITS-INTERFACE

Tillæg 14: FJERNKOMMUNIKATIONSFUNKTION

Tillæg 15: MIGRATION: FORVALTNING AF SAMEKSISTENSEN AF UDSTYRSGENERATIONER

Tillæg 16: ADAPTER TIL KØRETØJER I KLASSE M1 OG N1

1 DEFINITIONER

I dette bilag forstås ved:

a) »aktivering«:

den fase, hvori takografen bliver helt driftsklar og implementerer alle funktioner, herunder sikkerhedsfunktioner, ved hjælp af et værkstedskort

b) »ægthedsbekræftelse«:

en funktion, som er bestemt til at fastslå og efterprøve en påberåbt identitet

c) »ægthed«:

den egenskab ved oplysninger, at de kommer fra en part, hvis identitet kan efterprøves

d) »indbygget test (BIT)«:

test, som køres på ordre fra operatøren eller fra eksternt udstyr

▼B

e) »kalenderdag«:

et døgn fra kl. 0:00 til kl. 24:00. Alle kalenderdage går efter UTC-tid (koordineret verdenstid)

f) »kalibrering« af en intelligent takograf:

opdatering eller bekræftelse af de køretøjsparametre, som skal ligge i datalageret. Køretøjsparametre omfatter køretøjsidentifikation (VIN, VRN og den medlemsstat, der foretager registreringen) samt køretøjskarakteristika (w, k, l, dækstørrelse, hastighedsbegrænserens indstilling (hvis relevant), aktuel UTC-tid, aktuel kilometerstand). Ved kalibrering af et kontrolapparat skal type og ID for alle monterede plomber, der relevante for typegodkendelsen, også registreres i datalageret.

En opdatering eller bekræftelse, som udelukkende omfatter UTC-tid, betragtes som en tidsjustering og ikke som en kalibrering, forudsat at det ikke er i strid med krav 409.

Til kalibrering af et kontrolapparat kræves værkstedskort

g) »kortnummer«:

et nummer, som består af 16 alfanumeriske tegn og entydigt identificerer et takografkort i en medlemsstat. I kortnummeret indgår et fortløbende kortindeks (hvis relevant), et korterstatningsindeks og et kortfornyelsesindeks.

Et kort er således entydigt identificeret ved den udstedende medlemsstats kode og kortnummeret

h) »fortløbende kortindeks«:

kortnummerets 14. alfanumeriske tegn, som anvendes til at skelne mellem de forskellige kort, som udstedes til en virksomhed, et værksted eller en kontrolmyndighed med ret til at få udstedt flere forskellige takografkort. Virksomheden, værkstedet eller kontrolmyndigheden er entydigt identificeret ved de første 13 tegn i kortnummeret

i) »kortfornyelsesindeks«:

kortnummerets 16. alfanumeriske tegn, som øges, hver gang et takografkort fornys

j) »korterstatningsindeks«:

kortnummerets 15. alfanumeriske tegn, som øges, hver gang et takografkort erstattes

k) »køretøjets vejdrejetal«:

den karakteristiske størrelse, der angiver talværdien af udgangssignalet fra den køretøjsdel, der forbinder kontrolapparatet med køretøjet (gearkassens udgangsaksel eller hjulakslen), mens det tilbagelægger en afstand på 1 km under normale prøvebetingelser som defineret i krav 414. Vejdrejetallet udtrykkes i impulser pr. km (w = … imp/km)

l) »virksomhedskort«:

et takografkort, som medlemsstatens myndigheder udsteder til en transportvirksomhed, der skal betjene køretøjer monteret med en takograf, som identificerer transportvirksomheden og giver mulighed for at vise, overføre og udskrive data, der er lagret i takografen, og som denne transportvirksomhed har låst

▼B

m) »kontrolapparatets konstant«:

den karakteristiske størrelse, der angiver talværdien af det indgangssignal, som kræves for at vise og registrere en tilbagelagt afstand på 1 km. Denne konstant udtrykkes i impulser pr. km (k = … imp/km)

n) »sammenhængende køretid« beregnes i kontrolapparatet som ([1]):

Aktuel akkumuleret køretid for en given fører siden afslutningen af dennes sidste RÅDIGHED, PAUSE/HVILE eller periode, som er UKENDT ([2]) på 45 minutter eller derover (denne periode kan være fordelt i henhold til Europa-Parlamentets og Rådets forordning (EF) nr. 561/2006 ([3])). I beregningerne tages efter behov hensyn til tidligere aktiviteter, som er gemt på førerkortet. Når føreren ikke har isat sit kort, baseres beregningerne på de data, der er registreret vedrørende den aktuelle periode, hvor der ikke var isat et kort, og som vedrører den pågældende kortplads

o) »kontrolkort«:

et takografkort, som en medlemsstats myndigheder udsteder til en national kompetent kontrolmyndighed, som identificerer kontrolorganet og eventuelt kontrolmedarbejderen, og som giver adgang til de data, der er lagret i datalageret eller i førerkortene og eventuelt i værkstedskortene med henblik på læsning, udskrift og/eller dataoverførsel.

Kortet skal også give adgang til kalibreringskontrol ved vejsiden-funktionen og dataene fra læseren til kommunikationsudstyret til tidlig fjernafsløring

p) »akkumuleret pausetid« beregnes i kontrolapparatet som ([1]):

den akkumulerede kørepausetid beregnes for en given fører som de aktuelle akkumulerede perioder med RÅDIGHED, PAUSE/HVILE eller UKENDT ([2]) på hver mindst 15 minutter siden slutningen af den seneste periode af RÅDIGHED, PAUSE/HVILE eller UKENDT ([2]) periode på 45 minutter eller derover (sidstnævnte periode kan være fordelt i henhold til forordning (EF) nr. 561/2006).

I beregningerne tages efter behov hensyn til tidligere aktiviteter, som er gemt på førerkortet. Ukendte perioder, som har negativ varighed (dvs. ukendt periodes start > ukendt periodes slutning) pga. tidsoverlapning mellem to forskellige kontrolapparater, tages ikke i betragtning ved beregningen.

([1]) Denne beregningsmetode for sammenhængende køretid og akkumuleret pausetid benyttes af kontrolapparatet til beregning af advarselssignal for sammenhængende køretid. Den foregriber ikke, hvilken retlig fortolkning disse tider skal gøres til genstand for. Der kan anvendes andre metoder til beregning af den sammenhængende køretid og den akkumulerede pausetid i stedet for disse definitioner, hvis de som følge af opdateringer i anden relevant lovgivning er forældet.

([2]) Perioder med betegnelsen UKENDT er perioder, hvor førerens kort ikke var isat i et kontrolapparat, og for hvilke der ikke manuelt er indlæst føreraktiviteter.

([3]) Europa-Parlamentets og Rådets forordning (EF) nr. 561/2006 af 15. marts 2006 om harmonisering af visse sociale bestemmelser inden for vejtransport og om ændring af Rådets forordning (EØF) nr. 3821/85 og (EF) nr. 2135/98 samt ophævelse af Rådets forordning (EØF) nr. 3820/85 (EFT L 102 af 11.4.2006, s. 1)

▼B

Når føreren ikke har isat sit kort, baseres beregningerne på de data, der er registreret vedrørende den aktuelle periode, hvor der ikke var isat et kort, og som vedrører den pågældende kortplads.

q) »datalager«:

en elektronisk datalagerenhed, som er indbygget i kontrolapparatet

r) »digital underskrift«:

data, som er vedhæftet til eller er en kodet transformation af en gruppe data, og med hvilke modtageren af datagruppen kan fastslå ægthed og integritet af den pågældende gruppe data

s) »dataoverførsel«:

kopiering sammen med den digitale signatur af en del af eller et komplet sæt datafiler, som er gemt i køretøjsenhedens datalager eller i takografkortets datalager, forudsat at denne proces ikke ændrer eller sletter nogen lagrede data.

Fabrikanter af køretøjsenheder til intelligente takografer og fabrikanter af udstyr, der er konstrueret og beregnet til at overføre datafiler, træffer alle rimelige foranstaltninger til at sikre, at overførslen af sådanne data kan gennemføres med mindst mulig forsinkelse for transportvirksomheder og førere.

Det er muligvis ikke nødvendigt at overføre den detaljerede hastighedsfil for at fastslå, om forordning (EF) nr. 561/2006 er overholdt, men den kan anvendes til andre formål, f.eks. undersøgelse af en ulykke

t) »førerkort«:

et takografkort, som medlemsstatens myndigheder udsteder til en bestemt fører, og som identificerer føreren og giver mulighed for at lagre aktivitetsdata for føreren

u) »effektiv dækperiferi«:

gennemsnittet af de afstande, hvert enkelt af køretøjets trækkende hjul tilbagelægger ved en fuld omdrejning. Måling af sådanne afstande skal finde sted under normale prøvebetingelser som defineret i krav 414 og angives i formen »l = … mm«. Køretøjsfabrikanten kan erstatte måling af sådanne afstande med en teoretisk beregning, som tager hensyn til vægtfordelingen på akslerne for det driftsklare, ubelastede køretøj ([1]). Metoderne til en sådan teoretisk beregning skal godkendes af de kompetente myndigheder i en medlemsstat, og det skal ske, før takografen aktiveres

v) »hændelse«:

unormal funktion, som afsløres af den intelligente takograf og kan skyldes forsøg på misbrug

w) »eksternt GNSS-udstyr«:

udstyr, som indeholder GNSS-modtageren, når køretøjsenheden ikke er en enkeltstående enhed, og andre komponenter, der er nødvendige for at beskytte kommunikationen af placeringsdata til resten af køretøjsenheden

([1]) Kommissionens forordning (EU) nr. 1230/2012 af 12. december 2012 om gennemførelse af Europa-Parlamentets og Rådets forordning (EF) nr. 661/2009 for så vidt angår krav til typegodkendelse for masse og dimensioner for motorkøretøjer og påhængskøretøjer dertil og om ændring af Europa-Parlamentets og Rådets direktiv 2007/46/EF (EUT L 353 af 21.12.2012, s. 31), med de seneste ændringer.

▼B

x) »fejl«:

unormal funktion, som detekteres af den intelligente takograf og kan skyldes funktionsfejl ved apparatet eller svigt af dette

y) »GNSS-modtager«:

en elektronisk enhed, som modtager signaler fra et eller flere GNSS-systemer (Global Navigation Satellite System) og behandler dem digitalt for at tilvejebringe oplysninger om position, hastighed og tidspunkt

z) »montering«:

montering af en takograf i et køretøj

aa) »interoperabilitet«:

systemers og de bagvedliggende forretningsprocedurers evne til at udveksle data og dele information

bb) »grænseflade«:

en facilitet, der forbinder systemer og udgør det medium, hvorigennem de kan forbindes og fungere sammen

cc) »position«:

køretøjets geografiske koordinater på et givet tidspunkt

dd) »bevægelsessensor«:

en del af takografen, der afgiver et signal, som repræsenterer kørehastighed og/eller tilbagelagt afstand

ee) »ugyldigt kort«:

et kort, der enten findes defekt, som ikke har bestået den indledende ægthedskontrol, hvis gyldighedsperiode endnu ikke er begyndt, eller hvis udløbsdato er overskredet

ff) »åben standard«:

en standard som fastsat i et standardspecifikationsdokument, der kan fås gratis eller for et symbolsk beløb, og som det er tilladt at kopiere, distribuere eller bruge gratis eller for et symbolsk vederlag

gg) »uden for gyldighedsområdet«:

når kontrolapparat ikke kræves anvendt efter bestemmelserne i forordning (EF) nr. 561/2006

hh) »overskridelse af tilladt hastighed«:

overskridelse af tilladt hastighed for køretøjet, defineret som en vilkårlig periode på mere end 60 sekunder, i hvilken køretøjets målte hastighed overskrider den grænse for indstilling af hastighedsbegrænseren, som er fastlagt i Rådets direktiv 92/6/EØF ([1]), med senere ændringer

ii) »periodisk eftersyn«:

et sæt eftersyn, som udføres for at kontrollere, at takografen fungerer korrekt, at dens indstillinger svarer til køretøjets parametre, og at der ikke er nogen manipulerende anordninger knyttet til takografen

([1]) Rådets direktiv 92/6/EØF af 10. februar 1992 om montering og anvendelse af hastighedsbegrænsende anordninger i visse klasser af motorkøretøjer i Fællesskabet (EFT L 57 af 2.3.1992, s. 27).

▼B

jj) »printer«:

den komponent i kontrolapparatet, som leverer udskrifter af lagrede data

kk) »fjernkommunikation med henblik på tidlig afsløring«:

kommunikation mellem fjernkommunikationsudstyret til tidlig afsløring og læseren til fjernkommunikation med henblik på tidlig afsløring under målrettede vejsidekontroller med det formål at fjernregistrere mulig manipulation eller misbrug af kontroludstyr

ll) »udstyr til fjernkommunikation«:

det udstyr i køretøjsenheden, som anvendes til at udføre målrettede vejsidekontroller

mm) »læser til fjernkommunikation med henblik på tidlig afsløring«:

det system, som kontrolmedarbejdere anvender ved målrettede vejsidekontroller

nn) »fornyelse«:

udstedelse af et nyt takografkort, når et eksisterende kort enten udløber, fejlfungerer eller er blevet returneret til den udstedende myndighed. Fornyelse forudsætter altid, at der er sikkerhed for, at der ikke samtidig findes to gyldige kort

oo) »reparation«:

enhver reparation af en bevægelsessensor eller af en køretøjsenhed eller af et kabel, som kræver afbrydelse af dens strømforsyning, eller dens afbrydelse fra andre af takografens komponenter eller oplukning af bevægelsessensoren eller køretøjsenheden

pp) »korterstatning«:

udstedelse af et takografkort som erstatning for et eksisterende kort, som er erklæret tabt, stjålet eller defekt og ikke er returneret til den udstedende myndighed. Erstatning indebærer altid en risiko for, at der findes to gyldige kort samtidig

qq) »sikkerhedsattestering«:

den proces, hvorved det attesteres af et attesteringsorgan, der arbejder ud fra fælles kriterier, at kontrolapparatet (eller -komponenten) eller det undersøgte takografkort opfylder sikkerhedsforskrifterne i de relevante sikringsprofiler

rr) »selvtest«:

test, som af kontrolapparatet foretages periodisk og automatisk til afsløring af fejl

ss) »tidsmåling«:

en permanent digital registrering af den koordinerede verdenstid (UTC)

tt) »tidsjustering«:

en automatisk justering af aktuelt klokkeslæt regelmæssigt og inden for en højeste tolerance på et minut eller en justering foretaget ved kalibrering

uu) »dækstørrelse«:

dækdimensionsbetegnelse (udvendige drivende hjul) i henhold til Rådets direktiv 92/23/EØF ([1]) med senere ændringer

([1]) Rådets direktiv 92/23/EØF af 31. marts 1992 om dæk til motorkøretøjer og påhængskøretøjer samt om montering heraf (EFT L 129 af 14.5.1992, s. 95).

▼B

vv) »køretøjsidentifikation«:

de numre, som identificerer køretøjet: køretøjets indregistreringsnummer (VRN) med angivelse af den medlemsstat, hvor det er indregistreret, og køretøjets identifikationsnummer (VIN) ([1])

ww) til beregningsformål i kontrolapparatet forstås ved »uge«:

tidsrummet fra mandag kl. 00:00 UTC til søndag kl. 24:00 UTC

xx) »værkstedskort«:

et takografkort, som medlemsstatens myndigheder udsteder til udpeget personale hos en fabrikant af takografer, en installatør, en køretøjsfabrikant eller i et værksted, som er autoriseret af samme medlemsstat, som identificerer kortindehaveren og giver mulighed for afprøvning, kalibrering og aktivering af og/eller dataoverførsel fra takograferne

yy) »adapter«:

en anordning, der afgiver et signal, som vedvarende repræsenterer kørehastighed og/eller tilbagelagt distance, som ikke er den samme som den anordning, der bruges til uafhængig registrering af bevægelser, og som:

— alene installeres og anvendes i køretøjer af typerne M1 og N1 (som defineret i bilag II til Europa-Parlamentets og direktiv 2007/46/EF ([2]), med senere ændringer), der er taget i brug efter den 1. maj 2006

— installeres, når det mekanisk set ikke er muligt at installere nogen anden eksisterende type af bevægelsessensor, som er i overensstemmelse med de øvrige bestemmelser i dette bilag og de tilknyttede tillæg 1-15

— installeres mellem køretøjsenheden og det sted, hvor de hastigheds/afstandsrelaterede impulser genereres af integrerede følere eller alternative tilkoblinger

— set i forhold til køretøjsenheden fungerer adapteren, som om en bevægelsessensor, der opfylder bestemmelserne i dette bilag og de tilknyttede tillæg 1-16, var tilsluttet køretøjsenheden.

Anvendelsen af en sådan adapter i de ovenfor beskrevne køretøjer skal muliggøre installation og korrekt anvendelse af en køretøjsenhed, der opfylder alle krav i dette bilag.

For sådanne køretøjer omfatter den intelligente takograf kabler, en adapter og en køretøjsenhed.

([1]) Rådets direktiv 76/114/EØF af 18. december 1975 om indbyrdes tilnærmelse af medlemsstaternes lovgivning vedrørende skilte og foreskrevne påskrifter og disses anbringelsessted og -måde for motordrevne køretøjer og påhængskøretøjer dertil (EFT L 24 af 30.1.1976, s. 1).

([2]) Europa-Parlamentets og Rådets direktiv 2007/46/EF af 5. september 2007 om fastlæggelse af en ramme for godkendelse af motorkøretøjer og påhængskøretøjer dertil samt af systemer, komponenter og separate tekniske enheder til sådanne køretøjer (»Rammedirektiv«) (EUT L 263 af 9.10.2007, s. 1).

▼B

zz) »dataintegritet«:

sikring af, at lagrede data er nøjagtige og konsekvente, hvilket er kendetegnet ved, at der ikke er foretaget ændring af data mellem to opdateringer af en datapost. Integritet indebærer, at dataene er en nøjagtig kopi af den oprindelige udgave, f.eks. at de ikke er blevet beskadiget under indlæsning i eller udlæsning fra et takografkort eller en dedikeret enhed eller under transmission via en kommunikationskanal.

aaa) »beskyttelse af personlige data«:

de generelle tekniske foranstaltninger, som træffes for at sikre korrekt gennemførelse af de principper, der er fastlagt i Europa-Parlamentets og Rådets direktiv 95/46/EF ([1]), og de principper, der er fastlagt i Europa-Parlamentets og Rådets direktiv 2002/58/EF ([2])

bbb) »intelligent takografsystem«:

det kontrolapparat, de takografkort og alt det udstyr, der direkte eller indirekte indgår i et samspil under konstruktion, montering, brug, afprøvning og kontrol, såsom kort, læsere til fjernkommunikation og andet udstyr til dataoverførsel, dataanalyse, kalibrering og frembringelse, styring eller indførelse af sikkerhedselementer osv.

ccc) »dato for indførelse«:

36 måneder efter ikrafttrædelsesdatoen for de detaljerede bestemmelser i artikel 11 i Europa-Parlamentets og Rådets forordning (EU) nr. 165/2014 ([3]).

Denne er datoen, efter hvilken køretøjer, der er registreret for første gang,

— *skal være udstyret med en takograf med forbindelse til en positioneringstjeneste, der er baseret på et satellitnavigationssystem*

— *skal kunne sende data til brug ved målrettede vejsidekontroller til kompetente tilsynsførende myndigheder, mens køretøjet er i bevægelse*

— *og kan udstyres med standardiserede grænseflader, som muliggør brug af de data, der registreres eller frembringes af takografer, i en ekstern anordning under drift*

ddd) »sikringsprofil«:

et dokument, der anvendes i forbindelse med certificeringsprocessen ud fra fælles kriterier, og som indeholder en implementeringsuafhængig specifikation af sikkerhedskrav

([1]) Europa-Parlamentets og Rådets direktiv 95/46/EF af 24. oktober 1995 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (EFT L 281 af 23.11.1995, s. 31).

([2]) Europa-Parlamentets og Rådets direktiv 2002/58/EF af 12. juli 2002 om behandling af personoplysninger og beskyttelse af privatlivets fred i den elektroniske kommunikationssektor (Direktiv om databeskyttelse inden for elektronisk kommunikation) (EFT L 201 af 31.7.2002, s. 37).

([3]) Europa-Parlamentets og Rådets forordning (EU) nr. 165/2014 af 4. februar 2014 om takografer inden for vejtransport, om ophævelse af Rådets forordning (EØF) nr. 3821/85 om kontrolapparatet inden for vejtransport og om ændring af Europa-Parlamentets og Rådets forordning (EF) nr. 561/2006 om harmonisering af visse sociale bestemmelser inden for vejtransport (EUT L 60 af 28.2.2014, s. 1).

▼B

eee) »GNSS-nøjagtighed«:

betyder i forbindelse med registrering af positioner ud fra GNSS med takografer den talværdi for HDOP (Horizontal Dilution of Precision), som beregnes ud fra den mindste af de HDOP-værdier, der indsamles på de tilgængelige GNSS-systemer.

2 KONTROLAPPARATETS GENERELLE EGENSKABER OG FUNKTIONER

2.1 **Generelle egenskaber**

Kontrolapparatet har til formål at registrere, gemme, vise, udprinte og udlæse data vedrørende førerens aktiviteter.

Køretøjer, der er udstyret med kontrolapparat, som opfylder forskrifterne i dette bilag, skal være forsynet med hastighedsviser og kilometertæller. Disse funktioner skal være indeholdt i kontrolapparatet.

01) Kontrolapparatet omfatter kabler, en bevægelsessensor og en køretøjsenhed.

02) Grænsefladen mellem bevægelsessensorer og køretøjsenheder skal opfylde bestemmelserne i tillæg 11.

03) Køretøjsenheden skal være tilsluttet et eller flere globale satellitnavigationssystemer som anført i tillæg 12.

04) Køretøjsenheden skal kommunikere med udstyr til fjernkommunikation som anført i tillæg 14.

05) Køretøjsenheden kan omfatte en ITS-grænseflade som anført i tillæg 13.

Kontrolapparatet kan være tilsluttet andre faciliteter gennem ekstra grænseflader og/eller gennem den valgfri ITS-grænseflade.

06) Funktioner og anordninger, som indsættes i eller tilsluttes kontrolapparatet må, hvad enten de er godkendt eller ej, ikke forstyrre eller kunne forstyrre den korrekte og sikre funktion af kontrolapparatet eller overholdelsen af denne forordnings bestemmelser.

Kontrolapparatets brugere identificerer sig over for apparatet gennem takografkort.

07) Kontrolapparatet giver selektiv adgangsret til data og funktioner, afhængigt af brugerens type og/eller identitet.

Kontrolapparatet registrerer og gemmer data i sit datalager, i faciliteten til fjernkommunikation og på takografkortene.

Dette foregår i overensstemmelse med direktiv 95/46/EF af 24. oktober 1995 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger ([1]), direktiv 2002/58/EF af 12. juli 2002 om behandling af personoplysninger og beskyttelse af privatlivets fred i den elektroniske kommunikationssektor ([2]) samt artikel 7 i forordning (EU) nr. 165/2014.

([1]) EFT L 281 af 23.11.1995, s. 31.
([2]) EFT L 201 af 31.7.2002, s. 37.

▼B

2.2 **Funktioner**

08) Kontrolapparatet skal garantere følgende funktioner:

— overvågning af isætninger og udtagninger af kort

— måling af hastighed, afstand og position

— tidsmåling

— overvågning af førerens aktiviteter

— overvågning af kørestatus

— manuel indlæsning foretaget af føreren:

— indlæsning af de steder, hvor den daglige arbejdstid begynder og/eller slutter,

— manuel indlæsning af førerens aktiviteter

— indlæsning af særlige omstændigheder

— forvaltning af virksomhedslåse

— overvågning af kontrolaktiviteter

— detektion af hændelser og/eller fejl

— indbyggede tester og selvtester

— læsning fra datalager

— registrering og lagring i datalager

— læsning fra takografkort

— registrering og lagring på takografkort

— visning på skærm

— udprintning

— advarsler

— overførsel af data til eksterne medier

— fjernkommunikation i forbindelse med målrettede vejside-kontroller

— udlæsning af data til supplerende faciliteter

— kalibrering

— kalibreringskontrol ved vejsiden

— tidsjustering.

2.3 **Funktionstilstande**

09) Kontrolapparatet skal have fire funktionstilstande:

— driftstilstand

— kontroltilstand

— kalibreringstilstand

— virksomhedstilstand.

10) Kontrolapparatet skal skifte til følgende funktionstilstand, afhængigt af de gyldige takografkort, som indsættes i kortlæserne. Ved bestemmelse af funktionstilstanden er genereringen af takografkortet irrelevant, forudsat at det isatte kort er gyldigt. Et værkstedskort af første generation skal altid betragtes som ugyldigt, hvis det sættes i en køretøjsenhed af anden generation.

▼B

Funktionstilstand		Førerkortplads				
		Intet kort	Førerkort	Kontrolkort	Værkstedskort	Virksomhedskort
Kortplads for medchauffør	Intet kort	Operationelt	Operationelt	Kontrol	Kalibrering	Virksomhed
	Førerkort	Operationelt	Operationelt	Kontrol	Kalibrering	Virksomhed
	Kontrolkort	Kontrol	Kontrol	Kontrol (*)	Operationelt	Operationelt
	Værkstedskort	Kalibrering	Kalibrering	Operationelt	Kalibrering (*)	Operationelt
	Virksomheds-kort	Virksomhed	Virksomhed	Operationelt	Operationelt	Virksomhed (*)

(*) I disse situationer skal kontrolapparatet kun bruge det takografkort, der sættes i førerkortpladsen.

11) Kontrolapparatet skal ignorere ugyldige kort, som indsættes; dog skal det kunne vise, printe og overføre data, som ligger på et udgået kort.

12) Alle de i punkt 2.2 angivne funktioner skal virke i alle funktionstilstande, med følgende undtagelser:

— Kalibreringsfunktionen er kun tilgængelig i kalibreringstilstand

— Funktionen til kalibreringskontrol ved vejsiden er kun tilgængelig i kontroltilstand

— Funktionen styring af virksomhedslåse er kun tilgængelig i virksomhedstilstand

— Funktionen overvågning af kontrolaktivitet er operationel i kontroltilstand

— Dataoverførselsfunktionen er ikke tilgængelig i driftstilstand (bortset fra det i krav 193 fastlagte), undtagen ved overførsel af et førerkort, når der ikke er indsat andre korttyper i køretøjsenheden.

13) Kontrolapparatet kan udlæse alle data til skærm, printer og eksterne grænsefladeenheder, med følgende undtagelser:

— I driftstilstand slettes enhver personlig identifikation (efternavn og fornavn), som ikke modsvarer det isatte takografkort; alle kortnumre, som ikke svarer til det isatte kort, bliver delvis slettet (hver andet tegn — fra venstre mod højre — bliver slettet).

— I virksomhedstilstand kan førerrelaterede data (krav 102, 105 og 108) kun udlæses for perioder, som ikke er låst, eller som ingen anden virksomhed (således som denne er identificeret ved de første 13 cifre i virksomhedskortnummeret) har låst.

— Når der intet kort sidder i kontrolapparatet, kan førerrelaterede data kun udlæses for den aktuelle dato og de otte foregående kalenderdage.

— Personoplysninger, der stammer fra køretøjsenheden, må ikke udlæses gennem enhedens ITS-grænseflade, medmindre samtykket fra den fører, som dataene vedrører, verificeres.

▼B

— Køretøjsenhederne har en gyldighedsperiode for normale operationer på 15 år fra og med den dato, hvor køretøjsenhedens certifikater blev udstedt, men køretøjsenheder kan anvendes i yderligere tre måneder, dog kun til dataoverførsel.

2.4 **Sikkerhed**

Med sikringen af systemet tilstræbes det at beskytte datahukommelsen på en sådan måde, at uvedkommende ikke kan få adgang til og manipulere med data, og således at forsøg herpå opdages, beskytte integriteten og ægtheden af data, som udveksles mellem bevægelsessensor og køretøjsenhed, beskytte integriteten og ægtheden af data, som udveksles mellem kontrolapparat og takografkort, beskytte integriteten og ægtheden af data, der udveksles mellem kontrolapparat og eksternt GNSS-udstyr, beskytte fortroligheden, integriteten og ægtheden af data, som udveksles gennem udstyret til fjernkommunikation med henblik på tidlig afsløring til kontrolformål, samt verificere integriteten og ægtheden af overførte data.

14) Af hensyn til systemets sikkerhed skal følgende komponenter opfylde sikkerhedsforskrifterne i deres sikringsprofiler som foreskrevet i tillæg 10:

— køretøjsenhed

— takografkort

— bevægelsessensor

— eksternt GNSS-udstyr (denne profil kræves og gælder kun for den eksterne GNSS-variant).

3 KONSTRUKTIONS- OG FUNKTIONSKRAV TIL KONTROLAPPARAT

3.1 **Overvågning af isætning og udtagning af kort**

15) Kontrolapparatet skal overvåge isætning og udtagning af kort i kortlæseenhederne.

16) Når et kort isættes, skal kontrolapparatet detektere, om kortet er et gyldigt takografkort, og, i bekræftende fald, dets type og generation.

Hvis et kort med samme kortnummer og et højere fornyelsesindeks allerede har været isat i kontrolapparatet, skal kontrolapparatet anse kortet for ugyldigt.

Hvis et kort med samme kortnummer og fornyelsesindeks, men med et højere korterstatningsindeks allerede har været isat i kontrolapparatet, skal kontrolapparatet anse kortet for ugyldigt.

17) Første generation af takografkort skal betragtes som ugyldige af kontrolapparatet, efter at muligheden for at bruge første generation af takografkort er blevet udelukket af et værksted i overensstemmelse med tillæg 15 (krav MIG003).

18) Første generation af værkstedskort, som sættes i kontrolapparater af anden generation, skal betragtes som ugyldige.

▼B

19) Kontrolapparatet skal være konstrueret således, at det låser takografkortene i stilling, når de isættes korrekt i kortlæserne.

20) Frigivelse af takografkort må kun være mulig, når køretøjet holder stille, og efter at de relevante data er blevet gemt på kortene. Frigivelse af kortet må kun kunne ske ved et aktivt indgreb af brugeren.

3.2 **Måling af hastighed, position og afstand**

21) Bevægelsessensoren (som kan være indlejret i adapteren) er det vigtigste værktøj til måling af hastighed og afstand.

22) Denne funktion skal til stadighed måle og kunne angive den kilometerstand, der svarer til den totale afstand tilbagelagt af køretøjet ved brug af impulserne fra bevægelsessensoren.

23) Desuden skal funktionen til stadighed måle og kunne angive køretøjets hastighed ved brug af impulserne fra bevægelsessensoren.

24) Hastighedsmålefunktionen skal endvidere kunne angive, om køretøjet er i bevægelse eller holder stille. Køretøjet anses for at være i bevægelse, så snart funktionen detekterer flere end 1 imp/sek. fra bevægelsessensoren i mindst fem sekunder, ellers anses det for at holde stille.

25) Anordninger, som viser hastighed (speedometer) og total tilbagelagt distance (kilometertæller) og er monteret i et køretøj med et kontrolapparat, som opfylder denne forordnings bestemmelser, skal opfylde forskrifterne for tilladelige maksimale tolerancer i dette bilag (se 3.2.1 og 3.2.2).

26) For at opdage manipulation af køredata for køretøjet skal oplysninger fra bevægelsessensoren bekræftes af oplysninger om køretøjets bevægelse fra GNSS-modtageren og eventuelt fra en eller flere andre kilder, som er uafhængige af bevægelsessensoren.

27) Denne funktion skal måle køretøjets position for at muliggøre automatisk registrering af:

— positioner, hvor føreren og/eller medchaufføren påbegynder sin daglige arbejdsperiode

— positioner, hvor førerens sammenhængende køretid når op på et multiplum af tre timer

— positioner, hvor føreren og/eller medchaufføren afslutter sin daglige arbejdsperiode.

3.2.1 *Måling af den tilbagelagte vejstrækning*

28) Den tilbagelagte afstand kan måles enten:

— så både fremadkørsel og bagudkørsel medregnes, eller

— ved fremadkørsel alene.

29) Kontrolapparatet skal måle afstande fra 0 til 9 999 999,9 km.

▼B

30) Ved afstandsmåling skal tolerancen være inden for følgende grænser (afstande på mindst 1 000 m):

— ± 1 % før montering

— ± 2 % ved montering og periodisk eftersyn

— ± 4 % under brug.

31) Afstandsmålingen skal have en opløsning på 0,1 km eller bedre.

3.2.2 *Måling af hastigheden*

32) Kontrolapparatet skal måle hastigheder fra 0 til 220 km/t.

33) For at sikre maksimal tolerance på den viste hastighed på ± 6 km/t under brug, og under hensyntagen til:

— en tolerance på ± 2 km/t på variationer i inddata (dækvariationer, …)

— en tolerance på ± 1 km/t på målinger udført under montering og periodiske eftersyn

skal kontrolapparatet ved hastigheder mellem 20 og 180 km/t, og ved vejdrejetal af køretøjet mellem 4 000 og 25 000 imp/km, måle hastigheden med en tolerance på ± 1 km/t (ved konstant hastighed).

Bemærk: Datalagringens opløsning medfører, at der skal tillægges en yderligere tolerance på ± 0,5 km/t på den hastighed, der er gemt af kontrolapparatet.

34) Inden for 2 sekunder efter afslutning af en hastighedsændring skal hastighedsmåling kunne foretages korrekt med de normale tolerancer, når hastighedsændringen er sket i et tempo på indtil 2 m/s^2.

35) Hastighedsmålingen skal have en opløsning på minimum 1 km/t.

3.2.3 *Måling af position*

36) Kontrolapparatet skal måle køretøjets absolutte position ved hjælp af GNSS-modtageren.

37) Den absolutte position måles i geografiske koordinater for breddegrad og længdegrad i grader og minutter med en opløsning på 1/10 af et minut.

3.3 **Tidsmåling**

38) Tidsmålefunktionen skal permanent og digitalt levere UTC-dato og -tid.

39) Der anvendes UTC-dato og -tid til at tidsbestemme data i kontrolapparatet (registreringer, dataudveksling) og til alle udskrifter, der er anført i tillæg 4 »Udskrifter«.

40) For at lokal tid kan vises, skal forskydningen af den viste tid kunne ændres i trin på en halv time. Ingen andre forskydninger end negative eller positive multipla af halve timer er tilladt.

41) Tidspunktdriften skal være inden for ± 2 sekunder i døgnet under typegodkendelsesomstændigheder og uden tidsjustering.

▼B

42) Tidsmålingens opløsning skal være minimum 1 sekund.

43) Tidsmålingen må under typegodkendelsesomstændigheder ikke kunne påvirkes af en afbrydelse i den eksterne strømforsyning på mindre end 12 måneder.

3.4 **Overvågning af føreraktiviteter**

44) Denne funktion skal permanent og særskilt overvåge aktiviteterne af én fører og én medchauffør.

45) Føreraktiviteter skal bestå i KØRSEL, ARBEJDE, RÅDIGHED eller PAUSE/HVILE.

46) Fører og/eller medchauffør skal manuelt kunne vælge ARBEJDE, RÅDIGHED eller PAUSE/HVILE.

47) Når køretøjet bevæger sig, skal der automatisk vælges KØRSEL for føreren og RÅDIGHED for medchaufføren.

48) Når køretøjet standser, skal der automatisk vælges ARBEJDE for føreren.

49) Det første aktivitetsskift til HVILE eller RÅDIGHED, som finder sted inden for 120 sekunder efter det ved standsning af køretøjet udløste automatiske skift til ARBEJDE, antages at have fundet sted på tidspunktet for køretøjets standsning (således at skiftet til ARBEJDE eventuelt ophæves).

50) Denne funktion skal udlæse aktivitetsskift til kontrolfunktionerne med en opløsning på et minut.

51) Er der for et givet kalenderminut registreret KØRSEL som aktivitet i både det umiddelbart foregående og umiddelbart efterfølgende minut, anses hele det pågældende minut for KØRSEL.

52) Et givet kalenderminut, der ikke anses for KØRSEL efter krav 051, anses for at bestå udelukkende af samme aktivitet som den længstvarende uafbrudte aktivitet i det pågældende minut (eller, for lige længe varende aktiviteter, den senest forekommende af disse).

53) Denne funktion skal endvidere overvåge førerens kontinuerlige køretid og akkumulerede pausetid.

3.5 **Overvågning af kørestatus**

54) Denne funktion overvåger kørestatus permanent og automatisk.

55) Som kørestatus vælges FØRERHOLD, når der er isat to gyldige førerkort i apparatet; i alle andre tilfælde vælges ÉN FØRER som kørestatus.

3.6 **Indlæsning foretaget af fører**

3.6.1 *Indlæsning af de steder, hvor den daglige arbejdstid begynder og/eller slutter*

56) Denne funktion skal give mulighed for indlæsning af de steder, hvor den daglige arbejdstid begynder og/eller slutter for fører og/eller medchauffør ifølge vedkommende selv.

▼B

57) Ved steder forstås den pågældende stat samt, hvor det er relevant, region, som indlæses eller bekræftes manuelt.

58) Ved udtagning af førerkort skal kontrolapparatet påminde fører eller medchauffør om at indlæse et »sted, hvor den daglige arbejdstid slutter«.

59) Føreren skal derefter indlæse køretøjets aktuelle placering, som anses for at være en midlertidig indlæsning.

60) Det skal være muligt at indlæse steder, hvor den daglige arbejdstid begynder og/eller slutter, ved hjælp af kommandoer i menuerne. Hvis der foretages mere end én sådan indlæsning inden for et kalenderminut, bevares kun den sidste indlæsning af begyndelsesstedet og den sidste indlæsning af slutstedet, som er foretaget inden for dette tidsrum.

3.6.2 *Manuel indlæsning af føreraktiviteter og førerens samtykke til brug af ITS-grænsefladen*

61) Kontrolapparatet skal efter isætning af fører- eller værkstedskortet, og først på det tidspunkt, tillade manuel indlæsning af aktiviteter. Manuel indlæsning af aktiviteter foretages med lokal tid og dato i den tidszone (UTC-forskydning), som køretøjsenheden aktuelt er indstillet til.

Ved isætning af fører- eller værkstedskort skal kortindehaveren mindes om:

— dato og klokkeslæt for den sidste udtagning af det pågældende kort

— valgfrit: den lokale tidsforskydning, som aktuelt er indstillet for køretøjsenheden.

Ved første isætning af et førerkort eller værkstedskort, som køretøjsenheden ikke kender, skal kortholderen opfordres til at give sit samtykke til udlæsning af takografrelaterede personoplysninger gennem den valgfri ITS-grænseflade.

Dette samtykke kan til enhver tid gives eller trækkes tilbage ved hjælp af kommandoer i menuen, forudsat at førerkortet eller værkstedskortet er isat.

Det skal være muligt at indlæse aktiviteter inden for følgende begrænsninger:

— Aktivitetstypen skal være ARBEJDE, RÅDIGHED eller PAUSE/HVILE

— Start- og sluttidspunkterne for hver aktivitet skal ligge inden for perioden mellem den sidste kortudtagning og den aktuelle isætning

— Aktiviteterne må ikke overlappe hinanden i tid.

Det skal være muligt at foretage manuelle indlæsninger ved den første isætning af et fører- eller værkstedskort, som ikke tidligere har været anvendt.

▼B

Proceduren for manuel indlæsning af aktiviteter skal bestå af lige så mange på hinanden følgende trin, som er nødvendige for at indstille en aktivitetstype og et start- og et sluttidspunkt for hver aktivitet. For enhver del af tidsperioden mellem den sidste kortudtagning og den aktuelle kortisætning skal kortindehaveren have mulighed for ikke at registrere nogen aktivitet.

Under de manuelle indlæsninger i forbindelse med kortisætningen skal kortindehaveren, hvis relevant, have mulighed for at indlæse:

— et sted, hvor en tidligere daglig arbejdsperiode er sluttet, og det tilknyttede tidspunkt (hvorved den indlæsning, der skete ved den sidste kortudtagning, overskrives)

— et sted, hvor den nuværende daglige arbejdsperiode begynder, og det tilknyttede tidspunkt.

Hvis kortindehaveren ikke indlæser et sted, hvor arbejdsperioden begynder eller slutter, under de manuelle indlæsninger i forbindelse med kortisætningen, anses dette for en angivelse af, at arbejdsperioden ikke har ændret sig siden den sidste kortudtagning. Den næste indlæsning af et sted, hvor en tidligere daglig arbejdsperiode ender, overskriver så den midlertidige indlæsning, der blev foretaget ved den sidste kortudtagning.

Hvis der indlæses et sted, skal det registreres i det relevante takografkort.

Manuelle indlæsninger skal afbrydes, hvis:

— kortet tages ud, eller

— køretøjet er i bevægelse og kortet sidder i førerens kortplads.

Yderligere afbrydelser er tilladt, f.eks. en timeout efter en vis periode med brugerinaktivitet. Hvis manuelle indlæsninger bliver afbrudt, skal kontrolapparatet godkende alle komplette indlæsninger af steder og aktiviteter (med enten entydigt sted og tid eller aktivitetstype og start- og sluttidspunkt), som allerede er foretaget.

Hvis der isættes et andet fører- eller værkstedskort, mens der er ved at blive foretaget manuelle indlæsninger af aktiviteter for et tidligere isat kort, skal de manuelle indlæsninger for det tidligere kort afsluttes, før der påbegyndes manuelle indlæsninger af det andet kort.

Kortindehaveren skal have mulighed for at tilføje manuelle indlæsninger i henhold til følgende minimumsprocedure:

— Manuel indlæsning af aktiviteter i kronologisk rækkefølge for perioden mellem den sidste kortudtagning og den aktuelle isætning.

— Starttidspunktet for den første aktivitet skal være sat til kortudtagningstidspunktet. For hver efterfølgende indlæsning skal starttidspunktet være forud sat således, at det følger umiddelbart efter den tidligere indlæsning. Der skal vælges aktivitetstype og sluttidspunkt for hver aktivitet.

▼B

Denne proces skal slutte, når sluttidspunktet for en manuelt indlæst aktivitet er lig kortisætningstidspunktet. Kontrolapparatet kan derefter eventuelt give kortindehaveren mulighed for at ændre en manuelt indlæst aktivitet, indtil den godkendes ved valg af en bestemt kommando. Derefter skal det være forbudt at foretage enhver sådan ændring.

3.6.3 *Indlæsning af særlige omstændigheder*

62) Kontrolapparatet skal give føreren mulighed for tidstro indlæsning af følgende to særlige omstændigheder:

— »UDEN FOR GYLDIGHEDSOMRÅDE« (start, slut)

— »OVERFART MED FÆRGE/TOG« (start, slut)

»OVERFART MED FÆRGE/TOG« kan ikke finde sted, når betingelsen »UDEN FOR GYLDIGHEDSOMRÅDE« er åbnet.

Er betingelsen »UDEN FOR GYLDIGHEDSOMRÅDE« åbnet, skal den automatisk lukkes af kontrolapparatet ved isætning eller udtagning af et førerkort.

Hvis betingelsen »UDEN FOR GYLDIGHEDSOMRÅDE« er åbnet, skal det forhindre følgende hændelser og advarsler:

— Kørsel uden behørigt kort

— Advarsler forbundet med sammenhængende køretid.

Markeringen af starten på tilstanden »OVERFART MED FÆRGE/TOG« skal angives, før føreren slukker motoren om bord på færgen/toget.

Tilstanden OVERFART MED FÆRGE/TOG slutter i følgende tilfælde:

— Føreren afslutter tilstanden OVERFART MED FÆRGE/TOG manuelt.

— Føreren tager sit kort ud.

En åbnet OVERFART MED FÆRGE/TOG skal afsluttes, når den ikke længere er gyldig på basis af reglerne i forordning (EF) nr. 561/2006.

3.7 **Forvaltning af virksomhedslåse**

63) Denne funktion skal give mulighed for styring af de låse, som oprettes af en virksomhed for at dataadgangen er forbeholdt virksomheden, når systemet er i virksomhedstilstand.

64) Virksomhedslåse består af startdato/klokkeslæt (lås-ind) og slutdato/klokkeslæt (lås-ud), knyttet til virksomhedens identitet som angivet af virksomhedskortets nummer (ved lås-ind).

65) Lås »ind« og lås »ud« kan kun foretages i realtid.

66) Enten skal kun den virksomhed kunne låse ud, som har låst »ind« (som angivet ved de første 13 cifre i virksomhedskortets nummer), eller også

67) skal lås-ud udføres automatisk, hvis en anden virksomhed låser ind.

▼B

68) Hvis en virksomhed låser ind, hvor forudgående lås var for samme virksomhed, antages det, at forudgående lås ikke er låst »ud« og stadig er »ind«.

3.8 **Overvågning af kontrolaktiviteter**

69) Denne funktion skal overvåge aktiviteterne VISNING PÅ SKÆRM, UDPRINTNING, UDLÆSNING på køretøjsenhed og kort samt KALIBRERINGSKONTROL VED VEJSIDEN, som finder sted i kontroltilstand.

70) Funktionen skal endvidere overvåge aktiviteter vedrørende KONTROL MED OVERSKRIDELSE AF TILLADT HASTIGHED i kontroltilstand. Kontrol med overskridelse af tilladt hastighed anses for at have fundet sted, når en udskrift om »overskridelse af tilladt hastighed« er sendt til printer eller til skærm, eller når der er overført data vedrørende »hændelser og fejl« fra køretøjsenhedens datalager.

3.9 **Detektion af hændelser og/eller fejl**

71) Denne funktion detekterer følgende hændelser og/eller fejl:

3.9.1 *Hændelsen »isætning af ugyldigt kort«*

72) Denne hændelse skal udløses ved isætning af et vilkårligt ugyldigt kort, ved isætning af et førerkort, der allerede er udskiftet, og/eller ved udløb af et isat gyldigt kort.

3.9.2 *Hændelsen »kortkonflikt«*

73) Denne hændelse skal udløses når en af de kombinationer af gyldige kort, som angivet med X i følgende tabel, forekommer:

Kortkonflikt		Førerkortplads				
		Intet kort	Førerkort	Kontrolkort	Værkstedskort	Virksomhedskort
Kortplads for medchauffør	Intet kort					
	Førerkort				X	
	Kontrolkort			X	X	X
	Værkstedskort		X	X	X	X
	Virksomhedskort			X	X	X

3.9.3 *Hændelsen »tidsoverlapning«*

74) Denne hændelse skal udløses, når dato/klokkeslæt for seneste udtagning af førerkort, læst på kortet, er senere end aktuel dato/aktuelt klokkeslæt på det kontrolapparat, hvori kortet indsættes.

3.9.4 *Hændelsen »kørsel uden behørigt kort«*

75) Denne hændelse skal udløses for enhver af de gyldige kombinationer af takografkort, som er angivet med X i følgende tabel, når føreraktiviteten skifter til KØRSEL, eller når der skiftes funktionstilstand, mens føreraktiviteten er KØRSEL:

▼B

Kørsel uden behørigt kort		Førerkortplads				
		Intet (eller ugyldigt) kort	Førerkort	Kontrolkort	Værkstedskort	Virksomhedskort
Kortplads for medchauffør	Intet (eller ugyldigt) kort	X		X		X
	Førerkort	X		X	X	X
	Kontrolkort	X	X	X	X	X
	Værkstedskort	X	X	X		X
	Virksomhedskort	X	X	X	X	X

3.9.5 *Hændelsen »isætning af kort under kørslen«*

76) Denne hændelse skal udløses, når der indsættes et takografkort i en vilkårlig kortplads, mens føreraktiviteten er KØRSEL.

3.9.6 *Hændelsen »sidste kortsession ikke korrekt afsluttet«*

77) Denne hændelse skal udløses, når kontrolapparatet ved isætning af kortet konstaterer, at foregående kortsession trods bestemmelserne i punkt 3.1 ikke er blevet afsluttet korrekt (kortet er taget ud, før alle relevante data er blevet gemt på kortet). Denne hændelse er kun relevant for fører- og værkstedskort.

3.9.7 *Hændelsen »overskridelse af tilladt hastighed«*

78) Denne hændelse skal udløses for hver overskridelse af tilladt hastighed.

3.9.8 *Hændelsen »afbrydelse af strømforsyning«*

79) Denne hændelse skal udløses ved enhver sådan afbrydelse af strømforsyningen til bevægelsessensor og/eller køretøjsenhed, som sker i en anden måde end kalibrerings- eller kontroltilstand og varer over 200 millisekunder. Afbrydelsestærsklen fastlægges af fabrikanten. Det fald i spændingsforsyningen, som fremkommer ved start af køretøjets motor, må ikke udløse denne hændelse.

3.9.9 *Hændelsen »fejl ved kommunikation med faciliteten til fjernkommunikation«*

80) Denne hændelse skal udløses **uden for kalibreringstilstand**, hvis faciliteten til fjernkommunikation ikke kvitterer for modtagelse af fjernkommunikationsdata sendt fra køretøjsenheden ved mere end tre forsøg.

3.9.10 *Hændelsen »manglende positionsoplysninger fra GNSS-modtager«*

81) Denne hændelse skal udløses **uden for kalibreringstilstand** i tilfælde af manglende positionsoplysninger fra GNSS-modtageren (intern eller ekstern) i mere end tre timer af akkumuleret køretid.

3.9.11 *Hændelsen »fejl ved kommunikation med det eksterne GNSS-udstyr«*

82) Denne hændelse skal udløses **uden for kalibreringstilstand** i tilfælde af afbrydelse af kommunikationen mellem det eksterne GNSS-udstyr og køretøjsenheden i mere end 20 minutter i træk, mens køretøjet er i bevægelse.

▼B

3.9.12 *Hændelsen »fejl ved køredata«*

83) Denne hændelse skal udløses **uden for kalibreringstilstand** ved afbrydelse af den normale dataudveksling mellem bevægelsessensor og køretøjsenhed og/eller ved fejl i dataintegritet eller -ægthedskontrol under dataudveksling mellem bevægelsessensor og køretøjsenhed.

3.9.13 *Hændelsen »køretøjsbevægelseskonflikt«*

84) Denne hændelse skal udløses **uden for kalibreringstilstand**, hvis den registrerede bevægelse er i strid med bevægelsesoplysninger beregnet ud fra bevægelsessensoren er i modstrid med bevægelsesoplysninger beregnet ud fra den interne GNSS-modtager eller fra det eksterne GNSS-udstyr og eventuelt andre uafhængige kilder, som anført i tillæg 12. Denne hændelse skal ikke udløses under en overfart med færge/tog, under omstændigheden »UDEN FOR GYLDIGHEDSOMRÅDE«, eller når der ikke foreligger positionsoplysninger fra GNSS-modtageren.

3.9.14 *Hændelsen »forsøg på sikkerhedsbrud«*

85) Denne hændelse skal udløses ved enhver anden hændelse, der berører sikkerheden ved bevægelsessensor og/eller køretøjsenhed og/eller det eksterne GNSS-udstyr som foreskrevet i tillæg 10, og som ikke finder sted i kalibreringstilstand.

3.9.15 *Hændelsen »tidskonflikt«*

86) Denne hændelse skal udløses **uden for kalibreringstilstand**, hvis køretøjsenheden registrerer en forskel på mere end 1 minut mellem tiden i køretøjsenhedens tidsmålingsfunktion og tidsangivelsen fra GNSS-modtageren. Denne hændelse registreres sammen med værdien i køretøjsenhedens interne ur og ledsages af en automatisk tidsjustering. Hvis hændelsen »tidskonflikt« er blevet udløst, vil køretøjsenheden ikke generere andre tidskonflikthændelser inden for de næste 12 timer. Denne hændelse skal ikke udløses, hvis GNSS-modtageren ikke har kunnet registrere et gyldigt GNSS-signal inden for de sidste 30 dage. Den automatiske tidsjustering skal dog genoptages, når positionsoplysningerne fra GNSS-modtageren er tilgængelige igen.

3.9.16 *Fejlen »kort«*

87) Denne fejl skal udløses, når der optræder fejl ved et takografkort under driften.

3.9.17 *Fejlen »kontrolapparat«*

88) Denne fejl skal udløses, når et af nedenstående svigt forekommer, uden at apparatet er i kalibreringstilstand:

— Intern fejl i køretøjsenhed

— Printerfejl

— Displayfejl

— Dataoverførselsfejl

— Følerfejl

— Fejl ved GNSS-modtager eller eksternt GNSS-udstyr

— Fejl ved faciliteten til fjernkommunikation

▼B

3.10 **Indbyggede tester og selvtester**

89) Kontrolapparatet skal selvdetektere fejl gennem selvtester og indbyggede tester i overensstemmelse med følgende tabel:

Den testede underenhed	Selvtest	Indbygget test
Programmel		Integritet
Datalager	Adgang	Adgang, dataintegritet
Kortlæseenheder	Adgang	Adgang
Tastatur		Manuelt eftersyn
Printer	(op til fabrikanten)	Udskrift
Skærm		Visuel kontrol
Dataoverførsel (udføres kun under dataoverførsel)	Korrekt funktion	
Føler	Korrekt funktion	Korrekt funktion
Faciliteten til fjernkommunikation	Korrekt funktion	Korrekt funktion
GNSS-udstyr	Korrekt funktion	Korrekt funktion

3.11 **Læsning fra datalager**

90) Kontrolapparatet skal kunne læse alle data, som er gemt i dets lager.

3.12 **Registrering og lagring i datalageret**

Med henblik på bestemmelserne i dette afsnit

— defineres »365 dage« som 365 kalenderdage med en aktivitet i køretøjet svarende til gennemsnitsførerens. Den gennemsnitlige aktivitet pr. dag i et køretøj defineres som mindst seks førere eller medchauffører, seks cyklusser med isætning/udtagning af kort samt 256 aktivitetsskift. »365 dage« omfatter således mindst 2 190 (med)chauffører, 2 190 cyklusser med kortisætning og -udtagning samt 93 440 aktivitetsskift.

— defineres det gennemsnitlige antal positioner pr. dag som mindst seks positioner, hvor den daglige arbejdsperiode starter, seks positioner, hvor førerens sammenhængende køretid når op på et multiplum af tre timer, og seks positioner, hvor den daglige arbejdsperiode slutter, så »365 dage« omfatter mindst 6 570 positioner

— registreres klokkeslæt med en opløsning på 1 minut, medmindre andet er angivet

— registreres kilometerstand med en opløsning på 1 kilometer

— registreres hastigheder med en opløsning på 1 km/t

— registreres positioner (breddegrad og længdegrad) i grader og minutter med en opløsning på 1/10 minut og den tilhørende GNSS-nøjagtighed og -indlæsningstid.

▼B

91) Data gemt i datalageret må under typegodkendelsesomstændigheder ikke kunne påvirkes af en afbrydelse i den eksterne strømforsyning af under tolv måneders varighed. Derudover må data gemt i den eksterne facilitet til fjernkommunikation som defineret i tillæg 14 ikke kunne påvirkes af en afbrydelse i strømforsyningen af under 28 dages varighed.

92) Kontrolapparatet skal implicit eller eksplicit kunne registrere følgende data og gemme dem i datalageret:

3.12.1 *Identifikationsdata for apparat*

3.12.1.1 Identifikationsdata for køretøjsenhed

93) Kontrolapparatet skal i sit datalager kunne lagre følgende identifikationsdata for køretøjsenheden:

— fabrikantens navn

— fabrikantens adresse

— reservedelsnummer

— serienummer

— køretøjsenhedens generation

— mulighed for at bruge takografkort af første generation

— programmellets versionsnummer

— installationsdato for den pågældende version af programmellet

— apparatets produktionsår

— godkendelsesnummer.

94) Køretøjsenhedens identifikationsnummer registreres og lagres én gang for alle af køretøjsenhedens fabrikant, bortset fra programmelrelaterede data og godkendelsesnummeret, som kan ændres ved eventuel opgradering af programmellet og mulighed for brug af takografkort af første generation.

3.12.1.2 Identifikationsdata for bevægelsessensor

95) Bevægelsessensoren skal kunne gemme følgende identifikationsdata i sit lager:

— fabrikantens navn

— serienummer

— godkendelsesnummer.

— navn på indlejret sikkerhedskomponent (f.eks. reservedelsnummer på intern chip/processor)

— betegnelse på operativsystem (f.eks. programmellets versionsnummer).

96) Identifikationsdata på bevægelsessensoren registreres og lagres én gang for alle i bevægelsessensoren af dennes fabrikant.

97) Køretøjsenheden skal kunne registrere og i sit datalager gemme følgende data vedrørende de 20 seneste parringer af bevægelsessensordata (hvis der er flere parringer inden for én kalenderdag, gemmes kun den første og den sidste parring på den pågældende dag):

▼B

Følgende data skal registreres for hver af disse parringer:

— identifikationsdata for bevægelsessensor

— serienummer

— godkendelsesnummer

— parringsdata for bevægelsessensor:

— dato for parring.

3.12.1.3 Identifikationsdata for globale satellitnavigationssystemer (GNSS)

98) Det eksterne GNSS-udstyr skal kunne gemme følgende identifikationsdata i sit lager:

— fabrikantens navn

— serienummer

— godkendelsesnummer.

— navn på indlejret sikkerhedskomponent (f.eks. reservedelsnummer på intern chip/processor)

— betegnelse på operativsystem (f.eks. programmellets versionsnummer).

99) Identifikationsdataene registreres og lagres én gang for alle i det eksterne GNSS-udstyr af dettes fabrikant.

100) Køretøjsenheden skal kunne registrere og i sit datalager gemme følgende data vedrørende de 20 seneste sammenkoblinger fra eksternt GNSS-udstyr (hvis der er flere sammenkoblinger inden for én kalenderdag, gemmes kun den første og den sidste sammenkobling på den pågældende dag)

Følgende data skal registreres for hver af disse sammenkoblinger:

— identifikationsdata for det eksterne GNSS-udstyr:

— serienummer

— godkendelsesnummer

— sammenkoblingsdata om eksternt GNSS-udstyr:

— dato for sammenkobling.

3.12.2 *Nøgler og certifikater*

101) Kontrolapparatet skal kunne gemme en række kryptografiske nøgler og certifikater som præciseret i tillæg 11, del A og B.

3.12.3 *Data vedrørende isætning og udtagning af førerkort eller værkstedskort*

102) For hver cyklus med isætning og udtagning af fører- eller værkstedskort i apparatet skal kontrolapparatet registrere og i datalageret gemme:

— kortindehaverens efternavn og fornavn(e), således som de er lagret på kortet

— kortnummer, udstedende medlemsstat og udløbsdato som lagret på kortet

— kortgeneration

▼B

— isætningsdato og -klokkeslæt

— køretøjets kilometerstand ved isætning af kortet

— den kortplads, som kortet sidder i

— dato og klokkeslæt for udtagning af kortet

— køretøjets kilometerstand ved udtagning af kortet

— følgende oplysninger om det foregående køretøj, føreren har anvendt, som lagret på kortet:

— køretøjets indregistreringsnummer og den indregistrerende medlemsstat

— køretøjsenhedens generation (hvis den foreligger)

— dato og klokkeslæt for udtagning af kortet

— et flag, som angiver, om kortindehaver ved isætning af kortet har indlæst aktiviteter manuelt eller ikke.

103) Datalageret skal kunne opbevare disse data i mindst 365 dage.

104) Når lagerpladsen er opbrugt, skal nye data erstatte de ældste data.

3.12.4 *Føreraktivitetsdata*

105) Følgende data skal af kontrolapparatet registreres og gemmes i datalageret ved enhver aktivitetsændring for fører og/eller medchauffør og/eller ethvert skift i kørestatus og/eller enhver isætning eller udtagning af et fører- eller værkstedskort:

— kørestatus (FØRERHOLD, ÉN FØRER)

— kortplads (FØRER, MEDCHAUFFØR)

— kortstatus for den pågældende kortplads (ISAT, IKKE ISAT)

— aktivitet (KØRSEL, RÅDIGHED, ARBEJDE, PAUSE/HVILE)

— dato og klokkeslæt for ændringen.

ISAT betyder, at et gyldigt fører- eller værkstedskort er sat i kortpladsen. IKKE ISAT betyder det modsatte, dvs. der sidder ikke et gyldigt fører- eller værkstedskort i kortpladsen (f.eks. er der isat et virksomhedskort, eller intet kort er isat).

Aktivitetsdata, som indlæses manuelt af føreren, bliver ikke registreret i datalageret.

106) Datalageret skal kunne opbevare føreraktivitetsdata i mindst 365 dage.

107) Når lagerpladsen er opbrugt, skal nye data erstatte de ældste data.

▼B

3.12.5 *Steder og positioner, hvor daglige arbejdsperioder starter og slutter og/eller hvor tre timers sammenhængende køretid nås*

108) Kontrolapparatet skal registrere og i sit datalager gemme:

— steder og positioner, hvor føreren og/eller medchaufføren påbegynder sin daglige arbejdsperiode

— positioner, hvor førerens sammenhængende køretid når op på et multiplum af tre timer

— steder og positioner, hvor føreren og/eller medchaufføren afslutter sin daglige arbejdsperiode.

109) Hvis køretøjets position ikke oplyses af GNSS-modtageren på disse tidspunkter, skal kontrolapparatet bruge den seneste tilgængelige position og den tilhørende dato og tid.

110) Sammen med hvert sted eller hver position skal kontrolapparatet registrere og i sit datalager gemme:

— kortnummer for fører (medchauffør) samt kortudstedende medlemsstat

— kortgeneration

— indlæsningsdato og -klokkeslæt

— indlæsningens art (begyndelse, slutning eller tre timers sammenhængende køretid)

— den tilhørende GNSS-nøjagtighed, dato og tid, hvis relevant

— køretøjets kilometerstand.

111) Datalageret skal kunne rumme steder og positioner, hvor daglige arbejdsperioder starter og slutter, og/eller hvor tre timers sammenhængende køretid nås, i mindst 365 dage.

112) Når lagerpladsen er opbrugt, skal nye data erstatte de ældste data.

3.12.6 *Kilometertællerdata*

113) Kontrolapparatet skal i sit datalager registrere køretøjets kilometerstand og den tilsvarende dato ved midnat hver kalenderdag.

114) Datalageret skal i mindst 365 kalenderdage kunne opbevare værdierne af kilometerstanden ved midnat.

115) Når lagerpladsen er opbrugt, skal nye data erstatte de ældste data.

3.12.7 *Detaljerede hastighedsdata*

116) Kontrolapparatet skal registrere og i sit datalager gemme køretøjets øjeblikkelige hastighed med tilhørende dato og klokkeslæt i hvert sekund i mindst de seneste 24 timer, køretøjet er blevet kørt.

3.12.8 *Data vedrørende hændelser*

Med henblik på bestemmelserne i dette afsnit skal tiden registreres med en opløsning på 1 sekund.

117) For hver hændelse, som detekteres, skal kontrolapparatet registrere følgende data og gemme dem i datalageret i overensstemmelse med følgende lagringsbestemmelser:

▼B

Hændelse	Lagringsbestemmelse	Data, som skal lagres for hver hændelse
Isætning af ugyldigt kort	— de 10 seneste hændelser	— dato og klokkeslæt for hændelsen — korttype, kortnummer, udstedende medlemsstat og generation af det kort, som er årsag til hændelsen — antal tilsvarende hændelser den pågældende dag
Kortkonflikt	— de 10 seneste hændelser	— hændelsens startdato og -klokkeslæt — hændelsens slutdato og -klokkeslæt — korttype, kortnummer, udstedende medlemsstat og generation af de to kort, som er årsag til konflikten.
Kørsel uden behørigt kort	— den længstvarige hændelse for hver af de 10 seneste dage, den er forekommet — de 5 længstvarende hændelser inden for de sidste 365 dage	— hændelsens startdato og -klokkeslæt — hændelsens slutdato og -klokkeslæt — korttype, kortnummer, udstedende medlemsstat og generation af kort, der er isat ved starten og/eller slutningen af hændelsen — antal tilsvarende hændelser den pågældende dag
Isætning af kort under kørslen	— den seneste hændelse for hver af de 10 seneste dage, den er forekommet	— dato og klokkeslæt for hændelsen — korttype, kortnummer, udstedende medlemsstat og generation — antal tilsvarende hændelser den pågældende dag
Seneste kortsession ikke korrekt afsluttet	— de 10 seneste hændelser	— dato og klokkeslæt for isætning af kortet — korttype, kortnummer, udstedende medlemsstat og generation — de seneste sessionsdata, aflæst fra kortet: — dato og klokkeslæt for isætning af kortet — VRN og den medlemsstat, der har indregistreret det, samt køretøjsenhedens generation.
Overskridelse af tilladt hastighed (1)	— den alvorligste hændelse for hver af de seneste 10 dage, hvor den er forekommet (dvs. den, hvor gennemsnitshastigheden har været størst) — de 5 alvorligste hændelser inden for de sidste 365 dage — den første hændelse, som har fundet sted efter sidste kalibrering	— hændelsens startdato og -klokkeslæt — hændelsens slutdato og -klokkeslæt — den højeste hastighed målt under hændelsen — den aritmetiske gennemsnitshastighed målt under hændelsen — korttype, kortnummer, udstedende medlemsstat og generation af førerkortet (hvis relevant) — antal tilsvarende hændelser den pågældende dag

▼B

Hændelse	Lagringsbestemmelse	Data, som skal lagres for hver hændelse
Strømforsyningssvigt (2)	— den længstvarende hændelse for hver af de 10 seneste dage, den er forekommet — de 5 længstvarende hændelser inden for de sidste 365 dage	— hændelsens startdato og -klokkeslæt — hændelsens slutdato og -klokkeslæt — korttype, kortnummer, udstedende medlemsstat og generation af kort, der er isat ved starten og/eller slutningen af hændelsen — antal tilsvarende hændelser den pågældende dag
Fejl ved kommunikation med faciliteten til fjernkommunikation	— den længstvarende hændelse for hver af de 10 seneste dage, den er forekommet — de 5 længstvarende hændelser inden for de sidste 365 dage	— hændelsens startdato og -klokkeslæt — hændelsens slutdato og -klokkeslæt — korttype, kortnummer, udstedende medlemsstat og generation af kort, der er isat ved starten og/eller slutningen af hændelsen — antal tilsvarende hændelser den pågældende dag
Manglende positionsoplysninger fra GNSS-modtager	— den længstvarende hændelse for hver af de 10 seneste dage, den er forekommet — de 5 længstvarende hændelser inden for de sidste 365 dage	— hændelsens startdato og -klokkeslæt — hændelsens slutdato og -klokkeslæt — korttype, kortnummer, udstedende medlemsstat og generation af kort, der er isat ved starten og/eller slutningen af hændelsen — antal tilsvarende hændelser den pågældende dag
Fejl ved køredata	— den længstvarende hændelse for hver af de 10 seneste dage, den er forekommet — de 5 længstvarende hændelser inden for de sidste 365 dage	— hændelsens startdato og -klokkeslæt — hændelsens slutdato og -klokkeslæt — korttype, kortnummer, udstedende medlemsstat og generation af kort, der er isat ved starten og/eller slutningen af hændelsen — antal tilsvarende hændelser den pågældende dag
Køretøjsbevægelseskonflikt	— den længstvarende hændelse for hver af de 10 seneste dage, den er forekommet — de 5 længstvarende hændelser inden for de sidste 365 dage	— hændelsens startdato og -klokkeslæt — hændelsens slutdato og -klokkeslæt — korttype, kortnummer, udstedende medlemsstat og generation af kort, der er isat ved starten og/eller slutningen af hændelsen — antal tilsvarende hændelser den pågældende dag
Forsøg på sikkerhedsbrud	— de 10 seneste hændelser for hver type hændelse	— hændelsens startdato og -klokkeslæt — hændelsens slutdato og -klokkeslæt (hvis relevant) — korttype, kortnummer, udstedende medlemsstat og generation af kort, der er isat ved starten og/eller slutningen af hændelsen — hændelsens type

▼B

Hændelse	Lagringsbestemmelse	Data, som skal lagres for hver hændelse
Tidskonflikt	— den længstvarende hændelse for hver af de 10 seneste dage, den er forekommet — de 5 længstvarende hændelser inden for de sidste 365 dage	— kontrolapparat, dato og klokkeslæt — GNSS, dato og klokkeslæt — korttype, kortnummer, udstedende medlemsstat og generation af kort, der er isat ved starten og/eller slutningen af hændelsen — antal tilsvarende hændelser den pågældende dag

(1) Kontrolapparatet skal desuden registrere og i sit datalager gemme:

— dato og klokkeslæt for seneste KONTROL FOR OVERSKRIDELSE AF TILLADT HASTIGHED

— dato og klokkeslæt for første overskridelse af tilladt hastighed siden denne KONTROL FOR OVERSKRIDELSE AF TILLADT HASTIGHED

— antal hændelser med overskridelse af tilladt hastighed siden seneste KONTROL FOR OVERSKRIDELSE AF TILLADT HASTIGHED.

(2) Disse data kan kun registreres ved genetablering af strømforsyningen. Klokkeslæt kan kendes med en nøjagtighed på 1 minut.

3.12.9 *Data vedrørende fejl*

Med henblik på bestemmelserne i dette afsnit skal tiden registreres med en opløsning på 1 sekund.

118) For hver funden fejl skal kontrolapparatet registrere følgende data og gemme dem i datalageret i overensstemmelse med følgende lagringsbestemmelser:

Fejl	Lagringsbestemmelse	Data, som skal gemmes for hver hændelse
Kortfejl	— de 10 seneste kortfejl for førerkortet	— startdato og -klokkeslæt for fejlen — slutdato og -klokkeslæt for fejlen — korttype, kortnummer, udstedende medlemsstat og generation
Fejl ved kontrolapparatet	— de 10 seneste fejl af hver type fejl — den første fejl efter seneste kalibrering	— startdato og -klokkeslæt for fejlen — slutdato og -klokkeslæt for fejlen — fejltype — korttype, kortnummer og udstedende medlemsstat samt generation af kort, der er isat ved starten og/eller slutningen af fejlen.

3.12.10 *Kalibreringsdata*

119) Kontrolapparatet skal registrere og i sit datalager gemme data vedrørende:

— kalibreringsparametre, som er kendte på aktiveringstidspunktet

▼B

— dets allerførste kalibrering efter aktivering

— dets første kalibrering i det nuværende køretøj (identificeret ved sit VIN)

— de 20 seneste kalibreringer (hvis der udføres flere kalibreringer samme kalenderdag, skal kun den første og sidste heraf gemmes).

120) Følgende data skal registreres for hver af disse kalibreringer:

— kalibreringens formål (aktivering, første montering, montering, periodisk eftersyn)

— værkstedets navn og adresse

— værkstedskortets nummer, den kortudstedende medlemsstat og kortets udløbsdato

— køretøjsidentifikation

— parametre, som er ført ajour eller bekræftet: w, k, l, dækstørrelse, hastighedsbegrænserens indstilling, kilometerstand (gammel og ny værdi), dato og klokkeslæt (gammel og ny værdi)

— type og id for alle monterede plomber.

121) Derudover skal kontrolapparatet registrere og i sit datalager gemme dets evne til at bruge takografkort af første generation (stadig aktiverede eller ej).

122) Bevægelsessensoren skal registrere og i sit datalager gemme følgende data vedrørende bevægelsessensorens montering:

— første parring med en køretøjsenhed (dato, klokkeslæt, køretøjsenhedens godkendelsesnummer og køretøjsenhedens serienummer)

— sidste parring med en køretøjsenhed (dato, klokkeslæt, køretøjsenhedens godkendelsesnummer og køretøjsenhedens serienummer).

123) Det eksterne GNSS-udstyr skal registrere og i sit datalager gemme følgende monteringsdata vedrørende udstyret:

— første sammenkobling med en køretøjsenhed (dato, klokkeslæt, køretøjsenhedens godkendelsesnummer og køretøjsenhedens serienummer)

— sidste sammenkobling med en køretøjsenhed (dato, klokkeslæt, køretøjsenhedens godkendelsesnummer og køretøjsenhedens serienummer).

3.12.11 *Tidsjusteringsdata*

124) Kontrolapparatet skal registrere og i sit datalager gemme data af relevans for tidsjusteringer foretaget i kalibreringstilstand, men ikke i forbindelse med regelmæssig kalibrering (def. f)):

— seneste justering af tidspunktet

— de fem største tidsjusteringer

125) Følgende data skal registreres for hver af disse tidsjusteringer:

— dato og klokkeslæt, gammel værdi

— dato og klokkeslæt, ny værdi

— værkstedets navn og adresse

— værkstedskortets nummer, den kortudstedende medlemsstat, kortgenerationen og kortets udløbsdato.

▼B

3.12.12 *Kontrolaktivitetsdata*

126) Kontrolapparatet skal registrere og i datalageret gemme følgende data vedrørende de 20 seneste kontrolaktiviteter:

— kontroldato og -klokkeslæt

— kontrolkortets nummer, den kortudstedende medlemsstat og kortgenerationen

— kontrollens art (visning på skærm og/eller udskrivning og/eller dataoverførsel på køretøjsenhed og/eller dataoverførsel på kort og/eller kalibreringskontrol ved vejsiden).

127) Ved dataoverførsel skal datoen for de ældste og de seneste overførte dage ligeledes registreres.

3.12.13 *Data vedrørende virksomhedslåse*

128) Kontrolapparatet skal registrere og i datalageret gemme data vedrørende de 255 seneste virksomhedslåse:

— dato og klokkeslæt for lås-ind

— dato og klokkeslæt for lås-ud

— virksomhedskortets nummer, den kortudstedende medlemsstat og kortgenerationen

— virksomhedens navn og adresse.

Data, som tidligere er låst med en lås, der ikke længere findes i datalageret på grund af ovennævnte grænse, behandles som ikke-låst.

3.12.14 *Data vedrørende dataoverførselsaktivitet*

129) Kontrolapparatet skal registrere og i sit datalager gemme følgende data vedrørende den seneste dataoverførsel fra datalageret til eksterne medier, som fandt sted i virksomhedstilstand eller i kalibreringtilstand:

— dato og klokkeslæt for dataoverførslen

— virksomhedskortets eller værkstedskortets nummer, den kortudstedende medlemsstat og kortgenerationen

— virksomhedens eller værkstedets navn.

3.12.15 *Data vedrørende særlige omstændigheder*

130) Kontrolapparatet skal registrere og i datalageret gemme følgende data vedrørende særlige omstændigheder:

— indlæsningsdato og -klokkeslæt

— den særlige omstændigheds art.

131) Datalageret skal være i stand til at opbevare data vedrørende særlige omstændigheder i mindst 365 dage (idet det forudsættes, at der i gennemsnit åbnes og lukkes en omstændighed dagligt). Når lagerpladsen er opbrugt, skal nye data erstatte de ældste data.

3.12.16 *Data vedrørende takografkort*

132) Kontrolapparatet skal kunne lagre følgende data vedrørende de forskellige takografkort, som er blevet anvendt i køretøjsenheden:

— takografens kortnummer og serienummer

— fabrikanten af takografkortet

▼B

— takografkortets type

— takografkortets version.

133) Kontrolapparatet skal kunne lagre mindst 88 sådanne poster.

3.13 **Læsning fra takografkort**

134) Kontrolapparatet skal i givet fald kunne læse de data fra takografkort af første og anden generation, som er nødvendige

— til fastlæggelse af korttype, kortindehaver, tidligere anvendt køretøj, dato og klokkeslæt for seneste udtagning af kort og den på det tidspunkt valgte aktivitet

— til kontrol af, at seneste kortsession blev afsluttet korrekt

— til beregning af førerens sammenhængende køretid, akkumulerede pausetid og akkumulerede køretider for den foregående og den aktuelle uge

— til at fremstille de nødvendige udskrifter vedrørende de data, som er registreret på et førerkort

— til at overføre data fra et førerkort til eksterne medier.

Dette krav gælder kun for takografkort af første generation, hvis brugen af dem ikke er blevet udelukket af et værksted.

135) Ved eventuel læsefejl skal kontrolapparatet højst tre gange forsøge at udføre samme læseordre, og derefter, hvis det stadig ikke er lykkedes, erklære kortet for defekt og ugyldigt.

3.14 **Registrering og lagring på takografkort**

3.14.1 *Registrering og lagring på takografkort af første generation*

136) Forudsat at brug af takografkort af første generation ikke er blevet udelukket af et værksted, skal kontrolapparatet registrere og lagre data på nøjagtig samme måde som et kontrolapparat af første generation ville gøre.

137) Kontrolapparatet skal sætte »kortsessionsdata« på fører- eller værkstedskort straks efter isætning af kortet.

138) Kontrolapparatet skal ajourføre de data, som er gemt på gyldige fører-, værksteds-, virksomheds- og/eller kontrolkort, med alle de nødvendige data vedrørende den periode, hvor kortet er isat, og vedrørende kortindehaveren. De data, som gemmes på disse kort, er angivet i afsnit 4.

139) Kontrolapparatet skal ajourføre de føreraktivitets- og steddata (som foreskrevet i 4.5.3.1.9 og 4.5.3.1.11), som er gemt på gyldige fører- og/eller værkstedskort, med de aktivitets- og steddata, som indlæses manuelt af kortindehaveren.

140) Hændelser, der ikke er defineret for kontrolapparater af første generation, skal ikke lagres på fører- og værkstedskortene.

▼B

141) Ajourføring af takografkort skal ske ved, at seneste data erstatter ældste data i det nødvendige omfang og under hensyntagen til kortets faktiske lagringskapacitet.

142) I tilfælde af læsefejl skal kontrolapparatet højst tre gange forsøge at udføre samme læseordre, og derefter, hvis det stadig ikke er lykkedes, erklære kortet for defekt og ugyldigt.

143) Før et førerkort frigives, og efter at alle relevante data er gemt på kortet, skal kontrolapparatet tilbagestille »kortsessionsdata«.

3.14.2 *Registrering og lagring på takografkort af anden generation*

144) Takografkort af anden generation skal omfatte to forskellige kortapplikationer, hvoraf den ene skal være nøjagtig den samme som TACHO-applikationen for takografkort af første generation, og den anden — »TACHO_G2« — skal være som fastsat i kapitel 4 og tillæg 2.

145) Kontrolapparatet skal sætte »kortsessionsdata« på fører- eller værkstedskort straks efter isætning af kortet.

146) Kontrolapparatet skal ajourføre de data, som er gemt på de to kortapplikationer for gyldige fører-, værksteds-, virksomheds- og/eller kontrolkort, med alle de nødvendige data vedrørende den periode, hvor kortet er isat, og vedrørende kortindehaveren. De data, som gemmes på disse kort, er angivet i afsnit 4.

147) Kontrolapparatet skal ajourføre de data om førerens aktivitetssteder og -positioner (som foreskrevet i 4.5.3.1.9, 4.5.3.1.11, 4.5.3.2.9 og 4.5.3.2.11), som er gemt på gyldige fører- og/eller værkstedskort, med de data om aktiviteter og steder, som indlæses manuelt af kortindehaveren.

148) Ajourføring af takografkort skal ske ved, at seneste data erstatter ældste data i det nødvendige omfang og under hensyntagen til kortets faktiske lagringskapacitet.

149) I tilfælde af læsefejl skal kontrolapparatet højst tre gange forsøge at udføre samme læseordre, og derefter, hvis det stadig ikke er lykkedes, erklære kortet for defekt og ugyldigt.

150) Før et førerkort frigives, og efter at alle relevante data er gemt på kortets to applikationer, skal kontrolapparatet tilbagestille »kortsessionsdata«.

3.15 **Visning på skærm**

151) Skærmen skal have mindst 20 tegn.

152) Der skal anvendes en mindste tegnstørrelse på 5 mm i højden og 3,5 mm i bredden.

153) Skærmen skal understøtte de tegnsæt, der er angivet i tillæg 1, kapitel 4 »Tegnsæt«. Skærmen kan anvende forenklede tegn (f.eks. kan tegn med accent vises uden accent, eller små bogstaver kan vises som store).

▼B

154) Skærmen skal være forsynet med tilstrækkelig ikkeblændende belysning.

155) Anvisningerne skal kunne ses udefra i forhold til kontrolapparatet.

156) Kontrolapparatet skal på skærmen kunne vise:

— automatisk valgte værdier

— data vedrørende advarselssignaler

— data vedrørende adgang via menu

— andre data, som en bruger ønsker.

Kontrolapparatet kan på skærmen vise supplerende oplysninger, forudsat at de tydeligt kan skelnes fra de ovenfor krævede oplysninger.

157) Kontrolapparatets skærm skal anvende de i tillæg 3 anførte piktogrammer eller piktogramkombinationer. Andre piktogrammer eller piktogramkombinationer kan anvendes af skærmen, hvis de tydeligt kan skelnes fra ovennævnte piktogrammer eller piktogramkombinationer.

158) Skærmen skal altid være tændt, når køretøjet er i bevægelse.

159) Kontrolapparatet kan have en manuel eller automatisk facilitet, som slukker for skærmen, når køretøjet ikke er i bevægelse.

Skærmformatet er foreskrevet i tillæg 5.

3.15.1 *Standardskærmbillede*

160) Når ingen andre oplysninger behøver vises på skærmen, skal denne automatisk vise følgende:

— lokaltid (som fremkommet af UTC-tid + forskydning som indstillet af fører)

— funktionstilstand

— aktuel føreraktivitet og aktuel medchaufføraktivitet

— oplysninger vedrørende fører:

— hvis den aktuelle aktivitet er KØRSEL, aktuel sammenhængende køretid og aktuel akkumuleret pausetid

— hvis den aktuelle aktivitet ikke er KØRSEL, aktuel varighed af denne aktivitet (siden den valgtes), og aktuel akkumuleret pausetid.

161) Data vedrørende de to chauffører skal på skærmen vises på en klar, enkel og utvetydig måde. Kan oplysningerne vedrørende fører og medchauffør ikke vises samtidig, skal kontrolapparatet automatisk vise oplysningerne vedrørende føreren og give brugeren mulighed for at se oplysningerne vedrørende medchaufføren.

162) Giver skærmens bredde ikke mulighed for automatisk visning af funktionstilstand, skal kontrolapparatet kortvarigt vise den nye funktionstilstand, når den ændres.

▼B

163) Ved isætning af kort skal kontrolapparatet kortvarigt vise korthaverens navn.

164) Når omstændigheden »UDEN FOR GYLDIGHEDSOMRÅDE« eller »FÆRGE/TOG« åbnes, skal skærmen automatisk ved hjælp af det pågældende piktogram vise, at netop denne omstændighed er åbnet. (Det kan godtages, at den aktuelle føreraktivitet ikke nødvendigvis vises samtidigt.)

3.15.2 *Visning af advarsel*

165) Kontrolapparatet skal på skærmen vise oplysninger om advarselssignaler, hvilket hovedsagelig sker ved hjælp af piktogrammerne i tillæg 3, om nødvendigt suppleret med en talkode. Advarslen kan desuden gives som tekst på det af føreren foretrukne sprog.

3.15.3 *Adgang via menu*

166) Kontrolapparatet skal stille de nødvendige kommandoer til rådighed gennem en hensigtsmæssig menustruktur.

3.15.4 *Andre skærmbilleder*

167) På kommando skal skærmen selektivt kunne vise:

— UTC-dato og -klokkeslæt og den lokale tidsforskydning

— indholdet af hver af de seks udskrifter, i samme format som udskriften selv

— førerens sammenhængende køretid og akkumulerede pausetid

— medchaufførens sammenhængende køretid og akkumulerede pausetid

— førerens akkumulerede køretid for den foregående og den aktuelle uge

— medchaufførens akkumulerede køretid for den foregående og den aktuelle uge

valgfrit:

— aktuel varighed af medchaufførens aktivitet (siden den valgtes)

— førerens akkumulerede køretid for den aktuelle uge

— medchaufførens akkumulerede køretid for den aktuelle daglige arbejdsperiode

— førerens akkumulerede køretid for den aktuelle daglige arbejdsperiode.

168) Visningen af udskriftens indhold skal være sekventiel, linje for linje. Er skærmen mindre end 24 tegn bred, skal brugeren have adgang til de fuldstændige oplysninger gennem en passende menu (flere linjer, rulning …).

Udskriftslinjer, som er afsat til håndskrevne oplysninger, kan udelades på skærmen.

▼B

3.16 **Udskrivning**

169) Kontrolapparatet skal kunne udskrive oplysninger fra sit datalager og/eller fra takografkort i henhold til nedenstående syv udskriftstyper:

— daglig udskrift af føreraktivitet fra kort

— daglig udskrift af føreraktivitet fra køretøjsenhed

— udskrift af hændelser og fejl fra kort

— udskrift af hændelser og fejl fra køretøjsenhed

— udskrift af tekniske data

— udskrift af overskridelse af tilladt hastighed

— takografkortdatahistorik for en given køretøjsenhed (se afsnit 3.12.16).

Det nærmere format og indhold af disse udskrifter er angivet i tillæg 4.

Yderligere data kan anføres sidst i udskrifterne.

Kontrolapparatet kan stille yderligere udskriftstyper til rådighed, hvis de tydeligt kan skelnes fra de syv ovennævnte udskriftstyper.

170) Der må ikke være adgang til »Daglig udskrift af føreraktiviteter fra kort« og »Udskrift af hændelser og fejl fra kort«, medmindre der er indsat et fører- eller værkstedskort i kontrolapparatet. Før udskrivningen påbegyndes, skal kontrolapparatet ajourføre data gemt på det pågældende kort.

171) For at hente »daglig udskrift af føreraktiviteter fra kort« eller »udskrift af hændelser og fejl fra kort« skal kontrolapparatet:

— enten automatisk vælge fører- eller værkstedskort, hvis kun det ene af disse kort er isat,

— eller stille en kommando til rådighed for valg af kildekort eller valg af kortet i førerkortpladsen, hvis der er isat to af disse kort i kontrolapparatet.

172) Printeren skal kunne udskrive 24 tegn pr. linje.

173) Der skal anvendes en mindste tegnstørrelse på 2,1 mm i højden og 1,5 mm i bredden.

174) Printeren skal understøtte de tegnsæt, der er angivet i tillæg 1, kapitel 4 »Tegnsæt«.

175) Printeren skal være således udformet, at disse udskrifter er så tydelige, at der ikke er fare for fejllæsning.

176) De skal bevare deres format og deres registreringer under normale luftfugtigheds- (10-90 %) og temperaturforhold.

177) Det typegodkendte papir, som anvendes i kontrolapparatet, skal være forsynet med det pågældende typegodkendelsesmærke og angivelse af de(n) type(r) kontrolapparat(er), det kan anvendes i.

▼B

178) Udskrifterne skal forblive letlæselige og identificerbare under normale opbevaringsforhold med hensyn til lysstyrke, fugtighed og temperatur i mindst to år.

179) Udskrifter skal som minimum overholde testspecifikationerne i tillæg 9.

180) Disse dokumenter skal kunne påføres håndskrevne påtegninger, f.eks. førerens underskrift.

181) Kontrolapparatet skal kunne håndtere »papir opbrugt«-hændelser under udskrivningen ved, efter isætning af nyt papir, at begynde forfra på udskrivningen eller fortsætte udskrivningen med en klar henvisning til den allerede udskrevne del.

3.17 **Advarsler**

182) Kontrolapparatet skal advare føreren, når det konstaterer en hændelse og/eller fejl.

183) Det kan tillades, at advarsel om afbrydelse af strømforsyningen først finder sted, efter at strømforsyningen er genoprettet.

184) Kontrolapparatet skal advare føreren, når den højeste tilladte sammenhængende køretid overskrides, samt 15 minutter inden dette sker.

185) Advarselssignaler skal være synlige. Akustiske advarselssignaler kan anvendes som supplement til synlige advarselssignaler.

186) Synlige advarselssignaler skal være let genkendelige for brugeren, skal være placeret i førerens synsfelt og skal være letlæselige både ved dag og ved nat.

187) Synlige advarselssignaler kan være indbygget i kontrolapparatet og/eller være placeret fjernt fra kontrolapparatet.

188) I sidstnævnte tilfælde skal de være forsynet med symbolet »T«.

189) Advarselssignaler skal have en varighed på mindst 30 sekunder, medmindre brugeren kvitterer ved at trykke på en eller flere bestemte knapper i kontrolapparatet. Denne første kvittering må ikke slette det i næste afsnit omhandlede skærmbillede: Årsag til advarselssignal.

190) Kontrolapparatets skærm skal vise årsagen til advarselssignalet og vedblive hermed, indtil brugeren kvitterer med en særlig kode eller kommando på kontrolapparatet.

191) Der kan afgives supplerende advarselssignaler, forudsat de ikke af føreren kan forveksles med de tidligere definerede.

3.18 **Dataoverførsel til eksterne medier**

192) Kontrolapparatet skal på kommando kunne overføre data fra sit lager eller fra et førerkort til eksterne lagermedier gennem kalibrerings- og dataoverførselsstikket. Før udskrivningen påbegyndes, skal kontrolapparatet ajourføre data gemt på det pågældende kort.

▼B

193) Som en ikke obligatorisk facilitet kan kontrolapparatet desuden i enhver funktionstilstand overføre data til en virksomhed, hvis identitet er bekræftet gennem denne kanal, på andre måder. I så fald skal der for denne dataoverførsel gælde samme adgangsret til data som i virksomhedstilstand.

194) Overførslen må ikke ændre eller slette lagrede data.

195) Den elektriske grænseflade for kalibrering/dataoverførsel er specificeret i tillæg 6.

196) Dataoverførselsprotokoller er specificeret i tillæg 7.

3.19 **Fjernkommunikation i forbindelse med målrettede vejsidekontroller**

197) Når køretøjet er sat i tænding, skal køretøjsenheden hvert 60. sekund i faciliteten til fjernkommunikation lagre de seneste data, der er nødvendige for at foretage målrettede vejsidekontroller. Disse data skal krypteres og signeres som foreskrevet i tillæg 11 og 14.

198) De data, der skal fjernkontrolleres, skal være tilgængelige for fjernkommunikationslæsere via trådløs kommunikation som beskrevet i tillæg 14.

199) De data, der er nødvendige for at foretage målrettede vejsidekontroller, skal vedrøre:

— det seneste forsøg på sikkerhedsbrud

— den længste afbrydelse af strømforsyning

— sensorfejl

— fejl ved køredata

— køretøjsbevægelseskonflikt

— kørsel uden gyldigt kort

— isætning af kort under kørslen

— tidsjusteringsdata

— kalibreringsdata, herunder datoerne for de to senest lagrede kalibreringsposter

— køretøjets indregistreringsnummer

— hastighed registreret af takografen.

3.20 **Udlæsning af data til supplerende eksterne enheder**

200) Kontrolapparatet kan også udrustes med standardiserede grænseflader, som muliggør brug af de data, der registreres eller frembringes af takografer, i en ekstern facilitet i drifts- eller kalibreringstilstand.

I tillæg 13 præsenteres en standardiseret valgfri ITS-grænseflade. Der kan samtidig anvendes andre lignende grænseflader, forudsat at de fuldt ud overholder minimumskravene i tillæg 13 med hensyn til data, sikkerhed og førerens samtykke.

Følgende krav gælder for ITS-data, der tilvejebringes via den pågældende grænseflade:

— Der er tale om udvalgte eksisterende data fra takografens dataordliste (tillæg 1).

▼B

— En delmængde af disse udvalgte data er markeret som »personoplysninger«.

— »Personoplysningerne« er kun tilgængelige, hvis der indhentes verificerbart samtykke fra føreren om, at vedkommendes personoplysninger må hentes ud af netværket.

— Dette samtykke kan til enhver tid gives eller trækkes tilbage ved hjælp af kommandoer i menuen, forudsat at førerkortet er isat.

— Både de samlede data og delmængder heraf udsendes via trådløs protokol (Bluetooth) inden for førerhusets radius med en opdateringsfrekvens på 1 minut.

— Parringen af den eksterne enhed med ITS-grænsefladen vil være beskyttet af en særlig tilfældig pinkode på mindst 4 cifre, der registreres i hver enkelt køretøjsenhed og er tilgængelig via dennes skærm.

— Under ingen omstændigheder må ITS-grænsefladens tilstedeværelse forstyrre eller påvirke køretøjsenhedens funktionstilstand og sikkerhed.

Ud over de udvalgte eksisterende data, der betragtes som et minimum, kan andre data også udlæses, forudsat at de ikke kan betragtes som personoplysninger.

Kontrolapparatet skal underrette andre eksterne faciliteter om førerens samtykke.

Når køretøjet er sat i tænding, skal disse data udsendes permanent.

201) Den grænseflade til den serielle dataforbindelse, der er anført i bilag 1B til forordning (EØF) nr. 3821/85 (med ændringer), kan fortsat anvendes i takografer for at sikre bagudkompatibilitet. Førerens samtykke skal indhentes, hvis personoplysninger overføres.

3.21 **Kalibrering**

202) Kalibreringsfunktionen skal give mulighed for:

— at samparre bevægelsessensoren automatisk med køretøjsenheden

— at sammenkoble det eksterne GNSS-udstyr automatisk med køretøjsenheden om nødvendigt

— at tilpasse kontrolapparatets konstant (k) digitalt til køretøjets vejdrejetal (w)

— at justere det aktuelle tidspunkt inden for gyldighedsperioden for det isatte værkstedskort

— at justere den aktuelle kilometerstand

— at opdatere datalagerets identifikationsdata for bevægelsessensoren

— om nødvendigt at opdatere identifikationsdata for eksternt GNSS-udstyr, der er gemt i datalageret

▼B

— at opdatere type og id for alle monterede plomber

— at ajourføre eller bekræfte andre parametre, som kontrolapparatet har kendskab til: køretøjsidentifikation, w, l, dækstørrelse og, hvis relevant, fartbegrænserens indstilling.

203) Endvidere skal kalibreringsfunktionen gøre det muligt at udelukke brug af takografkort af første generation i kontrolapparatet, forudsat at betingelserne i tillæg 15 er opfyldt.

204) Samparring af bevægelsessensor med køretøjsenhed skal i det mindste omfatte følgende:

— ajourføring af bevægelsessensorens monteringsdata, som opbevares af bevægelsessensoren (efter behov)

— kopiering af de nødvendige data til identifikation af bevægelsessensoren fra føleren til køretøjsenhedens datalager.

205) Sammenkobling af det eksterne GNSS-udstyr til køretøjsenheden skal som minimum bestå af:

— opdatering af det eksterne GNSS-udstyrs monteringsdata, som opbevares af udstyret (efter behov)

— kopiering af de nødvendige identifikationsdata for det eksterne GNSS-udstyr, herunder udstyrets serienummer, fra udstyret til køretøjsenhedens datalager.

Efter sammenkoblingen skal GNSS-udstyrets positionsoplysninger kontrolleres.

206) Kalibreringsfunktionen skal kunne indlæse data gennem kalibrerings-/overførselsstikket i henhold til den i tillæg 8 fastlagte kalibreringsprotokol. Kalibreringsfunktionen kan derudover indlæse de nødvendige data ved brug af andre midler.

3.22 **Kalibreringskontrol ved vejsiden**

207) Funktionen til kalibreringskontrol ved vejsiden skal gøre det muligt at aflæse serienummeret på den bevægelsessensor (muligvis indlejret i adapteren) og (om nødvendigt) det eksterne GNSS-udstyr, der er forbundet til køretøjsenheden på tidspunktet for anmodningen.

208) Denne aflæsning skal som minimum kunne foretages på køretøjsenhedens skærmbillede via kommandoer i menuerne.

209) Funktionen til kalibreringskontrol ved vejsiden skal desuden gøre det muligt at styre valget af I/O-funktionstilstand for kalibrerings-I/O-signallinjen, som anført i tillæg 6, via K-linjegrænsefladen. Dette skal ske gennem funktionen ECUAdjustmentSession som beskrevet i tillæg 8, afsnit 7 »Styring af testimpulser — funktionsenhed for ind-/uddatastyring«.

3.23 **Tidsjustering**

210) Tidsjusteringsfunktionen skal give mulighed for automatisk justering af det aktuelle klokkeslæt. I kontrolapparatet anvendes to kilder til tidsjustering, nemlig 1) køretøjsenhedens interne ur og 2) GNSS-modtageren.

▼B

211) Køretøjsenhedens interne urs tidsindstilling skal automatisk tilpasses med intervaller på højst 12 timer. Hvis der ikke foreligger noget GNSS-signal inden for de 12 timer, skal tidsindstillingen foretages, så snart køretøjsenheden kan få adgang til en gyldig tidsværdi fra GNSS-modtageren, afhængigt af køretøjets tændingstilstand. Referencetidspunktet for den automatiske indstilling af køretøjsenhedens interne ur skal hentes fra GNSS-modtageren. Hændelsen »tidskonflikt« skal udløses, hvis det aktuelle klokkeslæt afviger med mere end ét (1) minut fra tidsoplysningerne fra GNSS-modtageren.

212) Tidsjusteringsfunktionen skal også muliggøre hændelsesudløst justering af det aktuelle klokkeslæt i kalibreringstilstand.

3.24 **Funktionsspecifikationer**

213) Køretøjsenheden skal være helt driftsklar i temperaturområdet – 20 °C til 70 °C. For det eksterne GNSS-udstyr er temperaturområdet – 20 °C til 70 °C, og for bevægelsessensoren er temperaturområdet – 40 °C til 135 °C. Datalagerets indhold skal kunne opbevares ved temperaturer ned til – 40 °C.

214) Takografen skal være fuldt funktionsdygtig i fugtighedsintervallet 10 % til 90 %.

215) Plomberne i den intelligente takograf skal kunne tåle de samme forhold som de takografkomponenter, de er fastgjort til.

216) Kontrolapparatet skal være beskyttet mod overspænding, omvendt polaritet af strømtilførslen samt kortslutning.

217) Bevægelsessensorer skal

— reagere på et magnetisk felt, som forstyrrer detekteringen af køretøjets bevægelse. I dette tilfælde vil køretøjsenheden registrere og gemme en fejl ved føler (krav 88)

— eller have et følerelement, som er beskyttet mod eller upåvirkelig af magnetiske felter.

218) Kontrolapparatet og det eksterne GNSS-udstyr skal overholde bestemmelserne i det internationale regelsæt UN ECE R10 og være beskyttet mod elektrostatiske udladninger og spændingsvariationer.

3.25 **Materialer**

219) Alle kontrolapparatets komponenter skal være udført i materialer af tilstrækkelig stabilitet og mekanisk styrke samt med stabile elektriske og magnetiske egenskaber.

220) Med henblik på normale driftsbetingelser skal alle apparatets indvendige dele være beskyttet mod fugt og støv.

221) Køretøjsenheden og det eksterne GNSS-udstyr skal opfylde beskyttelsesgrad IP 40, og bevægelsessensoren skal opfylde beskyttelsesgrad IP 64 i henhold til standard IEC 60529:1989, herunder A1:1999 og A2:2013.

222) Kontrolapparatet skal opfylde de pågældende tekniske forskrifter for ergonomisk udformning.

▼B

223) Kontrolapparatet skal være beskyttet mod hændelig beskadigelse.

3.26 **Mærkning**

224) Hvis kontrolapparatet viser køretøjets kilometerstand og hastighed på skærmen, skal følgende angivelser vises på skærmen:

— ved det tal, som viser kilometerstanden, måleenheden angivet ved forkortelsen »km«

— ved det tal, som angiver hastigheden, måleenheden »km/t«.

Kontrolapparatet kan desuden være stillet om til at vise hastighed i miles per hour, i hvilket tilfælde hastighedsmåleenheden skal være angivet ved forkortelsen »mph«. Kontrolapparatet kan desuden være stillet om til at vise afstand i miles, i hvilket tilfælde afstandsmåleenheden skal være angivet ved forkortelsen »mi«.

225) På hver af kontrolapparatets separate komponenter skal være fastgjort en tavle med følgende enkeltheder:

— udstyrsfabrikantens navn og adresse

— fabrikantens reservedelsnummer og apparatets fremstillingsår

— apparatets serienummer

— kontrolapparattypens godkendelsesmærke.

226) Når der ikke er tilstrækkelig plads til at angive alle ovenstående oplysninger, skal skiltet i det mindste angive fabrikantens navn eller mærke, og apparatets reservedelsnummer.

4 KONSTRUKTIONS- OG FUNKTIONSKRAV TIL TAKOGRAFKORT

4.1 **Synlige data**

Forsiden skal indeholde:

227) svarende til kortets art, ordet »Førerkort« eller »Kontrolkort« eller »Værkstedskort« eller »Virksomhedskort«, trykt med store bogstaver på de(t) officielle sprog i den medlemsstat, som har udstedt kortet

228) angivelse af navnet på den udstedende medlemsstat er valgfrit

229) den udstedende medlemsstats nationalitetsmærke, trykt med negativ skrift i et blåt rektangel og omgivet af 12 gule stjerner. Nationalitetsmærkerne er følgende:

B	Belgien	LV	Letland
BG	Bulgarien	L	Luxembourg
CZ	Den Tjekkiske Republik	LT	Litauen
CY	Cypern	M	Malta
DK	Danmark	NL	Nederlandene
D	Tyskland	A	Østrig
EST	Estland	PL	Polen

▼B

GR	Grækenland	P RO SK SLO	Portugal Rumænien Slovakiet Slovenien
E	Spanien	FIN	Finland
F HR H	Frankrig Kroatien Ungarn	S	Sverige
IRL	Irland	UK	Det Forenede Kongerige
I	Italien		

230) oplysninger, der er specifikke for det udstedte kort, nummereret som følger:

	Førerkort	Kontrolkort	Virksomheds- eller værkstedskort
1.	førerens efternavn	kontrolinstansens navn	virksomhedens eller værkstedets navn
2.	førerens fornavn(e)	den tilsynsførendes efternavn (hvis relevant)	kortindehaverens efternavn (hvis relevant)
3.	førerens fødselsdato	den tilsynsførendes fornavn(e) (hvis relevant)	kortindehaverens fornavn(e) (hvis relevant)
4.a	første dato i kortets gyldighedsperiode		
4.b	kortets udløbsdato		
4.c	den udstedende myndigheds navn (kan trykkes på bagsiden)		
4.d	(evt.) nummer, der er forskelligt fra nummeret under punkt 5, til administrative formål		
5.a	kørekortnummer (på udstedelsesdatoen for førerkortet)	—	—
5.b	kortnummer		
6.	fotografi af føreren	(evt.) fotografi af den tilsynsførende	(evt.) fotografi af installatøren
7.	(evt.) indehaverens underskrift		
8.	(evt.) førerens sædvanlige bopæl eller postadresse	kontrolinstansens postadresse	virksomhedens eller værkstedets postadresse

231) datoer skrives i formatet »dd/mm/yyyy« eller »dd.mm.yyyy« (dag, måned, år).

Bagsiden skal indeholde:

232) en forklaring til de nummererede punkter på kortets forside

▼B

233) med indehaverens udtrykkelige skriftlige godkendelse kan der tilføjes data, som ikke har forbindelse med administrationen af kortet; sådanne tilføjelser ændrer ikke på nogen måde modellens anvendelse som takografkort.

234) Takografkort skal være trykt med følgende dominerende baggrundsfarve:

— førerkort: hvid

— kontrolkort: blå

— værkstedskort: rød

— virksomhedskort: gul.

235) Takografkort skal have mindst følgende egenskaber til beskyttelse mod forfalskning og indgreb fra uvedkommende:

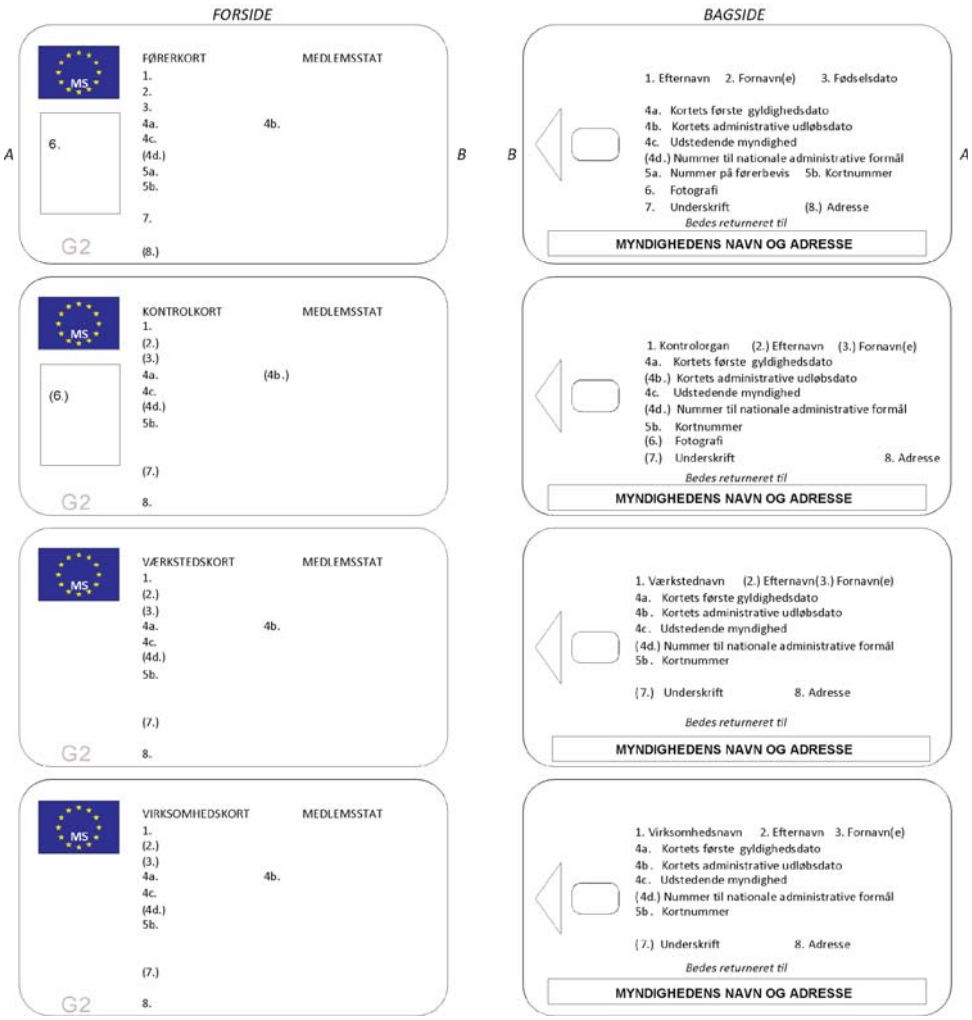
— sikkerhedsbaggrund med fint slangeornament og regnbuetryk

— i fotografiets område skal sikkerhedsbaggrund og fotografi overlappe

— mindst én tofarvet mikroprintlinje.

▼C3

TAKOGRAFKORT I HENHOLD TIL FÆLLESSKABSMODELLEN



▼B

236) Medlemsstaterne kan efter at have rådført sig med Kommissionen tilføje farve eller mærker som f.eks. nationale symboler og sikkerhedsdetaljer, uden at dette berører de øvrige bestemmelser i bilaget.

237) De midlertidige kort omhandlet i artikel 26, stk. 4, i forordning (EU) nr. 165/2014 skal overholde bestemmelserne i dette bilag.

4.2 **Sikkerhed**

Sikringen af systemet skal beskytte integritet og ægthed af data, som udveksles mellem kort og kontrolapparat, beskytte integritet og ægthed af data, som overføres fra kortene, bevirke, at visse skriveprocedurer på kortene er forbeholdt kontrolapparatet, dekryptere bestemte data, udelukke forfalskning af data, som opbevares på kortene, forhindre indgreb fra uvedkommende og afsløre ethvert forsøg derpå.

238) Af hensyn til systemets sikkerhed skal takografkortene opfylde sikkerhedsforskrifterne i tillæg 10 og 11.

239) Takografkort skal kunne læses med andet udstyr som f.eks. pc'er.

4.3 **Standarder**

240) Takografkort skal være i overensstemmelse med følgende standarder:

— ISO/IEC 7810 Identification cards — Physical characteristics

— ISO/IEC 7816 Identification cards — Integrated circuit cards:

— Part 1: Physical characteristics

— Part 2: Dimensions and position of the contacts (ISO/IEC 7816-2:2007)

— Part 3: Electrical interface and transmission protocols (ISO/IEC 7816-3:2006)

— Part 4: Organisation, security and commands for interchange (ISO/IEC 7816-4:2013 + Cor 1:2014)

— Part 6: Interindustry data elements for interchange (ISO/IEC 7816-6:2004 + Cor 1:2006)

— Part 8: Commands for security operations (ISO/IEC 7816-8:2004).

— Takografkort skal afprøves i overensstemmelse med ISO/IEC 10373-3:2010 Identification cards — Test methods — Part 3: Integrated circuit cards with contacts and related interface devices.

4.4 **Miljømæssige og elektriske specifikationer**

241) Takografkort skal kunne fungere korrekt under alle de klimabetingelser, som normalt optræder på fællesskabets område, og det mindste i temperaturområdet – 25 °C til + 70 °C med lejlighedsvise maksima på indtil + 85 °C, idet der ved »lejlighedsvis« forstås højst 4 timer ad gangen og højst 100 gange i løbet af kortets levetid.

242) Takografkort skal fungere korrekt inden for luftfugtighedsintervallet 10-90 %.

▼B

243) Takografkort skal kunne fungere korrekt i fem år, hvis de anvendes i overensstemmelse med de miljømæssige og elektriske specifikationer.

244) Under drift skal takografkort opfylde kravene i ECE R10 om elektromagnetisk kompatibilitet og skal være beskyttet mod elektrostatiske udladninger.

4.5 **Lagring af oplysninger**

Med henblik på bestemmelserne i dette afsnit

— registreres klokkeslæt med en opløsning på 1 minut, medmindre andet er angivet

— registreres kilometerstand med en opløsning på 1 kilometer

— hastigheder registreres med en opløsning på 1 km/t

— positioner (breddegrad og længdegrad) registreres i grader og minutter med en opløsning på 1/10 minut.

Takografkortets funktioner, kommandoer og logiske strukturer, som opfylder datalagringsbestemmelserne, er nærmere angivet i tillæg 2.

Medmindre andet anføres, skal datalagring på takografkort tilrettelægges på en sådan måde, at nye data erstatter de ældste data, hvis den planlagte lagerplads til de pågældende poster er opbrugt.

245) I dette afsnit fastsættes tilladelig mindste lagerkapacitet til applikationens forskellige datafiler. Takografkort skal til kontrolapparatet kunne angive den faktiske lagerkapacitet til disse datafiler.

246) Skal kortet herudover benyttes til lagring af andre data vedrørende andre applikationer, som kortet understøtter, skal disse lagres i overensstemmelse med direktiv 95/46/EF, direktiv 2002/58/EF og artikel 7 i forordning (EU) nr. 165/2014.

247) Hver hovedfil (MF) på ethvert takografkort skal indeholde op til fem elementærfiler (EF) til kortstyring, anvendelse og identifikation af chip samt to dedikerede filer (DF):

— DF Tachograph (dedikeret takograffil), som indeholder den applikation, der er tilgængelig for første generation af køretøjsenheder, og som også findes i takografkort af første generation

— DF Tachograph_G2, som indeholder den applikation, der kun er tilgængelig for anden generation af køretøjsenheder, og som kun findes i takografkort af anden generation.

Nærmere oplysninger om takografkortets opbygning findes i tillæg 2.

4.5.1 *Elementærfiler til identifikation og kortstyring*

4.5.2 *Identifikation af IC-kort*

248) Takografkort skal kunne lagre følgende data til identifikation af chipkort:

— »clock stop«

▼B

— kortets serienummer (herunder produktionshenvisninger)

— kortets typegodkendelsesnummer

— identifikation af kortnavn (ID)

— indlejrer-ID

— IC-navn.

4.5.2.1 Identifikation af chip

249) Takografkort skal kunne lagre følgende data til identifikation af IC (IC = integreret kreds):

— IC-serienummer

— IC-produktionshenvisninger.

4.5.2.2 DIR (findes kun i takografkort af anden generation)

250) Takografkort skal kunne lagre de i tillæg 2 anførte dataobjekter til identifikation af applikationen.

4.5.2.3 ATR-oplysninger (betingede, findes kun i takografkort af anden generation)

251) Takografkort skal kunne lagre følgende dataobjekt med udvidet informationslængde:

— det dataobjekt med udvidet informationslængde, der er anført i tillæg 2, hvis takografkortet understøtter felter med udvidet længde.

4.5.2.4 Oplysninger med udvidet længde (betingede, findes kun i takografkort af anden generation)

252) Takografkort skal kunne lagre følgende dataobjekter med udvidet informationslængde:

— de dataobjekter med udvidet informationslængde, der er anført i tillæg 2, hvis takografkortet understøtter felter med udvidet længde.

4.5.3 *Førerkort*

4.5.3.1 Takografapplikation (tilgængelig for køretøjsenheder af første og anden generation)

4.5.3.1.1 Identifikation af applikation

253) Førerkortet skal kunne lagre følgende data til identifikation af applikationen:

— identifikation af takografapplikation

— identifikation af takografkortets type.

4.5.3.1.2 Nøgler og certifikater

254) Førerkortet skal kunne gemme en række kryptografiske nøgler og certifikater som præciseret i tillæg 11, del A.

▼B

4.5.3.1.3 Identifikation af kort

255) Førerkortet skal kunne lagre følgende data til identifikation af kortet:

— kortnummer

— udstedende medlemsstat, navn på udstedende myndighed, udstedelsesdato

— startdato på kortets gyldighedsperiode, kortets udløbsdato.

4.5.3.1.4 Identifikation af kortindehaver

256) Førerkortet skal kunne lagre følgende data til identifikation af kortindehaver:

— indehaverens efternavn

— indehaverens fornavn(e)

— fødselsdato

— foretrukket sprog.

4.5.3.1.5 Dataoverførsel på kort

257) Førerkortet skal kunne lagre følgende data vedrørende dataoverførsel på kort:

— dato og klokkeslæt for seneste dataoverførsel på kort (til andre formål end kontrol).

258) Førerkortet skal kunne opbevare én sådan post.

4.5.3.1.6 Oplysninger om førerbevis

259) Førerkortet skal kunne lagre følgende data vedrørende førerbevis:

— udstedende medlemsstat, navn på udstedende myndighed

— førerbevisets nummer (på kortets udstedelsesdato).

4.5.3.1.7 Data vedrørende hændelser

Med henblik på bestemmelserne i dette afsnit skal tiden registreres med en opløsning på 1 sekund.

260) Førerkortet skal kunne lagre data vedrørende følgende hændelser, som kontrolapparatet har detekteret, mens kortet var isat:

— tidsoverlapning (når kortet er årsag til denne hændelse)

— isætning af kort under kørslen (når kortet er genstand for denne hændelse)

— seneste kortsession ikke korrekt afsluttet (når kortet er genstand for denne hændelse)

— afbrydelse i strømforsyningen

— fejl ved køredata

— forsøg på sikkerhedsbrud.

261) Førerkortet skal kunne lagre følgende data vedrørende disse hændelser:

— hændelseskode

— startdato og -klokkeslæt for hændelsen (eller for isætning af kortet, hvis dette fandt sted i hændelsesperioden)

▼B

— slutdato og -klokkeslæt for hændelsen (eller for udtagning af kortet, hvis dette fandt sted i hændelsesperioden)

— VRN og den medlemsstat, som har indregistreret det køretøj, hvor hændelsen optrådte.

Bemærk: For hændelsen »tidsoverlapning«

— skal hændelsens startdato og -klokkeslæt svare til dato og klokkeslæt for udtagning af kortet fra det foregående køretøj

— skal hændelsens slutdato og -klokkeslæt svare til dato og klokkeslæt for isætning af kortet i det aktuelle køretøj

— skal køretøjsdata svare til det aktuelle køretøj, som giver anledning til hændelsen.

Bemærk: For hændelsen »seneste kortsession ikke korrekt afsluttet«

— skal hændelsens startdato og -klokkeslæt svare til dato og klokkeslæt for ukorrekt afslutning af sessionen

— skal hændelsens slutdato og -klokkeslæt svare til dato og klokkeslæt for isætning af kortet ved den session, under hvilken hændelsen blev konstateret (den aktuelle session)

— skal køretøjsdata svare til det køretøj, i hvilket sessionen ikke blev afsluttet korrekt

262) skal førerkortet kunne lagre data for de seks senest optrådte hændelser af hver type (dvs. 36 hændelser).

4.5.3.1.8 Data vedrørende fejl

Med henblik på bestemmelserne i dette afsnit skal tiden registreres med en opløsning på 1 sekund.

263) Førerkortet skal kunne lagre data vedrørende følgende hændelser, som kontrolapparatet har detekteret, mens kortet var isat:

— kortfejl (når kortet er genstand for hændelsen)

— fejl ved kontrolapparat.

264) Førerkortet skal kunne lagre følgende data vedrørende disse hændelser:

— fejlkode

— startdato og -klokkeslæt for hændelsen (eller for isætning af kortet, hvis dette fandt sted inden for hændelsesperioden)

— slutdato og -klokkeslæt for fejlen (eller for udtagning af kortet, hvis dette fandt sted inden for hændelsesperioden)

— VRN og den medlemsstat, som har indregistreret det køretøj, hvor fejlen optrådte.

265) Førerkortet skal kunne lagre data for de tolv senest optrådte hændelser af hver type (dvs. 24 hændelser).

▼B

4.5.3.1.9 Føreraktivitetsdata

266) Førerkortet skal kunne lagre følgende data for hver kalenderdag, hvor kortet har været anvendt, eller hvor føreren har indtastet aktiviteter manuelt:

— dato

— en tæller for daglig tilstedeværelse (øges med én for hver af de pågældende kalenderdage)

— den samlede distance, som føreren har tilbagelagt det pågældende døgn

— førerstatus kl. 00:00

— samlet distance tilbagelagt af føreren den pågældende dag, hver gang føreren har skiftet aktivitet og/eller kørestatus og/eller har isat eller udtaget sit kort:

— kørestatus (FØRERHOLD, ÉN FØRER)

— kortplads (FØRER, MEDCHAUFFØR)

— kortstatus (ISAT, IKKE ISAT)

— aktivitet (KØRSEL, RÅDIGHED, ARBEJDE, PAUSE/HVILE)

— tidspunkt for ændringen.

267) Førerkortets lager skal kunne opbevare data vedrørende førerens aktivitet i mindst 28 dage (gennemsnitsaktiviteten for en fører defineres som 93 aktivitetsskift pr. dag).

268) De under forskrift 261, 264 og 266 angivne data skal opbevares på en måde, som giver mulighed for at hente aktiviteterne i den rækkefølge, de har fundet sted, også når der er tidsmæssig overlapning.

4.5.3.1.10 Data vedrørende anvendte køretøjer

269) Førerkortet skal kunne lagre følgende data for hver kalenderdag, kortet er blevet anvendt, og for hver anvendelsesperiode for et givet køretøj den pågældende dag (en sådan periode omfatter alle på hinanden følgende cyklusser med isætning/udtagning af kortet i køretøjet, som det »ses« af kortet):

— dato og klokkeslæt for første anvendelse af køretøjet (dvs. første kortisætning til denne anvendelsesperiode for køretøjet, eller 00:00, hvis det pågældende tidspunkt er inden for anvendelsesperioden)

— køretøjets kilometerstand på det pågældende tidspunkt

— dato og klokkeslæt for seneste anvendelse af køretøjet (dvs. første kortudtagning med henblik på denne anvendelsesperiode for køretøjet, eller 23:59, hvis det pågældende tidspunkt er inden for anvendelsesperioden)

▼B

— køretøjets kilometerstand på det pågældende tidspunkt

— VRN og den indregistrerende medlemsstat.

270) Førerkortet skal kunne lagre mindst 84 sådanne poster.

4.5.3.1.11 Steder, hvor den daglige arbejdstid begynder og/eller slutter

271) Førerkortet skal kunne opbevare følgende data vedrørende de steder, hvor den daglige arbejdstid begynder og/eller slutter, og som er indlæst af føreren:

— dato og klokkeslæt for indlæsningen (eller dato/klokkeslæt knyttet til indlæsningen, når indlæsning fandt sted under den manuelle indlæsningsprocedure)

— indlæsningens art (begyndelse eller slutning, omstændighed ved indlæsningen)

— den indlæste stat og region

— køretøjets kilometerstand.

272) Førerkortets lager skal kunne rumme mindst 42 par poster af denne art.

4.5.3.1.12 Kortsessionsdata

273) Førerkortet skal kunne opbevare følgende data vedrørende det køretøj, som åbnede kortets aktuelle session:

— dato og klokkeslæt for åbning af sessionen (dvs. isætning af kort) med en opløsning på ét sekund

— VRN og den indregistrerende medlemsstat.

4.5.3.1.13 Kontrolaktivitetsdata

274) Førerkortet skal kunne lagre følgende data vedrørende kontrolaktiviteter:

— kontroldato og -klokkeslæt

— kontrolkortets nummer og den kortudstedende medlemsstat

— kontrollens art (visning og/eller udskrivning og/eller dataoverførsel på køretøjsenhed og/eller dataoverførsel på kort (se bemærkning))

— ved dataoverførsel den overførte periode

— køretøjets indregistreringsnummer og den medlemsstat, som har indregistreret det køretøj, hvor kontrollen fandt sted.

Bemærk: dataoverførsel på kort vil kun blive registreret, hvis det sker gennem et kontrolapparat.

275) Førerkortet skal kunne opbevare én sådan post.

4.5.3.1.14 Data vedrørende særlige omstændigheder

276) Førerkortet skal kunne opbevare følgende data vedrørende særlige omstændigheder, som er indlæst, mens kortet var isat (uanset i hvilken kortplads):

— indlæsningsdato og -klokkeslæt

— den særlige omstændigheds art.

▼B

277) Førerkortet skal kunne lagre mindst 56 sådanne poster.

4.5.3.2 Takografapplikation af anden generation (ikke tilgængelig for køretøjsenheder af første generation)

4.5.3.2.1 Identifikation af applikation

278) Førerkortet skal kunne lagre følgende data til identifikation af applikationen:

— identifikation af takografapplikation

— identifikation af takografkortets type.

4.5.3.2.2 Nøgler og certifikater

279) Førerkortet skal kunne gemme en række kryptografiske nøgler og certifikater som præciseret i tillæg 11, del B.

4.5.3.2.3 Identifikation af kort

280) Førerkortet skal kunne lagre følgende data til identifikation af kortet:

— kortnummer

— udstedende medlemsstat, navn på udstedende myndighed, udstedelsesdato

— startdato på kortets gyldighedsperiode, kortets udløbsdato.

4.5.3.2.4 Identifikation af kortindehaver

281) Førerkortet skal kunne lagre følgende data til identifikation af kortindehaver:

— indehaverens efternavn

— indehaverens fornavn(e)

— fødselsdato

— foretrukket sprog.

4.5.3.2.5 Dataoverførsel på kort

282) Førerkortet skal kunne lagre følgende data vedrørende dataoverførsel på kort:

— dato og klokkeslæt for seneste dataoverførsel på kort (til andre formål end kontrol).

283) Førerkortet skal kunne opbevare én sådan post.

4.5.3.2.6 Oplysninger om førerbevis

284) Førerkortet skal kunne lagre følgende data vedrørende førerbevis:

— udstedende medlemsstat, navn på udstedende myndighed

— førerbevisets nummer (på kortets udstedelsesdato).

4.5.3.2.7 Data vedrørende hændelser

Med henblik på bestemmelserne i dette afsnit skal tiden registreres med en opløsning på 1 sekund.

▼B

285) Førerkortet skal kunne lagre data vedrørende følgende hændelser, som kontrolapparatet har detekteret, mens kortet var isat:

— tidsoverlapning (når kortet er årsag til denne hændelse)

— isætning af kort under kørslen (når kortet er genstand for denne hændelse)

— seneste kortsession ikke korrekt afsluttet (når kortet er genstand for denne hændelse)

— afbrydelse i strømforsyningen

— fejl ved kommunikation med faciliteten til fjernkommunikation

— manglende positionsoplysninger fra GNSS-modtager

— fejl ved kommunikation med det eksterne GNSS-udstyr

— fejl ved køredata

— køretøjsbevægelseskonflikt

— forsøg på sikkerhedsbrud

— tidskonflikt.

286) Førerkortet skal kunne lagre følgende data vedrørende disse hændelser:

— hændelseskode

— startdato og -klokkeslæt for hændelsen (eller for isætning af kortet, hvis dette fandt sted i hændelsesperioden)

— slutdato og -klokkeslæt for hændelsen (eller for udtagning af kortet, hvis dette fandt sted i hændelsesperioden)

— VRN og den medlemsstat, som har indregistreret det køretøj, hvor hændelsen optrådte.

Bemærk: For hændelsen »tidsoverlapning«

— skal hændelsens startdato og -klokkeslæt svare til dato og klokkeslæt for udtagning af kortet fra det foregående køretøj

— skal hændelsens slutdato og -klokkeslæt svare til dato og klokkeslæt for isætning af kortet i det aktuelle køretøj

— skal køretøjsdata svare til det aktuelle køretøj, som giver anledning til hændelsen.

Bemærk: For hændelsen »seneste kortsession ikke korrekt afsluttet«

— skal hændelsens startdato og -klokkeslæt svare til dato og klokkeslæt for ukorrekt afslutning af sessionen

— skal hændelsens slutdato og -klokkeslæt svare til dato og klokkeslæt for isætning af kortet ved den session, under hvilken hændelsen blev konstateret (den aktuelle session)

▼B

— skal køretøjsdata svare til det køretøj, i hvilket sessionen ikke blev afsluttet korrekt

287) skal førerkortet kunne lagre data for de seks senest optrådte hændelser af hver type (dvs. 66 hændelser).

4.5.3.2.8 Data vedrørende fejl

Med henblik på bestemmelserne i dette afsnit skal tiden registreres med en opløsning på 1 sekund.

288) Førerkortet skal kunne lagre data vedrørende følgende hændelser, som kontrolapparatet har detekteret, mens kortet var isat:

— kortfejl (når kortet er genstand for hændelsen)

— fejl ved kontrolapparat.

289) Førerkortet skal kunne lagre følgende data vedrørende disse hændelser:

— fejlkode

— startdato og -klokkeslæt for hændelsen (eller for isætning af kortet, hvis dette fandt sted inden for hændelsesperioden)

— slutdato og -klokkeslæt for fejlen (eller for udtagning af kortet, hvis dette fandt sted inden for hændelsesperioden)

— VRN og den medlemsstat, som har indregistreret det køretøj, hvor fejlen optrådte.

290) Førerkortet skal kunne lagre data for de tolv senest optrådte hændelser af hver type (dvs. 24 hændelser).

4.5.3.2.9 Føreraktivitetsdata

291) Førerkortet skal kunne lagre følgende data for hver kalenderdag, hvor kortet har været anvendt, eller hvor føreren har indtastet aktiviteter manuelt:

— dato

— en tæller for daglig tilstedeværelse (øges med én for hver af de pågældende kalenderdage)

— den samlede distance, som føreren har tilbagelagt det pågældende døgn

— førerstatus kl. 00:00

— samlet distance tilbagelagt af føreren den pågældende dag, hver gang føreren har skiftet aktivitet og/eller kørestatus og/eller har isat eller udtaget sit kort:

— kørestatus (FØRERHOLD, ÉN FØRER)

— kortplads (FØRER, MEDCHAUFFØR)

— kortstatus (ISAT, IKKE ISAT)

— aktivitet (KØRSEL, RÅDIGHED, ARBEJDE, PAUSE/HVILE)

▼B

— tidspunkt for ændringen.

292) Førerkortets lager skal kunne opbevare data vedrørende førerens aktivitet i mindst 28 dage (gennemsnitsaktiviteten for en fører defineres som 93 aktivitetsskift pr. dag).

293) De under forskrift 286, 289 og 291 angivne data skal opbevares på en måde, som giver mulighed for at hente aktiviteterne i den rækkefølge, de har fundet sted, også når der er tidsmæssig overlapning.

4.5.3.2.10 Data vedrørende anvendte køretøjer

294) Førerkortet skal kunne lagre følgende data for hver kalenderdag, kortet er blevet anvendt, og for hver anvendelsesperiode for et givet køretøj den pågældende dag (en sådan periode omfatter alle på hinanden følgende cyklusser med isætning/udtagning af kortet i køretøjet, som det »ses« af kortet):

— dato og klokkeslæt for første anvendelse af køretøjet (dvs. første kortisætning til denne anvendelsesperiode for køretøjet, eller 00:00, hvis det pågældende tidspunkt er inden for anvendelsesperioden)

— køretøjets kilometerstand på det pågældende tidspunkt

— dato og klokkeslæt for seneste anvendelse af køretøjet (dvs. første kortudtagning med henblik på denne anvendelsesperiode for køretøjet, eller 23:59, hvis det pågældende tidspunkt er inden for anvendelsesperioden)

— køretøjets kilometerstand på tidspunktet for seneste anvendelse

— VRN og den indregistrerende medlemsstat

— køretøjets VIN.

295) Førerkortet skal kunne lagre mindst 84 sådanne poster.

4.5.3.2.11 Steder og positioner, hvor den daglige arbejdstid begynder og/eller slutter

296) Førerkortet skal kunne opbevare følgende data vedrørende de steder, hvor den daglige arbejdstid begynder og/eller slutter, og som er indlæst af føreren:

— dato og klokkeslæt for indlæsningen (eller dato/klokkeslæt knyttet til indlæsningen, når indlæsning fandt sted under den manuelle indlæsningsprocedure)

— indlæsningens art (begyndelse eller slutning, omstændighed ved indlæsningen)

— den indlæste stat og region

— køretøjets kilometerstand

— køretøjets position

— GNSS-nøjagtigheden, dato og klokkeslæt for registrering af positionen.

297) Førerkortets lager skal kunne rumme mindst 84 par poster af denne art.

▼B

4.5.3.2.12 Kortsessionsdata

298) Førerkortet skal kunne opbevare følgende data vedrørende det køretøj, som åbnede kortets aktuelle session:

— dato og klokkeslæt for åbning af sessionen (dvs. isætning af kort) med en opløsning på ét sekund

— VRN og den indregistrerende medlemsstat.

4.5.3.2.13 Kontrolaktivitetsdata

299) Førerkortet skal kunne lagre følgende data vedrørende kontrolaktiviteter:

— kontroldato og -klokkeslæt

— kontrolkortets nummer og den kortudstedende medlemsstat

— kontrollens art (visning og/eller udskrivning og/eller dataoverførsel på køretøjsenhed og/eller dataoverførsel på kort (se bemærkning))

— ved dataoverførsel den overførte periode

— køretøjets indregistreringsnummer og den medlemsstat, som har indregistreret det køretøj, hvor kontrollen fandt sted.

Bemærk: Sikkerhedsforskrifterne indebærer, at dataoverførsel på kort kun vil blive registreret, hvis det sker gennem et kontrolapparat.

300) Førerkortet skal kunne opbevare én sådan post.

4.5.3.2.14 Data vedrørende særlige omstændigheder

301) Førerkortet skal kunne opbevare følgende data vedrørende særlige omstændigheder, som er indlæst, mens kortet var isat (uanset i hvilken kortplads):

— indlæsningsdato og -klokkeslæt

— den særlige omstændigheds art.

302) Førerkortet skal kunne lagre mindst 56 sådanne poster.

4.5.3.2.15 Data vedrørende anvendte køretøjsenheder

303) Førerkortet skal kunne lagre følgende data vedrørende de forskellige køretøjsenheder, som kortet er blevet brugt i:

— dato og klokkeslæt for starten af køretøjsenhedens anvendelsesperiode (dvs. første isætning af kortet i køretøjsenheden i den pågældende periode)

— fabrikanten af køretøjsenheden

— køretøjsenhedens type

— versionsnummeret på det programmel, der anvendes i køretøjsenheden.

304) Førerkortet skal kunne lagre mindst 84 sådanne poster.

▼B

4.5.3.2.16 Data vedrørende den position, hvor tre timers sammenhængende køretid nås

305) Førerkortet skal kunne opbevare følgende data vedrørende køretøjets position, hvor førerens sammenhængende køretid når op på et multiplum af tre timer:

— dato og klokkeslæt, hvor kortindehaverens sammenhængende køretid når op på et multiplum af tre timer

— køretøjets position

— GNSS-nøjagtigheden, dato og klokkeslæt for registrering af positionen.

306) Førerkortet skal kunne lagre mindst 252 sådanne poster.

4.5.4 *Værkstedskort*

4.5.4.1 Takografapplikation (tilgængelig for køretøjsenheder af første og anden generation)

4.5.4.1.1 Identifikation af applikation

307) Værkstedskortet skal kunne lagre følgende data til identifikation af applikationen:

— identifikation af takografapplikation

— identifikation af takografkortets type.

4.5.4.1.2 Nøgler og certifikater

308) Værkstedskortet skal kunne gemme en række kryptografiske nøgler og certifikater som præciseret i tillæg 11, del A.

309) Værkstedskortet skal kunne lagre et personligt identifikationsnummer (en PIN-kode).

4.5.4.1.3 Identifikation af kort

310) Værkstedskortet skal kunne lagre følgende data til kortidentifikation:

— kortnummer

— udstedende medlemsstat, navn på udstedende myndighed, udstedelsesdato

— startdato på kortets gyldighedsperiode, kortets udløbsdato.

4.5.4.1.4 Identifikation af kortindehaver

311) Værkstedskortet skal kunne lagre følgende data til identifikation af kortindehaver:

— værkstedets navn

— værkstedets adresse

— indehaverens efternavn

— indehaverens fornavn(e)

— foretrukket sprog.

4.5.4.1.5 Dataoverførsel på kort

312) Værkstedskortet skal kunne lagre data om dataoverførsel på kort på samme måde som et førerkort.

▼B

4.5.4.1.6 Kalibrerings- og tidsjusteringsdata

313) Værkstedskortet skal kunne opbevare poster vedrørende de kalibreringer og/eller tidsjusteringer, som er udført, mens kortet er indsat i et kontrolapparat.

314) Hver kalibreringspost skal kunne indeholde følgende data:

— kalibreringens formål (aktivering, første montering, montering, periodisk eftersyn)

— identifikation af køretøjer

— parametre, som er opdateret eller bekræftet (w, k, l, dækstørrelse, indstilling af hastighedsbegrænser, kilometertæller (ny og gammel værdi), dato og klokkeslæt (ny og gammel værdi))

— identifikation af kontrolapparatet (køretøjsenhedens reservedelsnummer, køretøjsenhedens serienummer).

315) Værkstedskortet skal kunne lagre mindst 88 sådanne poster.

316) Værkstedskortet skal have en tæller, som angiver det samlede antal kalibreringer, der er udført med kortet.

317) Værkstedskortet skal have en tæller, som angiver det samlede antal kalibreringer, der er udført siden sidste dataoverførsel på kortet.

4.5.4.1.7 Data vedrørende hændelser og fejl

318) Værkstedskortet skal kunne lagre dataposter om hændelser og fejl på samme måde som et førerkort.

319) Værkstedskortet skal kunne lagre data for de tre senest optrådte hændelser af hver type (dvs. 18 hændelser) og de tre senest optrådte fejl af hver type (dvs. 12 fejl).

4.5.4.1.8 Føreraktivitetsdata

320) Værkstedskortet skal kunne lagre data om førerens aktivitet på samme måde som et førerkort.

321) Værkstedskortet skal kunne lagre data om førerens aktivitet i mindst 1 dag med gennemsnitlig føreraktivitet.

4.5.4.1.9 Data vedrørende anvendte køretøjer

322) Værkstedskortet skal kunne lagre dataposter om anvendte køretøjer på samme måde som et førerkort.

323) Værkstedskortet skal kunne lagre mindst 4 sådanne poster.

4.5.4.1.10 Data vedrørende steder, hvor den daglige arbejdstid begynder og/eller slutter

324) Værkstedskortet skal kunne lagre dataposter om den daglige arbejdstids begyndelse og/eller slutning på samme måde som et førerkort.

325) Værkstedskortet skal kunne lagre mindst 3 par poster af denne art.

▼B

4.5.4.1.11 Kortsessionsdata

326) Værkstedskortet skal kunne lagre data om kortsessioner på samme måde som et førerkort.

4.5.4.1.12 Kontrolaktivitetsdata

327) Værkstedskortet skal kunne lagre data om kontrolaktivitet på samme måde som et førerkort.

4.5.4.1.13 Data vedrørende særlige omstændigheder

328) Værkstedskortet skal kunne lagre data vedrørende særlige omstændigheder på samme måde som et førerkort.

329) Værkstedskortet skal kunne lagre mindst 2 sådanne poster.

4.5.4.2 Takografapplikation af anden generation (ikke tilgængelig for køretøjsenheder af første generation)

4.5.4.2.1 Identifikation af applikation

330) Værkstedskortet skal kunne lagre følgende data til identifikation af applikationen:

— identifikation af takografapplikation

— identifikation af takografkortets type.

4.5.4.2.2 Nøgler og certifikater

331) Værkstedskortet skal kunne gemme en række kryptografiske nøgler og certifikater som præciseret i tillæg 11, del B.

332) Værkstedskortet skal kunne lagre et personligt identifikationsnummer (en PIN-kode).

4.5.4.2.3 Identifikation af kort

333) Værkstedskortet skal kunne lagre følgende data til kortidentifikation:

— kortnummer

— udstedende medlemsstat, navn på udstedende myndighed, udstedelsesdato

— startdato på kortets gyldighedsperiode, kortets udløbsdato.

4.5.4.2.4 Identifikation af kortindehaver

334) Værkstedskortet skal kunne lagre følgende data til identifikation af kortindehaver:

— værkstedets navn

— værkstedets adresse

— indehaverens efternavn

— indehaverens fornavn(e)

— foretrukket sprog.

4.5.4.2.5 Dataoverførsel på kort

335) Værkstedskortet skal kunne lagre data om dataoverførsel på kort på samme måde som et førerkort.

▼B

4.5.4.2.6 Kalibrerings- og tidsjusteringsdata

336) Værkstedskortet skal kunne opbevare poster vedrørende de kalibreringer og/eller tidsjusteringer, som er udført, mens kortet er indsat i et kontrolapparat.

337) Hver kalibreringspost skal kunne indeholde følgende data:

— kalibreringens formål (aktivering, første montering, montering, periodisk eftersyn)

— køretøjsidentifikation

— Parametre, som er opdateret eller bekræftet (w, k, l, dækstørrelse, indstilling af hastighedsbegrænser, kilometertæller (ny og gammel værdi), dato og klokkeslæt (ny og gammel værdi))

— identifikation af kontrolapparatet (køretøjsenhedens reservedelsnummer, køretøjsenhedens serienummer, bevægelsessensorens serienummer, serienummeret på faciliteten til fjernkommunikation og det eksterne GNSS-udstyrs serienummer, hvis relevant)

— type og id for alle monterede plomber

— køretøjsenhedens mulighed for at bruge takografkort af første generation (uanset om det er aktiveret).

338) Værkstedskortet skal kunne lagre mindst 88 sådanne poster.

339) Værkstedskortet skal have en tæller, som angiver det samlede antal kalibreringer, der er udført med kortet.

340) Værkstedskortet skal have en tæller, som angiver det samlede antal kalibreringer, der er udført siden sidste dataoverførsel på kortet.

4.5.4.2.7 Data vedrørende hændelser og fejl

341) Værkstedskortet skal kunne lagre dataposter om hændelser og fejl på samme måde som et førerkort.

342) Værkstedskortet skal kunne lagre data for de tre senest optrådte hændelser af hver type (dvs. 33 hændelser) og de tre senest optrådte fejl af hver type (dvs. 12 fejl).

4.5.4.2.8 Føreraktivitetsdata

343) Værkstedskortet skal kunne lagre data om førerens aktivitet på samme måde som et førerkort.

344) Værkstedskortet skal kunne lagre data om førerens aktivitet i mindst 1 dag med gennemsnitlig føreraktivitet.

4.5.4.2.9 Data vedrørende anvendte køretøjer

345) Værkstedskortet skal kunne lagre dataposter om anvendte køretøjer på samme måde som et førerkort.

346) Værkstedskortet skal kunne lagre mindst 4 sådanne poster.

▼B

4.5.4.2.10 Data vedrørende steder, hvor den daglige arbejdstid begynder og/eller slutter

347) Værkstedskortet skal kunne lagre dataposter om den daglige arbejdstids begyndelse og/eller slutning på samme måde som et førerkort.

348) Værkstedskortet skal kunne lagre mindst 3 par poster af denne art.

4.5.4.2.11 Kortsessionsdata

349) Værkstedskortet skal kunne lagre data om kortsessioner på samme måde som et førerkort.

4.5.4.2.12 Kontrolaktivitetsdata

350) Værkstedskortet skal kunne lagre data om kontrolaktivitet på samme måde som et førerkort.

4.5.4.2.13 Data vedrørende anvendte køretøjsenheder

351) Værkstedskortet skal kunne lagre følgende data vedrørende de forskellige køretøjsenheder, som kortet er blevet brugt i:

— dato og klokkeslæt for starten af køretøjsenhedens anvendelsesperiode (dvs. første isætning af kortet i køretøjsenheden i den pågældende periode)

— fabrikanten af køretøjsenheden

— køretøjsenhedens type

— versionsnummeret på det programmel, der anvendes i køretøjsenheden.

352) Værkstedskortet skal kunne lagre mindst 4 sådanne poster.

4.5.4.2.14 Data vedrørende den position, hvor tre timers sammenhængende køretid nås

353) Værkstedskortet skal kunne opbevare følgende data vedrørende køretøjets position, hvor førerens sammenhængende køretid når op på et multiplum af tre timer:

— dato og klokkeslæt, hvor kortindehaverens sammenhængende køretid når op på et multiplum af tre timer

— køretøjets position

— GNSS-nøjagtigheden, dato og klokkeslæt for registrering af positionen.

354) Værkstedskortet skal kunne lagre mindst 18 sådanne poster.

4.5.4.2.15 Data vedrørende særlige omstændigheder

355) Værkstedskortet skal kunne lagre data vedrørende særlige omstændigheder på samme måde som et førerkort.

356) Værkstedskortet skal kunne lagre mindst 2 sådanne poster.

▼B

4.5.5 *Kontrolkort*

4.5.5.1 Takografapplikation (tilgængelig for køretøjsenheder af første og anden generation)

4.5.5.1.1 Identifikation af applikation

357) Kontrolkortet skal kunne lagre følgende data til identifikation af applikationen:

— identifikation af takografapplikation

— identifikation af takografkortets type.

4.5.5.1.2 Nøgler og certifikater

358) Kontrolkortet skal kunne gemme en række kryptografiske nøgler og certifikater som præciseret i tillæg 11, del A.

4.5.5.1.3 Identifikation af kort

359) Kontrolkortet skal kunne lagre følgende data til kortidentifikation:

— kortnummer

— udstedende medlemsstat, navn på udstedende myndighed, udstedelsesdato

— startdato på kortets gyldighedsperiode, kortets eventuelle udløbsdato.

4.5.5.1.4 Identifikation af kortindehaver

360) Kontrolkortet skal kunne lagre følgende data til identifikation af kortindehaveren:

— kontrolinstansens navn

— kontrolinstansens adresse

— indehaverens efternavn

— indehaverens fornavn(e)

— foretrukket sprog.

4.5.5.1.5 Kontrolaktivitetsdata

361) Kontrolkortet skal kunne lagre følgende data vedrørende kontrolaktivitet:

— kontroldato og -klokkeslæt

— kontrollens art (visning på skærm og/eller udskrivning og/eller dataoverførsel på køretøjsenhed og/eller dataoverførsel på kort og/eller kalibreringskontrol ved vejsiden)

— eventuel periode, som er overført

— køretøjets indregistreringsnummer og den indregistrerende myndighed i det kontrollerede køretøj

— kontrolkortets nummer og den medlemsstat, som har udstedt det kontrollerede førerkort.

362) Kontrolkortet skal kunne lagre mindst 230 sådanne poster.

▼B

4.5.5.2 Takografapplikation af anden generation (ikke tilgængelig for køretøjsenheder af første generation)

4.5.5.2.1 Identifikation af applikation

363) Kontrolkortet skal kunne lagre følgende data til identifikation af applikationen:

— identifikation af takografapplikation

— identifikation af takografkortets type.

4.5.5.2.2 Nøgler og certifikater

364) Kontrolkortet skal kunne gemme en række kryptografiske nøgler og certifikater som præciseret i tillæg 11, del B.

4.5.5.2.3 Identifikation af kort

365) Kontrolkortet skal kunne lagre følgende data til kortidentifikation:

— kortnummer

— udstedende medlemsstat, navn på udstedende myndighed, udstedelsesdato

— startdato på kortets gyldighedsperiode, kortets eventuelle udløbsdato.

4.5.5.2.4 Identifikation af kortindehaver

366) Kontrolkortet skal kunne lagre følgende data til identifikation af kortindehaveren:

— kontrolinstansens navn

— kontrolinstansens adresse

— indehaverens efternavn

— indehaverens fornavn(e)

— foretrukket sprog.

4.5.5.2.5 Kontrolaktivitetsdata

367) Kontrolkortet skal kunne lagre følgende data vedrørende kontrolaktivitet:

— kontroldato og -klokkeslæt

— kontrollens art (visning på skærm og/eller udskrivning og/eller dataoverførsel på køretøjsenhed og/eller dataoverførsel på kort og/eller kalibreringskontrol ved vejsiden)

— eventuel periode, som er overført

— køretøjets indregistreringsnummer og den indregistrerende myndighed i det kontrollerede køretøj

— kontrolkortets nummer og den medlemsstat, som har udstedt det kontrollerede førerkort.

368) Kontrolkortet skal kunne lagre mindst 230 sådanne poster.

▼B

4.5.6 *Virksomhedskort*

4.5.6.1 Takografapplikation (tilgængelig for køretøjsenheder af første og anden generation)

4.5.6.1.1 Identifikation af applikation

369) Virksomhedskortet skal kunne lagre følgende data til identifikation af applikationen:

— identifikation af takografapplikation

— identifikation af takografkortets type.

4.5.6.1.2 Nøgler og certifikater

370) Virksomhedskortet skal kunne gemme en række kryptografiske nøgler og certifikater som præciseret i tillæg 11, del A.

4.5.6.1.3 Identifikation af kort

371) Virksomhedskortet skal kunne lagre følgende data til kortidentifikation:

— kortnummer

— udstedende medlemsstat, navn på udstedende myndighed, udstedelsesdato

— startdato på kortets gyldighedsperiode, kortets eventuelle udløbsdato.

4.5.6.1.4 Identifikation af kortindehaver

372) Virksomhedskortet skal kunne lagre følgende data til identifikation af kortindehaveren:

— virksomhedens navn

— virksomhedens adresse.

4.5.6.1.5 Virksomhedsaktivitetsdata

373) Virksomhedskortet skal kunne lagre følgende virksomhedsaktivitetsdata:

— dato og klokkeslæt for aktiviteten

— aktivitetens art (låse ind/ud på køretøjsenhed og/eller dataoverførsel på køretøjsenhed og/eller dataoverførsel på kort)

— eventuel periode, som er overført

— køretøjets indregistreringsnummer og den myndighed, som har registreret det

— kortets nummer og den kortudstedende medlemsstat (ved dataoverførsel på kort).

374) Virksomhedskortet skal kunne opbevare mindst 230 sådanne poster.

▼B

4.5.6.2 Takografapplikation af anden generation (ikke tilgængelig for køretøjsenheder af første generation)

4.5.6.2.1 Identifikation af applikation

375) Virksomhedskortet skal kunne lagre følgende data til identifikation af applikationen:

— identifikation af takografapplikation

— identifikation af takografkortets type.

4.5.6.2.2 Nøgler og certifikater

376) Virksomhedskortet skal kunne gemme en række kryptografiske nøgler og certifikater som præciseret i tillæg 11, del B.

4.5.6.2.3 Identifikation af kort

377) Virksomhedskortet skal kunne lagre følgende data til kortidentifikation:

— kortnummer

— udstedende medlemsstat, navn på udstedende myndighed, udstedelsesdato

— startdato på kortets gyldighedsperiode, kortets eventuelle udløbsdato.

4.5.6.2.4 Identifikation af kortindehaver

378) Virksomhedskortet skal kunne lagre følgende data til identifikation af kortindehaveren:

— virksomhedens navn

— virksomhedens adresse.

4.5.6.2.5 Virksomhedsaktivitetsdata

379) Virksomhedskortet skal kunne lagre følgende virksomhedsaktivitetsdata:

— dato og klokkeslæt for aktiviteten

— aktivitetens art (låse ind/ud på køretøjsenhed og/eller dataoverførsel på køretøjsenhed og/eller dataoverførsel på kort)

— eventuel periode, som er overført

— køretøjets indregistreringsnummer og den myndighed, som har registreret det

— kortets nummer og den kortudstedende medlemsstat (ved dataoverførsel på kort).

380) Virksomhedskortet skal kunne opbevare mindst 230 sådanne poster.

5 MONTERING AF KONTROLAPPARATET

5.1 **Montering**

381) Nye kontrolapparater skal leveres i ikke-aktiveret stand til installatører eller køretøjsfabrikanter, med alle de i afsnit 3.21 opregnede kalibreringsparametre sat til hensigtsmæssige og gyldige standardværdier. Når ingen særlig værdi er passende, sættes strengparametre til værdien »?« og talparametre til »0«. Levering af sikkerhedsrelevante dele til kontrolapparatet kan om nødvendigt begrænses under sikkerhedscertificeringen.

▼B

382) Inden kontrolapparatet er aktiveret, skal kontrolapparatet give adgang til kalibreringsfunktionen, også når det ikke er i kalibreringstilstand.

383) Før kontrolapparatet er aktiveret, må det hverken registrere eller lagre de i punkt 3.12.3, 3.12.9 og 3.12.12 to 3.12.15 inkl. omhandlede data.

384) Under monteringen skal køretøjets fabrikant forudindstille alle parametre, som kendes.

385) Køretøjsfabrikant eller -installatør skal senest aktivere det monterede kontrolapparat, før køretøjet anvendes inden for anvendelsesområdet for forordning (EF) nr. 561/2006.

386) Kontrolapparatet skal automatisk aktiveres ved første isætning af et gyldigt værkstedskort i en af dets kortlæsere.

387) Eventuelle nødvendige særlige samparringsprocedurer mellem bevægelsessensor og køretøjsenhed skal udføres automatisk før eller under aktivering.

388) Ligeledes skal eventuelle særlige sammenkoblingsprocedurer mellem eksternt GNSS-udstyr og køretøjsenhed udføres automatisk før eller under aktivering.

389) Når kontrolapparatet er blevet aktiveret, skal det fuldt ud håndhæve funktioner og adgangsret til data.

390) Efter aktivering af kontrolapparatet skal dette sende de sikrede data, der er nødvendige for at foretage målrettede vejsidekontroller, til faciliteten til fjernkommunikation.

391) Kontrolapparatets registrerings- og lagringsfunktioner skal være fuldt funktionsdygtige efter første aktivering af apparatet.

392) Monteringen skal efterfølges af en kalibrering. Det er ikke nødvendigt, at den første kalibrering omfatter indlæsning af køretøjets indregistreringsnummer, hvis det godkendte værksted, som skal foretage kalibreringen, ikke kender det. I så fald skal ejeren af køretøjet have mulighed for at indlæse indregistreringsnummeret ved hjælp af virksomhedskortet, før køretøjet anvendes inden for anvendelsesområdet for forordning (EF) nr. 561/2006 (f.eks. ved at anvende kommandoer ved hjælp af en passende menustruktur i køretøjsenhedens menneske-maskine-grænseflade), og kun på det tidspunkt ([1]). Det må kun være muligt at opdatere eller bekræfte denne indlæsning ved hjælp af et værkstedskort.

393) Ved montering af eksternt GNSS-udstyr skal dette kobles sammen med køretøjsenheden, og efterfølgende skal GNSS-positionsoplysningerne kontrolleres.

394) Kontrolapparatet skal være anbragt på en sådan måde i køretøjet, at føreren har adgang til de nødvendige funktioner fra førersædet.

([1]) EUT L 102 af 11.4.2006, s. 1.

▼B

5.2 **Installationsplade**

395) Når apparatet er blevet kontrolleret efter monteringen, anbringes en installationsplade med permanent indgravering eller tryk klart synligt og lettilgængeligt på kontrolapparatet. Hvis dette ikke er muligt, skal pladen fastgøres til køretøjets »B«-søjle, så den er klart synlig. I køretøjer, som ikke har en »B«-søjle, skal installationspladen fastgøres til dørindfatningen på førerens side af køretøjet og være klart synlig under alle omstændigheder.

Efter ethvert indgreb foretaget af en autoriseret installatør eller et autoriseret værksted skal installationspladen udskiftes med en ny plade.

396) Pladen skal være forsynet med mindst følgende oplysninger:

— den autoriserede installatørs eller det autoriserede værksteds navn og adresse eller firmanavn

— køretøjets vejdrejetal efter formlen »w = … imp/km«

— kontrolapparatets konstant, angivet ved »k = … imp/km«

— effektiv dækperiferi i formen »l = … mm«

— dækstørrelse

— datoen for måling af køretøjets vejdrejetal og dets effektive dækperiferi

— køretøjets identifikationsnummer

— om der forefindes eksternt GNSS-udstyr

— serienummeret på det eksterne GNSS-udstyr

— serienummeret på enheden til fjernkommunikation

— serienummeret på alle monterede plomber

— den del af køretøjet, hvor adapteren i givet fald er installeret

— den del af køretøjet, hvor bevægelsessensoren er installeret, hvis den ikke er sluttet til gearkassen, eller der ikke anvendes en adapter

— en angivelse af farven på kablet mellem adapteren og den del af køretøjet, der forsyner denne med impulser

— serienummeret på adapterens indlejrede bevægelsessensor.

397) Der kan udelukkende i forbindelse med M1- og N1-køretøjer, som er forsynet med en adapter i henhold til Kommissionens forordning (EF) nr. 68/2009 ([1]) med seneste ændringer, og hvor det ikke er muligt at anføre alle de nødvendige oplysninger som beskrevet i krav 396, anvendes en anden, supplerende plade. I så fald skal den supplerende plade indeholde mindst de sidste fire led i krav 396.

([1]) Kommissionens forordning (EF) Nr. 68/2009 af 23. januar 2009 om niende tilpasning til den tekniske udvikling af Rådets forordning (EØF) nr. 3821/85 om kontrolapparatet inden for vejtransport (EUT L 21 af 24.1.2009, s. 3).

▼B

Denne anden, supplerende plade anbringes, hvis den anvendes, ved siden af den første primære plade, som er beskrevet i krav 396, og skal have det samme beskyttelsesniveau. Endvidere skal der på den sekundære plade også være anført navn, adresse eller firmanavn på den autoriserede installatør eller det autoriserede værksted, som har udført monteringen, samt monteringsdatoen.

5.3 **Plombering**

398) Følgende dele skal være plomberet:

— enhver tilslutning, hvis afbrydelse medfører uopdagede ændringer eller uopdaget tab af data (dette kan f.eks. gælde for bevægelsessensorens tilslutning til gearkassen, adapteren til M1/N1-køretøjer, den eksterne GNSS-tilslutning eller køretøjsenheden)

— monteringspladen, medmindre den er anbragt således, at den ikke kan fjernes, uden at påskriften ødelægges.

399) Ovennævnte plomberinger kan brydes:

— i nødstilfælde

— med det formål at montere, justere eller reparere en hastighedsbegrænser eller anden anordning, som bidrager til trafiksikkerheden, forudsat at kontrolapparatet fortsat fungerer pålideligt og korrekt og plomberes igen af en autoriseret installatør eller et autoriseret værksted (i overensstemmelse med afsnit 6) straks efter montering af hastighedsbegrænser eller trafiksikkerhedsanordning, i andre tilfælde senest efter syv dage.

400) Hver gang disse plomber brydes, udfærdiges en skriftlig begrundelse herfor, som stilles til rådighed for den kompetente myndighed.

401) Plomberne skal bære et identifikationsnummer, som tildeles af fabrikanten. Dette nummer skal være unikt og adskille sig fra ethvert andet plombenummer, der er tildelt af andre plombefabrikanter.

Det unikke identifikationsnummer anføres som en markering i formatet MMNNNNNN, som ikke kan fjernes, hvor MM er et unikt fabrikant-id (databaseregistrering forvaltes af Europa-Kommissionen), og NNNNNN er plombens alfanumeriske nummer, som er unik i fabrikantens regi.

402) På plomberne skal der være plads til, at godkendte installatører, værksteder eller køretøjsfabrikanter kan tilføje et særligt mærke i overensstemmelse med artikel 22, stk. 3, i forordning (EU) nr. 165/2014.

Dette mærke må ikke dække plombens identifikationsnummer.

403) Plombefabrikanterne skal registreres i en særlig database og offentliggøre numrene på deres identifikationsplomber ved at følge en procedure, der skal fastlægges af Europa-Kommissionen.

404) Godkendte værksteder og køretøjsfabrikanter må i henhold til forordning (EU) nr. 165/2014 kun bruge plomber fra de plombefabrikanter, der står opført i ovennævnte database.

▼B

405) Plombefabrikanterne og deres distributører skal sikre fyldestgørende sporbarhedsfortegnelser for de plomber, der sælges til brug som omhandlet i forordning (EU) nr. 165/2014, og de skal fremlægge dem for de kompetente nationale myndigheder efter anmodning.

406) Plombernes unikke identifikationsnumre skal være klart synlige på installationspladen.

6 KONTROL, EFTERSYN OG REPARATIONER

Punkt 5.3 i dette bilag indeholder bestemmelser for, under hvilke omstændigheder plomber må fjernes som omhandlet i artikel 22, stk. 5, i forordning (EØF) nr. 165/2014.

6.1 **Autorisering af installatører, værksteder og køretøjsfabrikanter**

Medlemsstaterne godkender, kontrollerer regelmæssigt og certificerer de organer, som skal udføre:

— montering

— eftersyn

— kontrol

— reparationer.

Værkstedskort må kun udstedes til installatører og/eller værksteder, som er godkendt til aktivering og/eller kalibrering af kontrolapparater i overensstemmelse med dette bilag, og som, medmindre det behørigt begrundes:

— ikke er berettiget til et virksomhedskort

— og hvis øvrige faglige virksomhed ikke frembyder en mulig fare for systemets overordnede sikkerhed som foreskrevet i tillæg 10.

6.2 **Kontrol af nye eller reparerede instrumenter**

407) For hver enkelt ny eller repareret anordning kontrolleres den korrekte funktion og nøjagtigheden af angivelser og optegnelser inden for de i afsnit 3.2.1, 3.2.2, 3.2.3 og 3.3 fastlagte grænser ved plombering i henhold til afsnit 5.3 og kalibrering.

6.3 **Monteringsinspektion**

408) Ved monteringen i et køretøj skal apparatet og hele installationen opfylde bestemmelserne i afsnit 3.2.1, 3.2.2, 3.2.3 og 3.3 vedrørende maksimale tolerancer.

6.4 **Periodisk kontrol**

409) Periodisk eftersyn af det i køretøjet monterede apparat skal foretages efter reparation af apparatet, efter ændring af køretøjets vejdrejetal, efter ændring af den effektive dækperiferi, når apparatets UTC-tid har været over 20 minutter forkert, når køretøjets indregistreringsnummer er ændret, og mindst én gang inden for to år (24 måneder) efter den seneste kontrol.

410) Især kontrolleres:

— at kontrolapparatet fungerer korrekt, herunder også lagring af data på takografkortet og kommunikationen med læsere til fjernkommunikation

▼B

— at overholdelse af bestemmelserne i afsnit 3.2.1 og 3.2.2 om maksimale tolerancer ved monteringen er sikret

— at overensstemmelse med bestemmelserne i afsnit 3.2.3 og 3.3 er sikret

— at kontrolapparatet er forsynet med typegodkendelsesmærke

— at der er anbragt en installationsplade som defineret i krav 396 og en typeplade som defineret i krav 225

— dækstørrelsen og den faktiske dækperiferi

— at der ikke er manipulerende anordninger fastgjort til kontrolapparatet

— at plomberne sidder korrekt og er i god stand, at deres identifikationsnumre er gyldige (godkendt plombefabrikant i Europa-Kommissionens database), og at deres identifikationsnumre svarer til markeringerne på installationspladen (se krav 401).

411) Hvis det konstateres, at en af hændelserne i afsnit 3.9 (Detektion af hændelser og/eller fejl) er indtruffet siden det sidste eftersyn, og takograffabrikanter og/eller nationale myndigheder anser den for potentielt at kunne bringe kontrolapparatets sikkerhed i fare, skal værkstedet:

a. sammenligne identifikationsdataene for den bevægelsessensor, der er tilsluttet gearkassen, med identifikationsdataene for den bevægelsessensor, der er samparret med køretøjsenheden og registreret deri

b. kontrollere, om de oplysninger, der er anført på installationspladen, svarer til de oplysninger, der er registreret i køretøjsenheden

c. kontrollere, om bevægelsessensorens serienummer og godkendelsesnummer, hvis de er trykt på bevægelsessensoren, svarer til de oplysninger, der er lagret i kontrolapparatets datalager

d. sammenligne eventuelle identifikationsdata på det eksterne GNSS-udstyrs typeplade med de data, der er lagret i køretøjsenhedens datalager.

412) Værkstedet skal i eftersynsrapporterne nævne resultater, der vedrører brudte plomberinger eller manipulerende anordninger. Værkstedet skal opbevare disse rapporter i mindst to år, og de skal til enhver tid stilles til rådighed for den kompetente myndighed efter anmodning.

413) Disse inspektioner skal omfatte kalibrering og forebyggende udskiftning af de plomber, som værkstedet har ansvaret for at montere.

6.5 **Måling af fejl**

414) Måling af fejl under installation og drift gennemføres på følgende betingelser, der er at anse som normale afprøvningsbetingelser:

— ubelastet køretøj i køreklar stand

— dæktryk i overensstemmelse med fabrikantens angivelser

▼B

— dækslitage inden for de ved national lov givne grænser

— køretøjets bevægelse:

— Køretøjet skal bevæge sig frem ved egen motorkraft i lige linje på jævnt terræn ved en hastighed på 50 ± 5 km/t. Måledistancen skal være mindst 1 000 m.

— Prøven kan også udføres på anden måde, forudsat tilsvarende nøjagtighed opnås, f.eks. med en egnet prøvestand.

6.6 **Reparationer**

415) Værksteder skal kunne overføre data fra kontrolapparatet for at anvende dem til tilbagemelding til den pågældende transportvirksomhed.

416) Det godkendte værksted skal til transportvirksomheden udfærdige en attest om manglende dataoverførsel, når fejl ved kontrolapparatet bevirker, at tidligere registrerede data ikke kan overføres, heller ikke efter reparation på det pågældende værksted. Værkstederne opbevarer en kopi af hver attest, som de har udstedt, i mindst to år.

7 UDSTEDELSE AF KORT

De af medlemsstaterne oprettede kortudstedelsesprocesser skal være i overensstemmelse med følgende:

417) I kortnummeret på et takografkort, som for første gang udstedes til en ansøger, indgår et fortløbende indeks (hvis relevant), et erstatningsindeks samt et fornyelsesindeks stillet på »0«.

418) På alle ikke personlige takografkort, som udstedes til en enkelt kontrolinstans, et enkelt værksted eller en enkelt transportvirksomhed, skal kortnumrenes første 13 cifre være identiske, og alle kortnumre skal have forskelligt fortløbende indeks.

419) Et takografkort, som udstedes til erstatning for et eksisterende takografkort, skal have samme kortnummer som det udskiftede, bortset fra udskiftningsindekset, som skal være øget med »1« (i rækkefølgen 0, …, 9, A, …, Z).

420) Et takografkort, som udstedes til erstatning for et eksisterende takografkort, skal have samme udløbsdato som det erstattede.

421) Et takografkort, som udstedes til fornyelse for et eksisterende takografkort, skal have samme kortnummer som det fornyede, bortset fra udskiftningsindekset, som skal være stillet på »0«, og fornyelsesindekset, som skal være øget med »1« (i rækkefølgen 0, …, 9, A, …, Z).

422) Udskiftning af et eksisterende takografkort med det formål at ændre administrative data skal følge reglerne for fornyelse, når det finder sted i samme medlemsstat, og reglerne for første udstedelse, når det finder sted i en anden medlemsstat.

423) »Kortindehavers efternavn« skal for ikkepersonlige værkstedseller kontrolkort udfyldes med værkstedets eller kontrolinstansens navn eller med installatørens eller kontrolmedarbejderens navn, hvis den enkelte medlemsstat vælger dette.

▼B

424) Medlemsstaterne udveksler data elektronisk for at sikre, at det førerkort, som de udsteder, er unikt, i overensstemmelse med artikel 31 i forordning (EU) nr. 165/2014.

8 TYPEGODKENDELSE AF KONTROLAPPARATUR OG TAKOGRAFKORT

8.1 **Almindelige bestemmelser**

I dette afsnit forstås ved »kontrolapparat« »kontrolapparatet eller dets komponenter«. Der kræves ingen typegodkendelse af det/de kabler, som forbinder bevægelsessensoren med køretøjsenheden, det eksterne GNSS-udstyr med køretøjsenheden eller faciliteten til fjernkommunikation med køretøjsenheden. Det papir, som skal anvendes af kontrolapparatet, anses for en komponent i kontrolapparatet.

En fabrikant kan anmode om typegodkendelse af sine komponenter sammen med enhver type bevægelsessensor, eksternt GNSS-udstyr og omvendt, hvis den enkelte komponent er i overensstemmelse med kravene i dette bilag. Alternativt kan fabrikanter anmode om typegodkendelse af kontrolapparater.

425) Ved forelæggelse til godkendelse skal kontrolapparatet være komplet med eventuelt indbygget ekstra tilbehør.

426) Typegodkendelse af kontrolapparater og takografkort skal omfatte sikkerhedsrelevante prøver, funktionsprøver og interoperabilitetsprøver. Positive resultater for hver af disse prøver angives ved en passende attest.

427) Medlemsstaternes typegodkendelsesmyndigheder udsteder ikke en typegodkendelsesattest, medmindre de er i besiddelse af:

— en sikkerhedsattest

— en funktionsattest

— og en interoperabilitetsattest

for det kontrolapparat eller det takografkort, som typegodkendelsesansøgningen omfatter.

428) Enhver ændring af en af apparatets komponenter eller af arten af de til dets fremstilling anvendte materialer skal, inden apparatet tages i brug, anmeldes til den myndighed, som har typegodkendt apparatet. Denne myndighed skal over for fabrikanten bekræfte udvidelsen af typegodkendelsen eller kan kræve opdatering eller bekræftelse af de relevante funktions-, sikkerheds- og/eller interoperabilitetsattester.

429) Procedurer til opgradering af programmel i et allerede monteret kontrolapparat skal være godkendt af den myndighed, som meddelte typegodkendelse af kontrolapparatet. Opgradering af programmel må ikke ændre eller slette føreraktivitetsdata, som er gemt i kontrolapparatet. Programmel må kun opgraderes under ansvar af kontrolapparatets fabrikant.

430) Typegodkendelse af softwareændringer, som har til formål at opgradere et tidligere typegodkendt kontrolapparat kan ikke nægtes, hvis ændringerne kun vedrører funktioner, som ikke beskrives i dette bilag. Indførelse af nye tegnsæt kan være undtaget fra en softwareopgradering af et kontrolapparat, hvis det ikke er teknisk muligt.

▼B

8.2 **Sikkerhedsattest**

431) Sikkerhedsattesten udstedes i overensstemmelse med bestemmelserne i tillæg 10 til dette bilag. De dele af kontrolapparatet, der skal certificeres, er køretøjsenheden, bevægelsessensoren, det eksterne GNSS-udstyr og takografkortet.

432) Hvis sikkerhedscertificeringsmyndighederne ekstraordinært afviser at certificere et nyt apparat med den begrundelse, at sikkerhedsmekanismerne er forældede, meddeles der alligevel typegodkendelse udelukkende under denne særlige og ekstraordinære omstændighed, hvis der ikke eksisterer en alternativ løsning, som er i overensstemmelse med forordningen.

433) Under denne omstændighed underretter den pågældende medlemsstat omgående Europa-Kommissionen, som senest 12 kalendermåneder efter meddelelsen af typegodkendelse, iværksætter en procedure, der sikrer, at sikkerhedsniveauet bringes tilbage til det oprindelige niveau.

8.3 **Funktionsattest**

434) Ansøgere til typegodkendelse skal forsyne medlemsstatens typegodkendelsesmyndigheder med alt det materiale og al den dokumentation, som myndigheden anser for nødvendigt.

435) Fabrikanterne stiller de relevante prøver af produkterne til typegodkendelse og den tilhørende nødvendige dokumentation til rådighed for de laboratorier, der er udpeget til at udføre funktionsprøver, senest en måned efter at anmodningen er fremsat. Den anmodende enhed afholder eventuelle udgifter i forbindelse med denne anmodning. Laboratoriet skal behandle alle kommercielt følsomme oplysninger fortroligt.

436) Der må ikke udstedes en funktionsattest til fabrikanten, før mindst alle de i tillæg 9 foreskrevne funktionsprøver er udført med tilfredsstillende resultat.

437) Funktionsattesten udstedes af typegodkendelsesmyndigheden. Denne attest skal ud over navnet på modtageren og identifikation af modellen indeholde en specificeret liste over de udførte prøver og resultaterne heraf.

438) Funktionsattesten for en komponent til et kontrolapparat skal også indeholde typegodkendelsesnumrene for de andre typegodkendte kompatible komponenter til kontrolapparatet, der afprøves ved certificering af det.

439) I funktionsattesten for en komponent til et kontrolapparat skal det desuden angives, hvilken ISO- eller CEN-standard der er anvendt til at certificere den funktionelle grænseflade.

8.4 **Interoperabilitetsattest**

440) Interoperabilitetsprøver udføres af ét enkelt laboratorium under Europa-Kommissionens myndighed og ansvar.

441) Laboratoriet registrerer de af fabrikanterne indgivne anmodninger om interoperabilitetsprøver i den kronologiske rækkefølge, de modtages.

442) Anmodningerne vil først blive officielt registreret, når laboratoriet er i besiddelse af:

— det fuldstændige sæt materiale og dokumenter, som er nødvendige til sådanne interoperabilitetsprøver

▼B

— den tilsvarende sikkerhedsattest

— den tilsvarende funktionsattest.

Fabrikanten underrettes om datoen for registreringen.

443) Laboratoriet udfører ikke interoperabilitetsprøver for kontrolapparater eller takografkort, for hvilke der ikke er udstedt et sikkerhedscertifikat og en funktionsattest, undtagen under de særlige omstændigheder, der er nævnt i krav 432.

444) Enhver fabrikant, som anmoder om interoperabilitetsprøver, forpligter sig til at overlade hele det sæt materiale og dokumenter, som han har fremskaffet med henblik på udførelse af prøverne, til det laboratorium, som forestår prøverne.

445) Interoperabilitetsprøver skal udføres i overensstemmelse med bestemmelserne i tillæg 9 til dette bilag, og i prøverne skal indgå henholdsvis alle de typer kontrolapparater og takografkort:

— for hvilke typegodkendelsen stadig er gyldig eller

— for hvilke typegodkendelsen er under behandling, og for hvilke der foreligger en gyldig interoperabilitetsattest.

446) Interoperabilitetsprøverne skal omfatter alle de generationer af kontrolapparater og takografkort, der stadig er i brug.

447) Der må ikke udstedes en interoperabilitetsattest til fabrikanten, før mindst alle de foreskrevne interoperabilitetsprøver er udført med tilfredsstillende resultat.

448) Giver interoperabilitetsprøverne ikke tilfredsstillende resultat med en (et) eller flere af kontrolapparaterne eller takografkortene, vil interoperabilitetsattesten ikke blive udstedt, før den anmodende fabrikant har gennemført de nødvendige ændringer og interoperabilitetsprøverne har givet tilfredsstillende resultat. Laboratoriet skal udfinde årsagen til problemet med assistance fra de fabrikanter, der berøres af denne interoperabilitetsmangel og skal søge at bistå den anmodende producent med at finde en teknisk løsning. I tilfælde, hvor fabrikanten har ændret sit produkt, påhviler det fabrikanten at søge de pågældende myndigheders bekræftelse på, at sikkerhedsattest og funktionsattest stadig er gyldige.

449) Interoperabilitetsattesten er gyldig i seks måneder. Efter slutningen af denne periode ophæves den, hvis fabrikanten ikke har modtaget en tilsvarende typegodkendelsesattest. Den fremsendes af fabrikanten til den typegodkendende myndighed i den medlemsstat, som har udstedt funktionsattesten.

450) Intet element, som kan tænkes at give anledning til en interoperabilitetsmangel, må anvendes til at opnå fortjeneste eller til at opnå en dominerende stilling.

8.5 **Typegodkendelsesattest**

451) Den typegodkendende myndighed i medlemsstaten kan udstede typegodkendelsesattesten, så snart den er i besiddelse af de nødvendige tre attester.

▼B

452) Typegodkendelsesattesten for en komponent til et kontrolapparat skal også indeholde typegodkendelsesnumrene for det andet typegodkendte interoperable kontrolapparatur.

453) Typegodkendelsesattesten kopieres af den typegodkendende myndighed til det laboratorium, som forestår interoperabilitetsprøverne, på det tidspunkt hvor den udstedes til fabrikanten.

454) Det laboratorium, som forestår interoperabilitetsprøverne, skal have et offentligt websted med en opdateret liste over de kontrolapparat- eller takografmodeller,

— for hvilke der er registreret en anmodning om interoperabilitetsprøver,

— for hvilke der er udstedt en interoperabilitetsattest (også selv om den er foreløbig),

— for hvilke der er udstedt en typegodkendelsesattest.

8.6 **Undtagelsesprocedure: første interoperabilitetsattest til kontrolapparater og takografkort af anden generation**

455) I en periode på fire måneder efter at et første sammenhørende sæt kontrolapparat af anden generation og tilhørende takografkort af anden generation (fører-, værksteds-, kontrol- og virksomhedskort) er attesteret som interoperabelt, anses en eventuelt udstedt interoperabilitetsattest (herunder også den første attest) vedrørende anmodninger registreret i denne periode for foreløbig.

456) Anses alle de omhandlede produkter efter slutningen af denne periode for indbyrdes interoperable, bliver alle tilsvarende interoperabilitetsattester endelige.

457) Findes der i løbet af denne periode interoperabilitetsmangel, skal det laboratorium, som forestår interoperabilitetsprøverne, finde årsagerne til problemerne med assistance fra alle de berørte fabrikanter og opfordre dem til at gennemføre de nødvendige ændringer.

458) Tilbagestår der efter slutningen af denne periode interoperabilitetsproblemer, skal det laboratorium, som forestår interoperabilitetsprøverne, i samarbejde med de pågældende fabrikanter og med de typegodkendelsesmyndigheder, som udstedte de tilsvarende funktionsattester, finde årsagen til interoperabilitetsmanglerne og fastlægge, hvilke ændringer hver af de pågældende fabrikanter bør foretage. Søgningen efter tekniske løsninger må vare højst to måneder; findes der derved ingen fælles løsning, tager Kommissionen efter samråd med det laboratorium, som forestår interoperabilitetsprøverne, stilling til, hvilke(t) apparat(er) og kort, der skal udstedes en endelig interoperabilitetsattest for, og angiver begrundelse herfor.

459) Eventuelle anmodninger om interoperabilitetsprøver, som af laboratoriet registreres i perioden fra fire måneder efter udstedelse af den første foreløbige interoperabilitetsattest til datoen for den i krav 455 omhandlede Kommissionsbeslutning, stilles i bero, til de første interoperabilitetsproblemer er løst. Disse anmodninger behandles derefter i samme kronologiske rækkefølge, som de er registreret.

▼B

Tillæg 1

DATAORDLISTE

INDHOLDSFORTEGNELSE

1. INDLEDNING

1.1. Fremgangsmåde anvendt ved definition af datatyper

1.2. Referencer

2. DEFINITIONER AF DATATYPER

2.1. ActivityChangeInfo

2.2. Adresse

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. Attester

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. Afstand

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. Speed

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. DEFINITIONER AF VÆRDI- OG STØRRELSESOMRÅDE

4. TEGNSÆT

5. KODNING

6. OBJEKTIDENTIFIKATORER OG APPLIKATIONSIDENTIFIKATORER

6.1. Objektidentifikatorer

6.2. Applikationsidentifikatorer

1. INDLEDNING

Dette tillæg fastlægger de dataformater, dataelementer og datastrukturer, som skal anvendes i kontrolapparater og takografkort.

1.1. **Fremgangsmåde anvendt ved definition af datatyper**

Til definition af datatyperne i dette tillæg er anvendt Abstract Syntax Notation One (ASN.1). På denne måde kan der defineres enkle og strukturerede data, uden at dette forudsætter en nærmere bestemt overføringssyntaks (kodningsregler), som vil være applikations- og miljøafhængig.

ASN.1-typebenævnelser er tildelt efter ISO/IEC 8824-1. Dette indebærer:

— at datatypens betydning, hvor det er muligt, er givet gennem de valgte navne,

— at når en datatype er sammensat af andre datatyper, består datatypens navn stadig af én enkelt sekvens af alfabetiske tegn med stort begyndelsesbogstav, dog anvendes store bogstaver inde i navnet til at angive den tilsvarende betydning,

— at datatypernes navne sædvanligvis hænger sammen med navnet på de datatyper, de er opbygget af, det udstyr, data bliver lagret på, og den funktion, der knytter sig til de pågældende data.

Er en ASN.1-type i forvejen defineret som del af en anden standard og relevant til brug i kontrolapparatet, vil den pågældende ASN.1-type være defineret i dette tillæg.

For at give mulighed for forskellige typer kodningsregler er visse ASN.1-typer i dette tillæg begrænset ved identifikatorer for værdiområdet. Identifikatorerne for værdiområde er defineret i punkt 3 og tillæg 2.

1.2. **Referencer**

I dette tillæg er følgende referencer anvendt:

ISO 639	Code for the representation of names of languages. First Edition: 1988.

▼B

ISO 3166	Codes for the representation of names of countries and their subdivisions — Part 1: Country codes, 2013
ISO 3779	Road vehicles — Vehicle identification number (VIN) — Content and structure. 2009
ISO/IEC 7816-5	Identification cards — Integrated circuit cards — Part 5: Registration of application providers. Second edition: 2004.
ISO/IEC 7816-6	Identification cards — Integrated circuit cards — Part 6: Interindustry data elements for interchange, 2004 + Technical Corrigendum 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	Information technology — 8 bit single-byte coded graphic character sets — Part 1: Latin alphabet No.1. First edition: 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 Technical Guideline TR-03110-3, Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS Token — Part 3 Common Specifications, version 2.20, 3. februar 2015

2. DEFINITIONER AF DATATYPER

For nedenstående datatyper vil datafeltet som standardværdi for ”ukendt” eller ”ikkerelevant” indhold være udfyldt med ‘FF’-bytes.

Alle datatyper anvendes til applikationer af første og anden generation, medmindre andet anføres.

2.1. **ActivityChangeInfo**

Med denne datatype kan der inden for et to bytes stort ord kodes skift af kortlæserstatus kl. 00:00 og/eller førerstatus kl. 00:00 og/eller skift af aktivitet og/eller skift af kørestatus og/eller skift af kortstatus for en fører eller medchauffør. Denne datatype er knyttet til krav 105, 266, 291, 320, 321, 343 og 344 i bilag 1C.

```
ActivityChangeInfo ::= OCTET STRING (SIZE(2))
```

Tilordnet værdi — Oktet udsluttet: ‘scpaatttttttttt’B (16 bit)

For registreringer i datalageret (eller status for kortplads):

‘s’B	Kortplads:
	‘0’B: FØRER
	‘1’B: MEDCHAUFFØR

▼B

‘c’B	Kørestatus:
	‘0’B: ÉN FØRER
	‘1’B: FØRERHOLD
‘p’B	Status for fører- (eller værksteds-)kortet i den pågældende kortplads:
	‘0’B: ISAT, der er isat et kort
	‘1’B: IKKE ISAT, kort er ikke isat (eller er taget ud)
‘aa’B	Aktivitet:
	‘00’B: PAUSE/HVILE
	‘01’B: RÅDIGHED
	‘10’B: ARBEJDE
	‘11’B: KØRSEL
‘ttttttttttt’B	Tidspunkt for ændringen: Antal minutter siden 00h00 den pågældende dag.

For registreringer på fører- (eller værksteds-)kortet (og førerstatus):

‘s’B	Kortplads (ikke relevant når ‘p’ = 1, se dog bemærkning nedenfor):
	‘0’B: FØRER
	‘1’B: MEDCHAUFFØR
‘c’B	Kørestatus (når ‘p’ = 0) eller
	Efter aktivitetsstatus (når ‘p’ = 1):
	‘0’B: ÉN FØRER
	‘0’B: UKENDT
	‘1’B: FØRERHOLD
	‘1’B: KENDT (= indlæst manuelt)
‘p’B	Kortstatus:
	‘0’B: ISAT, kortet er sat i et kontrolapparat
	‘1’B: IKKE ISAT, kortet er ikke isat (eller er taget ud)
‘aa’B	Aktivitet (ikke relevant, når ‘p’ = 1 og ‘c’ = 0, se dog bemærkning nedenfor):
	‘00’B: PAUSE/HVILE
	‘01’B: RÅDIGHED
	‘10’B: ARBEJDE
	‘11’B: KØRSEL
‘ttttttttttt’B	Tidspunkt for ændringen: Antal minutter siden 00h00 den pågældende dag.

▼B

Bemærkning vedrørende tilfældet "udtagning af kort":

Når kortet er taget ud:

— 's' er relevant og angiver den kortplads, kortet er fjernet fra

— 'c' skal være sat til 0

— 'p' skal være sat til 1

— 'aa' skal kode den aktuelle aktivitet, som er valgt på det pågældende tidspunkt

Bit 'c' og 'aa' i ordet (gemt på et kort) kan ved senere manuel indlæsning overskrives svarende til indlæsningen.

2.2. **Adresse**

En adresse.

```
Address ::= SEQUENCE {
   codePage                              INTEGER (0..255),
   address                               OCTET STRING (SIZE(35))
}
```

codePage angiver et tegnsæt, der er defineret i afsnit 4

address er en adresse, som er indkodet med det angivne tegnsæt.

2.3. **AESKey**

Anden generation:

En AES-nøgle med en længde på 128, 192 eller 256 bit.

```
AESKey ::= CHOICE {
   aes128Key                             AES128Key,
   aes192Key                             AES192Key,
   aes256Key                             AES256Key
}
```

Tilordnet værdi: Ikke yderligere angivet.

2.4. **AES128Key**

Anden generation:

En AES128-nøgle.

```
AES128Key ::= SEQUENCE {
   length                                INTEGER(0..255),
   aes128Key                             OCTET STRING (SIZE(16))
}
```

length er længden af AES128-nøglen i oktetter.

aes128Key er en AES-nøgle med en længde på 128 bit.

Tilordnet værdi:

Længden skal have værdien 16.

▼B

2.5. **AES192Key**

Anden generation:

En AES192-nøgle.

```
AES192Key ::= SEQUENCE {
   length                                  INTEGER(0..255),
   aes192Key                               OCTET STRING (SIZE(24))
}
```

length er længden af AES192-nøglen i oktetter.

aes192Key er en AES-nøgle med en længde på 192 bit.

Tilordnet værdi:

Længden skal have værdien 24.

2.6. **AES256Key**

Anden generation:

En AES256-nøgle.

```
AES256Key ::= SEQUENCE {
   length                                  INTEGER(0..255),
   aes256Key                               OCTET STRING (SIZE(32))
}
```

length er længden af AES256-nøglen i oktetter.

aes256Key er en AES-nøgle med en længde på 256 bit.

Tilordnet værdi:

Længden skal have værdien 32.

2.7. **BCDString**

BCDString anvendes til at fremstille decimaltal ved binær kode (BCD). Denne datatype anvendes til at fremstille ét decimalciffer ved én semioktet (4 bit). BCDString er baseret på ISO/IEC 8824-1 ”Character-StringType”.

```
BCDString ::= CHARACTER STRING (WITH COMPONENTS {
   identification ( WITH COMPONENTS {
   fixed PRESENT }) })
```

BCDString anvender ”hstring”-notation. Det hexadecimale tegn længst til venstre skal være mest betydende semioktet i første oktet. Til frembringelse af flere oktetter indsættes efter behov foranstillede nul-semioktetter fra semioktetpositionen længst til venstre i den første oktet.

De tilladte cifre er: 0, 1, .. 9.

2.8. **CalibrationPurpose**

Kode, som forklarer, hvorfor der blev registreret et sæt kalibreringsparametre. Denne datatype er knyttet til bilag 1B, krav 097 og 098, og bilag 1C, krav 119.

```
CalibrationPurpose ::= OCTET STRING (SIZE(1))
```

▼B

Tilordnet værdi:

Første generation:

'00'H	reserveret værdi
'01'H	aktivering: registrering af de kalibreringsparametre, som er kendt i det øjeblik, hvor køretøjsenheden aktiveres
'02'H	første installation: første kalibrering af køretøjsenheden, efter at den er aktiveret
'03'H	installation: første kalibrering af køretøjsenheden i det aktuelle køretøj
'04'H	periodisk eftersyn.

Anden generation:

Ud over værdierne for første generation anvendes følgende værdier:

'05'H	virksomhedens indlæsning af VRN
'06'H	tidsjustering uden kalibrering
'07'H til '7F'H	RFU
'80'H til 'FF'H	Fabrikantspecifik.

2.9. **CardActivityDailyRecord**

Oplysninger, gemt på kortet, vedrørende føreraktiviteterne for en given kalenderdag. Denne datatype er knyttet til krav 266, 291, 320 og 343 i bilag 1C.

```
CardActivityDailyRecord ::= SEQUENCE {
   activityPreviousRecordLength         INTEGER(0..CardActivityLengthRange),
   activityRecordLength                 INTEGER(0..CardActivityLengthRange),
   activityRecordDate                   TimeReal,
   activityDailyPresenceCounter         DailyPresenceCounter,
   activityDayDistance                  Distance,
   activityChangeInfo                   SET SIZE(1..1440) OF ActivityChangeInfo
}
```

activityPreviousRecordLength er den totale længde i bytes af den foregående døgnpost. Maksimumværdien er givet ved længden af den OCTET STRING, som indeholder disse poster (se CardActivityLengthRange, tillæg 2, punkt 4). Når denne post er den ældste døgnpost, skal activityPreviousRecordLength sættes til 0.

activityRecordLength er den totale længde i bytes af denne post. Maksimumværdien er givet ved længden af den OCTET STRING, som indeholder disse poster.

activityRecordDate er postens dato.

▼B

activityDailyPresenceCounter er tælleren for daglig tilstedeværelse for kortet det pågældende døgn.

activityDayDistance er den totale afstand, som er tilbagelagt det pågældende døgn.

activityChangeInfo er ActivityChangeInfo-datasættet for føreren det pågældende døgn. Det kan indeholde indtil 1 440 værdier (ét aktivitetsskift pr. minut). Dette datasæt indeholder altid ActivityChangeInfo med kode for førerstatus kl. 00:00.

2.10. **CardActivityLengthRange**

Antal bytes, som i et fører- eller værkstedskort er til rådighed for lagring af poster vedrørende føreraktivitet.

```
CardActivityLengthRange ::= INTEGER(0..2^16-1)
```

Tilordnet værdi: se tillæg 2.

2.11. **CardApprovalNumber**

Kortets typegodkendelsesnummer.

```
CardApprovalNumber ::= IA5String(SIZE(8))
```

Tilordnet værdi:

Godkendelsesnummeret skal tilvejebringes som offentliggjort på Europa-Kommissionens relevante websted, dvs. f.eks. med eventuelle bindestreger. Godkendelsesnummeret skal være venstrejusteret.

2.12. **CardCertificate**

Første generation:

Certifikat for et korts offentlige nøgle.

```
CardCertificate ::= Certificate
```

2.13. **CardChipIdentification**

Oplysninger, gemt på et kort, til identifikation af kortets integrerede kreds (IC) (Bilag 1C, krav 249). icSerialNumber identificerer sammen med icManufacturingReferences kortets chip entydigt. icSerialNumber alene identificerer ikke kortets chip entydigt.

```
CardChipIdentification ::= SEQUENCE {
   icSerialNumber                       OCTET STRING (SIZE(4)),
   icManufacturingReferences            OCTET STRING (SIZE(4))
}
```

icSerialNumber er serienummeret på den integrerede kreds.

icManufacturingReferences er id'et på fabrikanten af den integrerede kreds.

2.14. **CardConsecutiveIndex**

Et fortløbende kortindeks (definition h)).

```
CardConsecutiveIndex ::= IA5String(SIZE(1))
```

Tilordnet værdi: (Se bilag 1C, afsnit 7)

Rækkefølge af forøgelse: '0, …, 9, A, …, Z, a, …, z'

▼B

2.15. **CardControlActivityDataRecord**

Oplysninger, gemt på et fører- eller værkstedskort, vedrørende den seneste kontrol, som føreren har været genstand for (bilag 1C, krav 274, 299, 327 og 350).

```
CardControlActivityDataRecord ::= SEQUENCE {
   controlType                          ControlType,
   controlTime                          TimeReal,
   controlCardNumber                    FullCardNumber,
   controlVehicleRegistration           VehicleRegistrationIdentification,
   controlDownloadPeriodBegin           TimeReal,
   controlDownloadPeriodEnd             TimeReal
}
```

controlType er kontrollens type.

controlTime er dato og klokkeslæt for kontrollen.

controlCardNumber er FullCardNumber for den kontrollør, som har foretaget kontrollen.

controlVehicleRegistration er indregistreringsnummer og registrerende medlemsstat for det køretøj, i hvilket kontrollen fandt sted.

controlDownloadPeriodBegin og **controlDownloadPeriodEnd** angiver, ved dataoverførsel, den periode, for hvilken dataoverførsel har fundet sted.

2.16. **CardCurrentUse**

Oplysninger om kortets aktuelle anvendelse (bilag 1C, krav 273, 298, 326 og 349).

```
CardCurrentUse ::= SEQUENCE {
   sessionOpenTime                      TimeReal,
   sessionOpenVehicle                   VehicleRegistrationIdentification
}
```

sessionOpenTime er det tidspunkt, hvor kortet er indsat med henblik på den aktuelle anvendelse. Dette dataelement sættes til nul, når kortet tages ud.

sessionOpenVehicle er identifikationen af det aktuelt anvendte køretøj og bliver sat ved isætning af kortet. Dette dataelement sættes til nul, når kortet tages ud.

2.17. **CardDriverActivity**

Oplysninger, gemt på et fører- eller værkstedskort, vedrørende førerens aktiviteter (bilag 1C, krav 267, 268, 292, 293, 321 og 344).

```
CardDriverActivity ::= SEQUENCE {
   activityPointerOldestDayRecord       INTEGER(0.. CardActivityLengthRange-1),
   activityPointerNewestRecord          INTEGER(0.. CardActivityLengthRange-1),
   activityDailyRecords                 OCTET STRING
                                        (SIZE(CardActivityLengthRange))
}
```

activityPointerOldestDayRecord angiver begyndelsen på lagerpladsen (antal bytes fra strengens begyndelse) for den ældste fuldstændige døgnpost i activityDailyRecords-strengen. Maksimumværdien er givet ved længden af strengen.

▼B

activityPointerNewestRecord angiver begyndelsen på lagerpladsen (antal bytes fra strengens begyndelse) for den seneste døgnpost i activityDailyRecords-strengen. Maksimumværdien er givet ved længden af strengen.

activityDailyRecords er den plads, der er til rådighed til at gemme data vedrørende førerens aktivitet (datastruktur: CardActivityDailyRecord) for hver kalenderdag, hvor kortet har været anvendt.

Tilordnet værdi: Denne oktetstreng bliver cyklisk fyldt op med CardActivityDailyRecord-poster. Ved første gangs brug begynder lagringen ved strengens første byte. Alle nye poster bliver hæftet til slutningen af den foregående. Når strengen er fuld, fortsætter lagringen ved strengens første byte uafhængigt af, om der eventuelt er en afbrydelse inde i et dataelement. Før nye aktivitetsdata placeres i strengen (ved at den aktuelle activityDailyRecord bliver større, eller ved at der indsættes en ny activityDailyRecord) som erstatning for ældre aktivitetsdata, skal activityPointerOldestDayRecord opdateres svarende til den nye placering af den ældste fuldstændige døgnpost, og activityPreviousRecordLength for denne (nye) ældste fuldstændige døgnpost skal nulstilles.

2.18. **CardDrivingLicenceInformation**

Oplysninger, gemt på et førerkort, vedrørende kortindehaverens licensdata (bilag 1C, krav 259 og 284).

```
CardDrivingLicenceInformation ::= SEQUENCE {
   drivingLicenceIssuingAuthority       Name,
   drivingLicenceIssuingNation          NationNumeric,
   drivingLicenceNumber                 IA5String(SIZE(16))
}
```

drivingLicenceIssuingAuthority er den myndighed, som er ansvarlig for udstedelse af førerbeviset.

drivingLicenceIssuingNation er nationaliteten af den myndighed, som har udstedt førerbeviset.

drivingLicenceNumberer førerbevisets nummer.

2.19. **CardEventData**

Oplysninger, gemt på et fører- eller værkstedskort, vedrørende hændelser knyttet til kortindehaveren (bilag 1C, krav, 260, 285, 318 og 341).

```
CardEventData ::= SEQUENCE SIZE(6) OF {
   cardEventRecords                     SET SIZE(NoOfEventsPerType) OF
                                        CardEventRecord
}
```

CardEventData er en sekvens af cardEventRecords, ordnet efter stigende EventFaultType (bortset fra poster vedrørende forsøg på sikkerhedsbrud, som er samlet i sidste del af sekvensen).

cardEventRecords er et sæt hændelsesposter af en given hændelsestype (eller kategori ved hændelser bestående i forsøg på sikkerhedsbrud).

▼B

2.20. **CardEventRecord**

Oplysninger, gemt på et fører- eller værkstedskort, vedrørende en hændelse knyttet til kortindehaveren (bilag 1C, krav 261, 286, 318 og 341).

```
CardEventRecord ::= SEQUENCE {
   eventType                          EventFaultType,
   eventBeginTime                     TimeReal,
   eventEndTime                       TimeReal,
   eventVehicleRegistration           VehicleRegistrationIdentification
}
```

eventType er hændelsens type.

eventBeginTime er hændelsens startdato og -klokkeslæt.

eventEndTime er hændelsens slutdato og -klokkeslæt.

eventVehicleRegistration er indregistreringsnummer og registrerende medlemsstat for det køretøj, hvor hændelsen er indtruffet.

2.21. **CardFaultData**

Oplysninger, gemt på et fører- eller værkstedskort, vedrørende fejl knyttet til kortindehaveren (bilag 1C, krav 263, 288, 318 og 341).

```
CardFaultData ::= SEQUENCE SIZE(2) OF {
   cardFaultRecords                   SET SIZE(NoOfFaultsPerType) OF
                                      CardFaultRecord
}
```

CardFaultData er en sekvens af poster vedrørende fejl ved kontrolapparatet, efterfulgt af en mængde af poster vedrørende kortfejl.

cardFaultRecords er mængden af fejlposter af en given fejlkategori (kontrolapparat eller kort).

2.22. **CardFaultRecord**

Oplysninger, gemt på et fører- eller værkstedskort, vedrørende en fejl knyttet til kortindehaveren (bilag 1C, krav 264, 289, 318 og 341).

```
CardFaultRecord ::= SEQUENCE {
   faultType                          EventFaultType,
   faultBeginTime                     TimeReal,
   faultEndTime                       TimeReal,
   faultVehicleRegistration           VehicleRegistrationIdentification
}
```

faultType er fejlens type.

faultBeginTime er fejlens startdato og -klokkeslæt.

faultEndTime er fejlens slutdato og -klokkeslæt.

faultVehicleRegistration er indregistreringsnummer og registrerende medlemsstat for det køretøj, hvor fejlen er indtruffet.

▼B

2.23. **CardIccIdentification**

Oplysninger, gemt på et kort, til identifikation af kortet med integreret kreds (IC) (bilag 1C, krav 248).

```
CardIccIdentification ::= SEQUENCE {
   clockStop                          OCTET STRING (SIZE(1)),
   cardExtendedSerialNumber           ExtendedSerialNumber,
   cardApprovalNumber                 CardApprovalNumber,
   cardPersonaliserID                 ManufacturerCode,
   embedderIcAssemblerId              EmbedderIcAssemblerId,
   icIdentifier                       OCTET STRING (SIZE(2))
}
```

clockStop er klokstop-tilstand som defineret i tillæg 2.

cardExtendedSerialNumber er IC-kortets unikke serienummer som videre angivet ved datatypen ExtendedSerialNumber.

cardApprovalNumber er kortets typegodkendelsesnummer.

cardPersonaliserID er kortets person-ID kodet som ManufacturerCode.

embedderIcAssemblerId rummer oplysninger om embedder/IC assembler.

icIdentifier er datanavnet for kortets IC og IC-fabrikant som defineret i ISO/IEC 7816-6.

2.24. **CardIdentification**

Oplysninger, gemt på et kort, til identifikation af kortet (bilag 1C, krav 255, 280, 310, 333, 359, 365, 371 og 377).

```
CardIdentification ::= SEQUENCE {
   cardIssuingMemberState             NationNumeric,
   cardNumber                         CardNumber,
   cardIssuingAuthorityName           Name,
   cardIssueDate                      TimeReal,
   cardValidityBegin                  TimeReal,
   cardExpiryDate                     TimeReal
}
```

cardIssuingMemberState er koden på den medlemsstat, som har udstedt kortet.

cardNumberer kortets nummer.

cardIssuingAuthorityName er navnet på den myndighed, der har udstedt kortet.

cardIssueDate er datoen for udstedelse af kortet til den nuværende indehaver.

cardValidityBeginer kortets første gyldighedsdato.

cardExpiryDateer kortets udløbsdato.

▼B

2.25. **CardMACertificate**

Anden generation:

Certifikat for et korts offentlige nøgle til gensidig ægthedsbekræftelse med en køretøjsenhed. Dette certifikats opbygning er nærmere beskrevet i tillæg 11.

```
CardMACertificate ::= Certificate
```

2.26. **CardNumber**

Et kortnummer er defineret ved definition g).

```
CardNumber ::= CHOICE {
   SEQUENCE {
      driverIdentification              IA5String(SIZE(14)),
      cardReplacementIndex              CardReplacementIndex,
      cardRenewalIndex                  CardRenewalIndex
   },
   SEQUENCE {
      ownerIdentification               IA5String(SIZE(13)),
      cardConsecutiveIndex              CardConsecutiveIndex,
      cardReplacementIndex              CardReplacementIndex,
      cardRenewalIndex                  CardRenewalIndex
   }
}
```

driverIdentification er den entydige identifikation af en fører i en medlemsstat.

ownerIdentification er den entydige identifikation af en virksomhed, et værksted eller et kontrolorgan i en medlemsstat.

cardConsecutiveIndex er kortets fortløbende indeks.

cardReplacementIndex er kortets udskiftningsindeks.

cardRenewalIndex er kortets fornyelsesindeks.

Den første sekvens af valget er egnet til kodning af et førerkortnummer, den anden sekvens af valget er egnet til kodning af værksteds-, kontrol- og virksomhedskortnummer.

2.27. **CardPlaceDailyWorkPeriod**

Oplysninger, gemt på et fører- eller værkstedskort, vedrørende de steder, hvor den daglige arbejdstid begynder og/eller slutter (bilag 1C, krav 272, 297, 325 og 348)

```
CardPlaceDailyWorkPeriod ::= SEQUENCE {
   placePointerNewestRecord    INTEGER(0 .. NoOfCardPlaceRecords-1),
   placeRecords                SET SIZE(NoOfCardPlaceRecords) OF PlaceRecord
}
```

placePointerNewestRecorder indekset for den senest opdaterede stedpost.

Tilordnet værdi: Tal svarende til tælleren i stedposten, begyndende med '0' for den første forekomst af stedposterne i strukturen.

placeRecords er den mængde poster, der indeholder oplysninger om de indlæste steder.

▼B

2.28. **CardPrivateKey**

Første generation:

Et korts private nøgle.

```
CardPrivateKey ::= RSAKeyPrivateExponent
```

2.29. **CardPublicKey**

Et korts offentlige nøgle.

```
CardPublicKey ::= PublicKey
```

2.30. **CardRenewalIndex**

Et kortfornyelsesindeks (definition i)).

```
CardRenewalIndex ::= IA5String(SIZE(1))
```

Tilordnet værdi: (se kapitel VII i dette bilag).

‘0’ Første udstedelse.

Rækkefølge af forøgelse: ‘0, …, 9, A, …, Z’

2.31. **CardReplacementIndex**

Et korterstatningsindeks (definition j)).

```
CardReplacementIndex ::= IA5String(SIZE(1))
```

Tilordnet værdi: (se kapitel VII i dette bilag).

‘0’ Oprindeligt kort.

Rækkefølge af forøgelse: ‘0, …, 9, A, …, Z’

2.32. **CardSignCertificate**

Anden generation:

Certifikat for et korts offentlige nøgle til underskrift. Dette certifikats opbygning er nærmere beskrevet i tillæg 11.

```
CardSignCertificate ::= Certificate
```

2.33. **CardSlotNumber**

Kode, som anvendes til at skelne mellem de to kortpladser i en køretøjsenhed.

```
CardSlotNumber ::= INTEGER {
   driverSlot                          (0),
   co-driverSlot                       (1)
}
```

Tilordnet værdi: Ikke yderligere angivet.

2.34. **CardSlotsStatus**

Kode, som angiver den type kort, der sidder i køretøjsenhedens to kortpladser.

```
CardSlotsStatus ::= OCTET STRING (SIZE(1))
```

▼B

Tilordnet værdi — Oktet udsluttet: ‘ccccdddd’B

‘cccc’B Identifikation af den type kort, der sidder i medchaufførens kortplads

‘dddd’B Identifikation af den type kort, der sidder i førerens kortplads

med følgende identifikationskoder:

‘0000’B intet kort isat

‘0001’B et førerkort isat

‘0010’B et værkstedskort isat

‘0011’B et kontrolkort isat

‘0100’B et virksomhedskort isat.

2.35. **CardSlotsStatusRecordArray**

Anden generation:

CardSlotsStatus plus metadata, der anvendes i protokollen for dataoverførsel.

```
CardSlotsStatusRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF CardSlotsStatus
}
```

recordType angiver postens type (CardSlotsStatus). **Tilordnet værdi**: Se RecordType.

recordSize er størrelsen af CardSlotsStatus i bytes.

noOfRecords er antallet af poster i mængden af poster.

records er mængden af CardSlotsStatus-poster.

2.36. **CardStructureVersion**

Kode, som angiver versionen af den struktur, der er implementeret i et takografkort.

```
CardStructureVersion ::= OCTET STRING (SIZE(2))
```

Tilordnet værdi: ‘aabb’H:

‘aa’H Indeks for ændringer af strukturen.

‘00’H for applikationer af første generation

‘01’H for applikationer af anden generation

‘bb’H Indeks for ændringer vedrørende brug af de dataelementer, der er defineret for strukturen, er givet ved den høje byte.

‘00’H for denne version af applikationer af første generation

‘00’H for denne version af applikationer af anden generation

▼B

2.37. **CardVehicleRecord**

Oplysninger, gemt på et fører- eller værkstedskort, vedrørende en anvendelsesperiode for et køretøj på en kalenderdag (bilag 1C, krav 269, 294, 322 og 345).

Første generation:

```
CardVehicleRecord ::= SEQUENCE {
   vehicleOdometerBegin                    OdometerShort,
   vehicleOdometerEnd                      OdometerShort,
   vehicleFirstUse                         TimeReal,
   vehicleLastUse                          TimeReal,
   vehicleRegistration                     VehicleRegistrationIdentification,
   vuDataBlockCounter                      VuDataBlockCounter
}
```

vehicleOdometerBegin er køretøjets kilometerstand ved begyndelsen af anvendelsesperioden for køretøjet.

vehicleOdometerEnd er køretøjets kilometerstand ved slutningen af anvendelsesperioden for køretøjet.

vehicleFirstUse er startdato og -klokkeslæt for køretøjets anvendelsesperiode.

vehicleLastUse er slutdato og -klokkeslæt for køretøjets anvendelsesperiode.

vehicleRegistration er indregistreringsnummer og registrerende medlemsstat for køretøjet.

vuDataBlockCounterer værdien af VuDataBlockCounter ved sidste uddragning af køretøjets anvendelsesperiode.

Anden generation:

```
CardVehicleRecord ::= SEQUENCE {
   vehicleOdometerBegin                    OdometerShort,
   vehicleOdometerEnd                      OdometerShort,
   vehicleFirstUse                         TimeReal,
   vehicleLastUse                          TimeReal,
   vehicleRegistration                     VehicleRegistrationIdentification,
   vuDataBlockCounter                      VuDataBlockCounter,
   vehicleIdentificationNumber             VehicleIdentificationNumber
}
```

Ud over dataelementerne for første generation anvendes følgende dataelement:

VehicleIdentificationNumber er køretøjets identifikationsnummer, der refererer til køretøjet som helhed.

2.38. **CardVehiclesUsed**

Oplysninger, gemt på et fører- eller værkstedskort, vedrørende de køretøjer, der er anvendt af kortindehaveren (bilag 1C, krav 270, 295, 323 og 346).

```
CardVehiclesUsed := SEQUENCE {
   vehiclePointerNewestRecord          INTEGER(0..NoOfCardVehicleRecords-1),
   cardVehicleRecords                  SET SIZE(NoOfCardVehicleRecords) OF
                                       CardVehicleRecord
}
```

vehiclePointerNewestRecord er indekset for den senest opdaterede køretøjspost.

▼B

Tilordnet værdi: Tal svarende til tælleren i køretøjsposten, begyndende med '0' for den første forekomst af køretøjsposterne i strukturen.

cardVehicleRecords er den mængde poster, der indeholder oplysninger om de anvendte køretøjer.

2.39. **CardVehicleUnitRecord**

Anden generation:

Oplysninger, gemt på et fører- eller værkstedskort, vedrørende en anvendt køretøjsenhed (bilag 1C, krav 303 og 351).

```
CardVehicleUnitRecord ::= SEQUENCE {
   timeStamp                              TimeReal,
   manufacturerCode                       ManufacturerCode,
   deviceID                               INTEGER(0..255),
   vuSoftwareVersion                      VuSoftwareVersion
}
```

timeStamp er starten af køretøjsenhedens anvendelsesperiode (dvs. første isætning af kortet i køretøjsenheden i den pågældende periode).

manufacturerCode identificerer fabrikanten af køretøjsenheden.

deviceID identificerer en fabrikants køretøjsenheds type. Værdien er fabrikantspecifik.

vuSoftwareVersion er versionsnummeret på det programmel, der anvendes i køretøjsenheden.

2.40. **CardVehicleUnitsUsed**

Anden generation:

Oplysninger, gemt på et fører- eller værkstedskort, vedrørende de køretøjsenheder, der er anvendt af kortindehaveren (bilag 1C, krav 306 og 352).

```
CardVehicleUnitsUsed := SEQUENCE {
   vehicleUnitPointerNewestRecord       INTEGER(0..NoOfCardVehicleUnitRecords-1),
   cardVehicleUnitRecords               SET SIZE(NoOfCardVehicleUnitRecords) OF
                                        CardVehicleUnitRecord
}
```

vehiclePointerNewestRecord er indekset på den senest opdaterede køretøjsenhedspost.

Tilordnet værdi: Tal svarende til tælleren i køretøjsenhedsposten, begyndende med '0' for den første forekomst af køretøjsenhedsposterne i strukturen.

cardVehicleRecords er den mængde poster, der indeholder oplysninger om de anvendte køretøjsenheder.

2.41. **Attester**

Certifikatet for en offentlig nøgle, udstedt af et certificeringsorgan.

Første generation:

```
Certificate ::= OCTET STRING (SIZE(194))
```

▼B

Tilordnet værdi: Digital underskrift med delvis genfinding af et CertificateContent i henhold til tillæg 11 (fælles sikkerhedsmekanismer): Signature (128 bytes) || Public Key remainder (58 bytes) || Certification Authority Reference (8 bytes).

Anden generation:

```
Certificate ::= OCTET STRING (SIZE(204..341))
```

Tilordnet værdi: Se tillæg 11.

2.42. **CertificateContent**

Første generation:

Det (tydelige) indhold af certifikatet for en offentlig nøgle, som fremgår af tillæg 11, fælles sikkerhedsmekanismer.

```
CertificateContent ::= SEQUENCE {
   certificateProfileIdentifier          INTEGER(0..255),
   certificationAuthorityReference       KeyIdentifier,
   certificateHolderAuthorisation        CertificateHolderAuthorisation,
   certificateEndOfValidity              TimeReal,
   certificateHolderReference            KeyIdentifier,
   publicKey                             PublicKey
}
```

certificateProfileIdentifier er versionen af det tilsvarende certifikat.

Tilordnet værdi: '01h' for denne version.

certificationAuthorityReference angiver den certificeringsmyndighed, som udsteder certifikatet. Den angiver desuden denne certificeringsmyndigheds offentlige nøgle.

certificateHolderAuthorisation identificerer certifikatindehaverens rettigheder.

certificateEndOfValidity er den dato, hvor certifikatet udløber administrativt.

certificateHolderReference identificerer certifikatindehaveren. Den henviser desuden til dennes offentlige nøgle.

publicKey er den offentlige nøgle, som er certificeret ved det pågældende certifikat.

2.43. **CertificateHolderAuthorisation**

Identifikation af en certifikatindehavers rettigheder.

```
CertificateHolderAuthorisation ::= SEQUENCE {
   tachographApplicationID              OCTET STRING(SIZE(6))
   equipmentType                        EquipmentType
}
```

Første generation:

tachographApplicationID er datanavnet på takografapplikationen.

Tilordnet værdi: 'FFh' '54h' '41h' '43h' '48h' '4Fh'. Denne AID er en beskyttet, ikkeregistreret applikationsidentifikator i henhold til ISO/IEC 7816-5.

equipmentType er identifikationen af den type udstyr, som certifikatet er bestemt til.

Tilordnet værdi: i overensstemmelse med datatypen EquipmentType. 0, hvis certifikatet er fra en medlemsstat.

▼B

Anden generation:

tachographApplicationID angiver de seks vigtigste bytes i den tilsvarende applikationsidentifikator (AID) for takografkortet af anden generation. AID for takografkortapplikationen og AID for det eksterne GNSS-udstyr er nærmere beskrevet i afsnit 6.2.

Tilordnet værdi: 'FF 53 4D 52 44 54'

equipmentType er identifikationen af den type udstyr af anden generation, som certifikatet er bestemt til.

Tilordnet værdi: i overensstemmelse med datatypen EquipmentType.

2.44. **CertificateRequestID**

Entydig identifikation af en anmodning om certifikat. Den kan også benyttes som datanavn for et køretøjs offentlige nøgle, hvis serienummeret på den køretøjsenhed, som nøglen er bestemt for, ikke kendes på udfærdigelsestidspunktet for certifikatet.

```
CertificateRequestID ::= SEQUENCE{
   requestSerialNumber                  INTEGER(0..2^32-1),
   requestMonthYear                     BCDString(SIZE(2)),
   crIdentifier                         OCTET STRING(SIZE(1)),
   manufacturerCode                     ManufacturerCode
}
```

requestSerialNumber er et serienummer på anmodningen om certifikatet. Den er entydig for fabrikanten og for måneden nedenfor.

requestMonthYear identificerer måned og år for anmodningen om certifikatet.

Tilordnet værdi: Binært kodet decimaltal for måned (to cifre) og år (to sidste cifre).

crIdentifier er et datanavn, som har til formål at skelne en anmodning om certifikat fra et udvidet serienummer.

Tilordnet værdi: 'FFh'.

manufacturerCode er den numeriske kode for den producent, der anmoder om certifikatet.

2.45. **CertificationAuthorityKID**

Datanavn for den offentlige nøgle tilhørende en certificeringsmyndighed (en medlemsstat eller den europæiske certificeringsmyndighed).

```
CertificationAuthorityKID ::= SEQUENCE{
   nationNumeric                        NationNumeric,
   nationAlpha                          NationAlpha,
   keySerialNumber                      INTEGER(0..255),
   additionalInfo                       OCTET STRING(SIZE(2)),
   caIdentifier                         OCTET STRING(SIZE(1))
}
```

nationNumeric er den numeriske kode for certificeringsmyndigheden.

nationAlpha er den alfanumeriske nationskode for certificeringsmyndigheden.

▼B

keySerialNumber er et serienummer, som er bestemt til at skelne mellem certificeringsmyndighedens forskellige nøgler i tilfælde, hvor der skiftes nøgle.

additionalInfo er et felt på to bytes til supplerende kodning (specifik for certificeringsmyndigheden).

caIdentifier er et datanavn, som har til formål at skelne datanavnet for en certificeringsmyndigheds nøgle fra andre nøgledatanavne.

Tilordnet værdi: '01h'.

2.46. **CompanyActivityData**

Oplysninger, gemt på et virksomhedskort, vedrørende de aktiviteter, der udføres med kortet (bilag 1C, krav 373 og 379)

```
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 er indekset på den senest opdaterede companyActivityRecord.

Tilordnet værdi: Tal svarende til tælleren i virksomhedsaktivitetsposten, begyndende med '0' for første forekomst af virksomhedsaktivitetsposten i strukturen.

companyActivityRecords er mængden af alle virksomhedsaktivitetsposter.

companyActivityRecord er sekvensen af oplysninger vedrørende én virksomhedsaktivitet.

companyActivityType er virksomhedsaktivitetens type.

companyActivityTime er klokkeslæt og dato for virksomhedsaktiviteten.

cardNumberInformation er kortnummer og kortudstedende medlemsstat for det kort, hvis data er blevet overført (i givet fald).

vehicleRegistrationInformation er indregistreringsnummer og registrerende medlemsstat for det køretøj, hvis data er blevet overført, eller som er blevet låst ind eller ud.

downloadPeriodBegin og **downloadPeriodEnd** angiver den periode, hvor eventuel overførsel af data fra køretøjsenheden har fundet sted.

2.47. **CompanyActivityType**

Kode, som angiver en aktivitet udøvet af en virksomhed, som benytter sit virksomhedskort.

```
CompanyActivityType ::= INTEGER {
   card downloading                    (1),
   VU downloading                      (2),
   VU lock-in                          (3),
   VU lock-out                         (4)
}
```

▼B

2.48. **CompanyCardApplicationIdentification**

Oplysninger, gemt på et virksomhedskort, til identifikation af kortets applikation (bilag 1C, krav 369 og 375).

```
CompanyCardApplicationIdentification ::= SEQUENCE {
   typeOfTachographCardId              EquipmentType,
   cardStructureVersion                CardStructureVersion,
   noOfCompanyActivityRecords          NoOfCompanyActivityRecords
}
```

typeOfTachographCardId angiver den implementerede korttype.

cardStructureVersion angiver den version af strukturen, som er implementeret i kortet.

noOfCompanyActivityRecords er det antal virksomhedsaktivitetsposter, som kan lagres på kortet.

2.49. **CompanyCardHolderIdentification**

Oplysninger, gemt på et virksomhedskort, til identifikation af kortindehaveren (bilag 1C, krav 372 og 378)

```
CompanyCardHolderIdentification ::= SEQUENCE {
   companyName                         Name,
   companyAddress                      Address,
   cardHolderPreferredLanguage         Language
}
```

companyName er navnet på den virksomhed, der er indehaver af kortet.

companyAddress er adressen på den virksomhed, der er indehaver af kortet.

cardHolderPreferredLanguage er det af kortindehaveren foretrukne sprog.

2.50. **ControlCardApplicationIdentification**

Oplysninger, gemt på et kontrolkort, til identifikation af kortets applikation (bilag 1C, krav 357 og 363)

```
ControlCardApplicationIdentification ::= SEQUENCE {
   typeOfTachographCardId              EquipmentType,
   cardStructureVersion                CardStructureVersion,
   noOfControlActivityRecords          NoOfControlActivityRecords
}
```

typeOfTachographCardId angiver den implementerede korttype.

cardStructureVersion angiver den version af strukturen, som er implementeret i kortet.

noOfControlActivityRecords er det antal kontrolaktivitetsposter, som kan lagres på kortet.

▼B

2.51. **ControlCardControlActivityData**

Oplysninger, gemt på et kontrolkort, vedrørende de kontrolaktiviteter, der udføres med kortet (bilag 1C, krav 361 og 367).

```
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 er indekset på den senest opdaterede kontrolaktivitetspost.

Tilordnet værdi: Tal svarende til tælleren i kontrolaktivitetsposten, begyndende med '0' for første forekomst af kontrolaktivitetsposten i strukturen.

controlActivityRecords er det fuldstændige sæt kontrolaktivitetsposter.

controlActivityRecord er sekvensen af oplysninger vedrørende én kontrol.

controlType er kontrollens type.

controlTime er dato og klokkeslæt for kontrollen.

controlledCardNumber er kortnummer og kortudstedende medlemsstat for det kort, som kontrolleres.

controlledVehicleRegistration er indregistreringsnummer og registrerende medlemsstat for det køretøj, i hvilket kontrollen fandt sted.

controlDownloadPeriodBegin og **controlDownloadPeriodEnd** angiver den periode, for hvilken data derefter er blevet overført.

2.52. **ControlCardHolderIdentification**

Oplysninger, gemt på et kontrolkort, til identifikation af kortindehaveren (bilag 1C, krav 360 og 366).

```
ControlCardHolderIdentification ::= SEQUENCE {
   controlBodyName                    Name,
   controlBodyAddress                 Address,
   cardHolderName                     HolderName,
   cardHolderPreferredLanguage        Language
}
```

controlBodyName er navnet på kortindehaverens kontrolorgan.

controlBodyAddress er adressen på kortindehaverens kontrolorgan.

cardHolderNameer efternavn og fornavn(e) på kontrolkortets indehaver.

▼B

cardHolderPreferredLanguage er det af kortindehaveren foretrukne sprog.

2.53. **ControlType**

Kode, som angiver de aktiviteter, som udføres under en kontrol. Denne datatype er knyttet til krav 126, 274, 299, 327 og 350 i bilag 1C.

```
ControlType ::= OCTET STRING (SIZE(1))
```

Første generation:

Tilordnet værdi — Oktet udsluttet: 'cvpdxxxx'B (8 bits)

'c'B dataoverførsel for kort:

'0'B: Kortets data blev ikke overført under denne kontrolaktivitet

'1'B: Kortets data blev overført under denne kontrolaktivitet

'v'B dataoverførsel for køretøjsenhed:

'0'B: Køretøjsenhedens data blev ikke overført under denne kontrolaktivitet

'1'B: Køretøjsenhedens data blev overført under denne kontrolaktivitet

'p'B udprintning:

'0'B: Der blev ikke udprintet under denne kontrolaktivitet

'1'B: Der blev udprintet under denne kontrolaktivitet

'd'B visning på skærm:

'0'B: Der blev ikke anvendt visning på skærm under denne kontrolaktivitet

'1'B: Der blev anvendt visning på skærm under denne kontrolaktivitet

'xxxx'B Ikke anvendt.

Anden generation:

Tilordnet værdi — Oktet udsluttet: 'cvpdexxx'B (8 bits)

'c'B dataoverførsel for kort:

'0'B: Kortets data blev ikke overført under denne kontrolaktivitet

'1'B: Kortets data blev overført under denne kontrolaktivitet

'v'B dataoverførsel for køretøjsenhed:

'0'B: Køretøjsenhedens data blev ikke overført under denne kontrolaktivitet

'1'B: Køretøjsenhedens data blev overført under denne kontrolaktivitet

'p'B udprintning:

'0'B: Der blev ikke udprintet under denne kontrolaktivitet

'1'B: Der blev udprintet under denne kontrolaktivitet

▼B

‘d’B	visning på skærm:
	‘0’B: Der blev ikke anvendt visning på skærm under denne kontrolaktivitet
	‘1’B: Der blev anvendt visning på skærm under denne kontrolaktivitet
‘e’B	kalibreringskontrol ved vejsiden:
	‘0’B: kalibreringsparametre blev ikke kontrolleret under denne kontrolaktivitet
	‘1’B: kalibreringsparametre blev kontrolleret under denne kontrolaktivitet
‘xxx’B	RFU

2.54. **CurrentDateTime**

Kontrolapparatets aktuelle klokkeslæt og dato.

```
CurrentDateTime ::= TimeReal
```

Tilordnet værdi: Ikke yderligere angivet.

2.55. **CurrentDateTimeRecordArray**

Anden generation:

Aktuel dato og aktuelt klokkeslæt plus metadata, der anvendes i protokollen for dataoverførsel.

```
CurrentDateTimeRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF CurrentDateTime
}
```

recordType angiver postens type (CurrentDateTime). **Tilordnet værdi**: Se RecordType.

recordSize er størrelsen af CurrentDateTime i bytes.

noOfRecords er antallet af poster i mængden af poster.

records er mængden af aktuelle dato- og klokkeslætsposter.

2.56. **DailyPresenceCounter**

En tæller, som er gemt på et fører- eller værkstedskort, og hvis værdi øges med én for hver kalenderdag, kortet har været indsat i en køretøjsenhed. Denne datatype er knyttet til krav i bilag 1C, krav 266, 299, 320 og 343.

```
DailyPresenceCounter ::= BCDString(SIZE(2))
```

Tilordnet værdi: Fortløbende nummer med maksimumværdi = 9 999, hvorefter der tælles forfra fra 0. Ved første udstedelse af kortet stilles tælleren på nul.

▼B

2.57. **Datef**

Dato, angivet i numerisk, let printbart format.

```
Datef ::= SEQUENCE {
   year        BCDString(SIZE(2)),
   month       BCDString(SIZE(1)),
   day         BCDString(SIZE(1))
}
```

Tilordnet værdi:

yyyy	År
mm	Måned
dd	Dag
‘00000000’H	datoangivelse udtrykkeligt udeladt.

2.58. **DateOfDayDownloaded**

Anden generation:

Dato og klokkeslæt for overførslen.

```
DateOfDayDownloaded ::= TimeReal
```

Tilordnet værdi: Ikke yderligere angivet.

2.59. **DateOfDayDownloadedRecordArray**

Anden generation:

Dato og klokkeslæt for overførslen plus metadata, der anvendes i protokollen for dataoverførsel.

```
DateofDayDownloadedRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF
                                       DateOfDayDownloaded
}
```

recordType angiver postens type (DateOfDayDownloaded). **Tilordnet værdi**: Se RecordType.

recordSize er størrelsen af CurrentDateTime i bytes.

noOfRecords er antallet af poster i mængden af poster.

records er dato og klokkeslæt for overførselsposterne.

2.60. **Afstand**

En tilbagelagt distance (resultat af beregning af forskellen mellem to værdier af køretøjets kilometerstand).

```
Distance ::= INTEGER(0..2^16-1)
```

Tilordnet værdi: Binær uden fortegn. Værdi i km med området 0 til 9 999 km.

2.61. **DriverCardApplicationIdentification**

Oplysninger, gemt på et førerkort, til identifikation af kortets applikation (bilag 1C, krav 253 og 278).

▼B

Første generation:

```
DriverCardApplicationIdentification ::= SEQUENCE {
   typeOfTachographCardId              EquipmentType,
   cardStructureVersion                CardStructureVersion,
   noOfEventsPerType                   NoOfEventsPerType,
   noOfFaultsPerType                   NoOfFaultsPerType,
   activityStructureLength             CardActivityLengthRange,
   noOfCardVehicleRecords              NoOfCardVehicleRecords,
   noOfCardPlaceRecords                NoOfCardPlaceRecords
}
```

typeOfTachographCardId angiver den implementerede korttype.

cardStructureVersion angiver den version af strukturen, som er implementeret i kortet.

noOfEventsPerType er antal hændelser af hver hændelsestype, som kan gemmes på kortet.

noOfFaultsPerType er antal fejl af hver fejltype, som kan gemmes på kortet.

activityStructureLength angiver antal bytes til rådighed til lagring af aktivitetsposter.

noOfCardVehicleRecords er antallet af køretøjsposter, som kan gemmes på kortet.

noOfCardPlaceRecords er antallet af steder, som kan gemmes på kortet.

Anden generation:

```
DriverCardApplicationIdentification ::= SEQUENCE {
   typeOfTachographCardId              EquipmentType,
   cardStructureVersion                CardStructureVersion,
   noOfEventsPerType                   NoOfEventsPerType,
   noOfFaultsPerType                   NoOfFaultsPerType,
   activityStructureLength             CardActivityLengthRange,
   noOfCardVehicleRecords              NoOfCardVehicleRecords,
   noOfCardPlaceRecords                NoOfCardPlaceRecords,
   noOfGNSSCDRecords                   NoOfGNSSCDRecords,
   noOfSpecificConditionRecords        NoOfSpecificConditionRecords
}
```

Ud over dataelementerne for første generation anvendes følgende dataelementer:

noOfGNSSCDRecords er det antal GNSS-poster for sammenhængende køretid, som kan gemmes på kortet.

noOfSpecificConditionRecords er det antal poster vedrørende særlige omstændigheder, som kan gemmes på kortet.

2.62. **DriverCardHolderIdentification**

Oplysninger, gemt på et førerkort, til identifikation af kortindehaveren (bilag 1C, krav 256 og 281).

```
DriverCardHolderIdentification ::= SEQUENCE {
   cardHolderName                      HolderName,
   cardHolderBirthDate                 Datef,
   cardHolderPreferredLanguage         Language
}
```

▼B

cardHolderNameer efternavn og fornavn(e) på førerkortets indehaver.

cardHolderBirthDateer fødselsdato for førerkortets indehaver.

cardHolderPreferredLanguage er det af kortindehaveren foretrukne sprog.

2.63. **DSRCSecurityData**

Anden generation:

De oplysninger i form af almindelig tekst og det MAC-element, der skal overføres via DSRC fra takografen til fjernaflæseren. Nærmere oplysninger fremgår af tillæg 11, del B, afsnit 13.

```
DSRCSecurityData ::= SEQUENCE {
   tagLenthPlainText                    OCTET STRING(SIZE(2)),
   currentDateTime                      CurrentDateTime,
   counter                              INTEGER(0..2^24-1),
   vuSerialNumber                       VuSerialNumber,
   dSRCMKVersionNumber                  INTEGER(SIZE(1)),
   tagLengthMac                         OCTET STRING(SIZE(2)),
   mac                                  MAC
}
```

tagLength er en del af DER-TLV-kodningen og skal være sat til '81 10' (se tillæg 11, del B, afsnit 13).

currentDateTime er den aktuelle dato og det aktuelle klokkeslæt fra køretøjsenheden.

counter optæller antallet af RTM-meddelelser.

vuSerialNumber er serienummeret på køretøjsenheden.

dSRCMKVersionNumber er versionsnummeret på den DSRC-hovednøgle, hvorfra de køretøjsenhedsspecifikke DSRC-nøgler er udledt.

tagLengthMac er etiketten for og længden på MAC-dataobjektet i forbindelse med DER-TLV-kodningen. Etiketten skal sættes til '8E', og længden skal kode længden af MAC-elementet i oktetter (se tillæg 11, del B, afsnit 13).

mac er det MAC-element, der er beregnet over RTM-meddelelsen (se tillæg 11, del B, afsnit 13).

2.64. **EGFCertificate**

Anden generation:

Certifikat for det eksterne GNSS-udstyrs offentlige nøgle til gensidig ægthedsbekræftelse med en køretøjsenhed. Dette certifikats opbygning er nærmere beskrevet i tillæg 11.

```
EGFCertificate ::= Certificate
```

▼B

2.65. **EmbedderIcAssemblerId**

Rummer oplysninger om IC embedder.

```
EmbedderIcAssemblerId ::= SEQUENCE{
   countryCode                          IA5String(SIZE(2)),
   moduleEmbedder                       BCDString(SIZE(2)),
   manufacturerInformation              OCTET STRING(SIZE(1))
}
```

countryCode er landekoden på to bogstaver for den såkaldte "module embedder" i overensstemmelse med ISO 3166.

moduleEmbedder identificerer den såkaldte "module embedder".

manufacturerInformation er til fabrikantens interne brug.

2.66. **EntryTypeDailyWorkPeriod**

Kode, der benyttes til at skelne mellem start og slut på det indlæste sted for den daglige arbejdstid og omstændigheden ved indlæsning.

Første generation:

```
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)
}
```

Tilordnet værdi: I henhold til ISO/IEC 8824-1

Anden generation:

```
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)
}
```

Tilordnet værdi: I henhold til ISO/IEC 8824-1

2.67. **EquipmentType**

Kode, som benyttes til at skelne mellem forskellige typer udstyr til takografapplikationen.

```
EquipmentType ::= INTEGER(0..255)
```

▼B

Første generation:

```
--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)
```

Tilordnet værdi: I henhold til ISO/IEC 8824-1.

Værdien 0 er reserveret til at angive en medlemsstat eller EU i CHA-feltet i certifikaterne.

Anden generation:

De samme værdier som for første generation anvendes med følgende tilføjelser:

```
--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)
```

Bemærk: Værdierne for anden generation for pladen, adapteren og den eksterne GNSS-forbindelse samt værdierne for første generation af køretøjsenheden og bevægelsessensoren kan anvendes i SealRecord, hvis det er relevant.

2.68. **EuropeanPublicKey**

Første generation:

Den europæiske offentlige nøgle.

```
EuropeanPublicKey ::= PublicKey
```

2.69. **EventFaultRecordPurpose**

Kode, som forklarer, hvorfor en hændelse eller en fejl er blevet registreret.

```
EventFaultRecordPurpose ::= OCTET STRING (SIZE(1))
```

Tilordnet værdi:

'00'H	en af de 10 seneste hændelser eller fejl
'01'H	den længstvarende hændelse for en af de 10 seneste dage, den er forekommet
'02'H	en af de 5 længstvarende hændelser inden for de sidste 365 dage
'03'H	den seneste hændelse for en af de 10 seneste dage, den er forekommet
'04'H	den alvorligste hændelse for en af de 10 seneste dage, den er forekommet
'05'H	en af de 5 alvorligste hændelser inden for de sidste 365 dage
'06'H	den første hændelse eller fejl, som er forekommet efter sidste kalibrering
'07'H	en aktiv/igangværende hændelse eller fejl
'08'H to '7F'H	RFU
'80'H to 'FF'H	Fabrikantspecifik

▼B

2.70. **EventFaultType**

Kode, som bestemmer en hændelse eller en fejl.

```
EventFaultType ::= OCTET STRING (SIZE(1))
```

Tilordnet værdi:

Første generation:

'0x'H	Generelle hændelser
'00'H	Ingen yderligere detaljer
'01'H	Isætning af ugyldigt kort
'02'H	Kortkonflikt
'03'H	Tidsoverlapning
'04'H	Kørsel uden behørigt kort
'05'H	Isætning af kort under kørslen
'06'H	Seneste kortsession ikke korrekt afsluttet
'07'H	Overskridelse af tilladt hastighed
'08'H	Afbrydelse i strømforsyningen
'09'H	Fejl ved køredata
'0A'H	Køretøjsbevægelseskonflikt
'0B' to '0F'H	RFU

'1x'H	Hændelser, som er knyttet til køretøjsenheden og består i forsøg på sikkerhedsbrud
'10'H	Ingen yderligere detaljer
'11'H	Ægthedsbekræftelse for bevægelsessensor lykkedes ikke
'12'H	Ægthedsbekræftelse for takografkort lykkedes ikke
'13'H	Ubeføjet ændring af bevægelsessensor
'14'H	Integritetsfejl på indlæste kortdata
'15'H	Integritetsfejl på lagrede brugerdata
'16'H	Fejl ved intern dataoverførsel
'17'H	Ubehørig åbning af hus
'18'H	Hardware-sabotage
'19'H to '1F'H	RFU

'2x'H	Hændelser, som knyttet til føleren og består i forsøg på sikkerhedsbrud
'20'H	Ingen yderligere detaljer
'21'H	Ægthedskontrol lykkedes ikke
'22'H	Integritetsfejl på lagrede data
'23'H	Fejl ved intern dataoverførsel
'24'H	Ubehørig åbning af hus
'25'H	Hardware-sabotage
'26'H to '2F'H	RFU

'3x'H	Fejl ved kontrolapparat
'30'H	Ingen yderligere detaljer
'31'H	Intern fejl i køretøjsenhed
'32'H	Printerfejl
'33'H	Displayfejl
'34'H	Dataoverførselsfejl
'35'H	Følerfejl
'36'H to '3F'H	RFU

'4x'H	Kortfejl
'40'H	Ingen yderligere detaljer
'41'H to '4F'H	RFU

'50'H to '7F'H	RFU

'80'H to 'FF'H	Fabrikantspecifik.

▼B

Anden generation:

De samme værdier som for første generation anvendes med følgende tilføjelser:

‘0B’H	Tidskonflikt (GNSS kontra køretøjsenhedens interne ur)
‘0C’ to ‘0F’H	RFU
‘5x’H	GNSS-relaterede fejl
‘50’H	Ingen yderligere detaljer
‘51’H	Fejl ved intern GNSS-modtager
‘52’H	Fejl ved ekstern GNSS-modtager
‘53’H	Fejl ved ekstern GNSS-kommunikation
‘54’H	Ingen GNSS-placeringsdata
‘55’H	Registrering af manipulation af GNSS
‘56’H	Certifikat for eksternt GNSS-udstyr udløbet
‘57’H to ‘5F’H	RFU
‘6x’H	Fejl vedrørende modul til fjernkommunikation
‘60’H	Ingen yderligere detaljer
‘61’H	Fejl ved modul til fjernkommunikation
‘62’H	Fejl ved kommunikation med modul til fjernkommunikation
‘63’H to ‘6F’H	RFU
‘7x’H	Fejl ved ITS-grænseflade
‘70’H	Ingen yderligere detaljer
‘71’H to ‘7F’H	RFU

2.71. **ExtendedSealIdentifier**

Anden generation:

Det udvidede datanavn for en plombe identificerer entydigt plomben (bilag 1C, krav 401).

```
ExtendedSealIdentifier ::= SEQUENCE{
   manufacturerCode                    OCTET STRING (SIZE(2)),
   sealIdentifier                      OCTET STRING (SIZE(6))
}
```

manufacturerCode er en kode for fabrikanten af plomben.

sealIdentifier er et datanavn for plomben, som er unikt for fabrikanten.

2.72. **ExtendedSerialNumber**

Entydig identifikation af et stykke udstyr. Kan desuden bruge som datanavn for en offentlig nøgle for udstyr.

Første generation:

```
ExtendedSerialNumber ::= SEQUENCE{
   serialNumber                        INTEGER(0..2^32-1),
   monthYear                           BCDString(SIZE(2)),
   type                                OCTET STRING(SIZE(1)),
   manufacturerCode                    ManufacturerCode
}
```

serialNumber er udstyrets serienummer. Det er entydigt for udstyret, fabrikanten, udstyrets type og måneden og året nedenfor.

monthYear er identifikationen af fabrikationsmåned og -år (eller af tildelingen af serienummer).

▼B

Tilordnet værdi: Binært kodet decimaltal for måned (to cifre) og år (to sidste cifre).

type er et datanavn for udstyrets type.

Tilordnet værdi: Fabrikantspecifik, med 'FFh'-reserveret værdi.

manufacturerCode er den numeriske kode, som identificerer en fabrikant af typegodkendt udstyr.

Anden generation:

```
ExtendedSerialNumber ::= SEQUENCE{
   serialNumber                          INTEGER(0..2^32-1),
   monthYear                             BCDString(SIZE(2)),
   type                                  EquipmentType,
   manufacturerCode                      ManufacturerCode
}
```

serialNumber: Se første generation

monthYear: Se første generation

type angiver udstyrets type

manufacturerCode: Se første generation

2.73. **FullCardNumber**

Kode, som fuldstændig identificerer et takografkort.

```
FullCardNumber ::= SEQUENCE {
   cardType                              EquipmentType,
   cardIssuingMemberState                NationNumeric,
   cardNumber                            CardNumber
}
```

cardType er takografkortets type.

cardIssuingMemberState er koden på den medlemsstat, der har udstedt kortet.

cardNumber er kortnummeret.

2.74. **FullCardNumberAndGeneration**

Anden generation:

Kode, som fuldstændig identificerer et takografkort og dets generation.

```
FullCardNumberAndGeneration ::= SEQUENCE {
   fullCardNumber                        FullCardNumber,
   generation                            Generation
}
```

fullcardNumber identificerer takografkortet.

generation angiver det anvendte takografkorts generation.

▼B

2.75. **Generation**

Anden generation:

Angiver det anvendte takografkorts generation.

```
Generation ::= INTEGER(0..255)
```

Tilordnet værdi:

'00'H	RFU
'01'H	Første generation
'02'H	Anden generation
'03'H .. 'FF'H	RFU

2.76. **GeoCoordinates**

Anden generation:

Geo-koordinaterne kodes som heltal. Disse heltal er multipla af kodningen ± DDMM.M for breddegrad og ± DDDMM.M for længdegrad. Her angiver henholdsvis ± DD og ± DDD graderne, mens MM.M angiver minutterne.

```
GeoCoordinates ::= SEQUENCE {
   latitude                                INTEGER(-90000..90001),
   longitude                               INTEGER(-180000..180001)
}
```

latitude kodes som et multiplum (faktor 10) af gengivelsen af ± DDMM.M.

longitude kodes som et multiplum (faktor 10) af gengivelsen af ± DDDMM.M.

2.77. **GNSSAccuracy**

Anden generation:

GNSS-placeringsdataenes nøjagtighed (definition eee)). Denne nøjagtighed kodes som heltal og er et multiplum (faktor 10) af værdien X.Y i GSA NMEA-sætningen.

```
GNSSAccuracy ::= INTEGER(1..100)
```

2.78. **GNSSContinuousDriving**

Anden generation:

Oplysninger, gemt på et fører- eller værkstedskort, vedrørende køretøjets GNSS-position, hvis førerens sammenhængende køretid når op på et multiplum af tre timer (bilag 1C, krav 306 og 354).

```
GNSSContinuousDriving := SEQUENCE {
   gnssCDPointerNewestRecord               INTEGER(0..NoOfGNSSCDRecords -1),
   gnssContinuousDrivingRecords            SET SIZE(NoOfGNSSCDRecords) OF
                                           GNSSContinuousDrivingRecord
}
```

gnssCDPointerNewestRecord er indekset på den senest opdaterede GNSS-post for sammenhængende køretid.

▼B

Tilordnet værdi: Tal svarende til tælleren i GNSS-posten for sammenhængende køretid, begyndende med '0' for den første forekomst af GNSS-posten for sammenhængende køretid i strukturen.

gnssContinuousDrivingRecords er mængden af poster, der indeholder dato og klokkeslæt, hvor den sammenhængende køretid når op på et multiplum af tre timer, og oplysninger om køretøjets position.

2.79. **GNSSContinuousDrivingRecord**

Anden generation:

Oplysninger, gemt på et fører- eller værkstedskort, vedrørende køretøjets GNSS-position, hvis førerens sammenhængende køretid når op på et multiplum af tre timer (bilag 1C, krav 305 og 353).

```
GNSSContinuousDrivingRecord ::= SEQUENCE {
   timeStamp                                TimeReal,
   gnssPlaceRecord                          GNSSPlaceRecord
}
```

timeStamp er den dato og det klokkeslæt, hvor kortindehaverens sammenhængende køretid når op på et multiplum af tre timer.

gnssPlaceRecord indeholder oplysninger om køretøjets position.

2.80. **GNSSPlaceRecord**

Anden generation:

Oplysninger om køretøjets GNSS-position (bilag 1C, krav 108, 109, 110, 296, 305, 347 og 353).

```
GNSSPlaceRecord ::= SEQUENCE {
   timeStamp                                TimeReal,
   gnssAccuracy                             GNSSAccuracy,
   geoCoordinates                           GeoCoordinates
}
```

timeStamp er dato og klokkeslæt for registrering af GNSS-positionen.

gnssAccuracy er GNSS-placeringsdataenes nøjagtighed.

geoCoordinates er den position, der er registreret ved brug af GNSS.

2.81. **HighResOdometer**

Køretøjets kilometerstand: Samlet distance tilbagelagt af køretøjet i dettes driftstid.

```
HighResOdometer ::= INTEGER(0..2^32-1)
```

▼B

Tilordnet værdi: Binær uden fortegn. Talværdi i 1/200 km inden for området 0 til 21 055 406 km.

2.82. **HighResTripDistance**

En distance, som er tilbagelagt i løbet af en hel tur eller en del heraf.

```
HighResTripDistance ::= INTEGER(0..2^32-1)
```

Tilordnet værdi: Binær uden fortegn. Talværdi i 1/200 km inden for området 0 til 21 055 406 km.

2.83. **HolderName**

En kortindehavers efternavn og fornavn(e).

```
HolderName ::= SEQUENCE {
   holderSurname                    Name,
   holderFirstNames                 Name
}
```

holderSurname er indehaverens efternavn. Titler indgår ikke i efternavnet.

Tilordnet værdi: Når et kort ikke er personligt, indeholder holderSurname samme oplysninger som et companyName eller workshopName eller controlBodyName.

holderFirstNames er indehaverens fornavn(e) og initialer.

2.84. **InternalGNSSReceiver**

Anden generation:

Information om, hvorvidt GNSS-modtageren er intern eller ekstern i forhold til køretøjsenheden. Sandt betyder, at GNSS-modtageren er intern. Falsk betyder, at GNSS-modtageren er ekstern.

```
InternalGNSSReceiver ::= BOOLEAN
```

2.85. **K-ConstantOfRecordingEquipment**

Kontrolapparatets konstant (definition m)).

```
K-ConstantOfRecordingEquipment ::= INTEGER(0..2^16-1)
```

Tilordnet værdi: Impulser pr. kilometer inden for området 0 til 64 255 impulser/km.

2.86. **KeyIdentifier**

Et entydigt datanavn for en offentlig nøgle. Benyttes til at henvise til og vælge nøgle. Den identificerer desuden indehaveren af nøglen.

```
KeyIdentifier ::= CHOICE {
   extendedSerialNumber             ExtendedSerialNumber,
   certificateRequestID             CertificateRequestID,
   certificationAuthorityKID        CertificationAuthorityKID
}
```

▼B

Det første valg er egnet til henvisning til den offentlige nøgle for et køretøj eller for et takografkort.

Det andet valg er egnet til henvisning til den offentlige nøgle for en køretøjsenhed (når køretøjets serienummer ikke kan oplyses på tidspunktet for udfærdigelse af certifikatet).

Det tredje valg er egnet til henvisning til den offentlige nøgle for en medlemsstat.

2.87. **KMWCKey**

Anden generation:

AES-nøglen og den tilhørende version, som anvendes til parring af køretøjsenhed og bevægelsessensor. Nærmere oplysninger findes i tillæg 11.

```
KMWCKey ::= SEQUENCE {
   kMWCKey                                 AESKey,
   keyVersion                              INTEGER (SIZE(1))
}
```

kMWCKey er længden af AES-nøglen sammenkædet med den nøgle, der bruges til parring af køretøjsenhed og bevægelsessensor.

keyVersion keyVersion er AES-nøglens version.

2.88. **Language**

Kode, som identificerer et sprog.

```
Language ::= IA5String(SIZE(2))
```

Tilordnet værdi: En kode bestående af to minuskler i overensstemmelse med ISO 639.

2.89. **LastCardDownload**

Dato og klokkeslæt, gemt på førerkortet, for seneste dataoverførsel af kort (til andre formål end kontrol) (bilag 1C, krav 257 og 282). Denne dato kan ajourføres af en køretøjsenhed eller enhver kortlæser.

```
LastCardDownload ::= TimeReal
```

Tilordnet værdi: Ikke yderligere angivet.

2.90. **LinkCertificate**

Anden generation:

Linkcertifikatet mellem nøglepar i europæiske rodnøglecentre.

```
LinkCertificate ::= Certificate
```

2.91. **L-TyreCircumference**

Effektiv dækperiferi (definition u)).

```
L-TyreCircumference ::= INTEGER(0.. 2^16-1)
```

▼B

Tilordnet værdi: Binær uden fortegn, værdi i 1/8 mm inden for området 0 til 8 031 mm.

2.92. **MAC**

Anden generation:

En kryptografisk kontrolsum af 8, 12 eller 16 bytes længde svarende til de krypteringsprogrammer, der er angivet i tillæg 11.

```
MAC ::= CHOICE {
   mac8                                    OCTET STRING (SIZE(8)),
   mac12                                   OCTET STRING (SIZE(12)),
   mac16                                   OCTET STRING (SIZE(12))
}
```

2.93. **ManualInputFlag**

Kode, som fastslår, om en kortindehaver manuelt har eller ikke har indlæst føreraktiviteter ved isætning af kort (bilag 1B, krav 081, og bilag 1C, krav 102).

```
ManualInputFlag ::= INTEGER {
   noEntry                                 (0)
   manualEntries                           (1)
}
```

Tilordnet værdi: Ikke yderligere angivet.

2.94. **ManufacturerCode**

Kode, som identificerer en fabrikant af typegodkendt udstyr.

```
ManufacturerCode ::= INTEGER(0..255)
```

Det laboratorium, der forestår interoperabilitetsprøverne, fører og offentliggør listen over fabrikantkoder på sit websted (bilag 1C, krav 454).

Der tildeles midlertidigt ManufacturerCode til udviklere af takografudstyr efter ansøgning til det laboratorium, der forestår interoperabilitetsprøverne.

2.95. **ManufacturerSpecificEventFaultData**

Anden generation:

Fabrikantspecifikke fejlkoder, som sikrer enklere fejlanalyse og vedligeholdelse af køretøjsenheder.

```
ManufacturerSpecificEventFaultData ::= SEQUENCE {
   manufacturerCode                        ManufacturerCode,
   manufacturerSpecificErrorCode           OCTET STRING(SIZE(3))
}
```

manufacturerCode identificerer fabrikanten af køretøjsenheden.

manufacturerSpecificErrorCode er en fejlkode, der gælder specifikt for fabrikanten.

▼B

2.96. **MemberStateCertificate**

Certifikat for en medlemsstats offentlige nøgle, udstedt af den europæiske certificeringsmyndighed.

```
MemberStateCertificate ::= Certificate
```

2.97. **MemberStateCertificateRecordArray**

Anden generation:

Medlemsstatens certifikat plus metadata, der anvendes i protokollen for dataoverførsel.

```
MemberStateCertificateRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF
                                       MemberStateCertificate
}
```

recordType angiver postens type (MemberStateCertificate). **Tilordnet værdi**: Se RecordType.

recordSize er størrelsen af MemberStateCertificate i bytes.

noOfRecords er antallet af poster i mængden af poster. Værdien skal sættes til 1, da certifikaterne kan have forskellig længde.

records er mængden af medlemsstaters certifikater.

2.98. **MemberStatePublicKey**

Første generation:

En medlemsstats offentlige nøgle.

```
MemberStatePublicKey ::= PublicKey
```

2.99. **Name**

Et navn.

```
Name ::= SEQUENCE {
   codePage                            INTEGER (0..255),
   name                                OCTET STRING (SIZE(35))
}
```

codePage angiver et tegnsæt, der er defineret i afsnit 4.

name er et navn, som er indkodet med det angivne tegnsæt.

2.100. **NationAlpha**

Den alfabetiske henvisning til et land skal være i overensstemmelse med de nationalitetsbetegnelser, der anvendes på køretøjer i international færdsel (FN-Wienerkonventionen om vejtrafik af 1968).

```
NationAlpha ::= IA5String(SIZE(3))
```

NationAlpha- og NationNumeric-koderne skal være opført på en liste på webstedet for det laboratorium, som er udpeget til at udføre interoperabilitetsprøverne, jf. bilag 1C, krav 440.

▼B

2.101. **NationNumeric**

Numerisk henvisning til et land.

```
NationNumeric ::= INTEGER(0 .. 255)
```

Tilordnet værdi: se datatype 2.100 (NationAlpha).

Enhver ændring eller opdatering af den NationAlpha- eller NationNumeric -specifikation, der er beskrevet i ovennævnte afsnit, foretages først, efter at det udpegede laboratorium har indhentet udtalelser fra fabrikanter af typegodkendte køretøjsenheder til digitale takografer og intelligente takografer.

2.102. **NoOfCalibrationRecords**

Antal kalibreringsposter, som kan gemmes på et værkstedskort.

Første generation:

```
NoOfCalibrationRecords ::= INTEGER(0..255)
```

Tilordnet værdi: se tillæg 2.

Anden generation:

```
NoOfCalibrationRecords ::= INTEGER(0..2^16-1)
```

Tilordnet værdi: se tillæg 2.

2.103. **NoOfCalibrationsSinceDownload**

Tæller, som angiver det samlede antal kalibreringer, der er udført med et værkstedskort siden sidste dataoverførsel for kortet (bilag 1C, krav 317 og 340).

```
NoOfCalibrationsSinceDownload ::= INTEGER(0..2^16-1)
```

Tilordnet værdi: Ikke yderligere angivet.

2.104. **NoOfCardPlaceRecords**

Antal stedposter, som kan gemmes på et fører- eller værkstedskort.

Første generation:

```
NoOfCardPlaceRecords ::= INTEGER(0..255)
```

Tilordnet værdi: se tillæg 2.

Anden generation:

```
NoOfCardPlaceRecords ::= INTEGER(0..2^16-1)
```

Tilordnet værdi: se tillæg 2.

▼B

2.105. **NoOfCardVehicleRecords**

Antal anvendte køretøjer, som kan gemmes på et fører- eller værkstedskort.

```
NoOfCardVehicleRecords ::= INTEGER(0.. 2^16-1)
```

Tilordnet værdi: se tillæg 2.

2.106. **NoOfCardVehicleUnitRecords**

Anden generation:

Antal anvendte køretøjsenheder, som kan gemmes på et fører- eller værkstedskort.

```
NoOfCardVehicleUnitRecords ::= INTEGER(0.. 2^16-1)
```

Tilordnet værdi: se tillæg 2.

2.107. **NoOfCompanyActivityRecords**

Antal virksomhedsaktivitetsposter, som kan gemmes på et virksomhedskort.

```
NoOfCompanyActivityRecords ::= INTEGER(0.. 2^16-1)
```

Tilordnet værdi: se tillæg 2.

2.108. **NoOfControlActivityRecords**

Antal kontrolaktivitetsposter, som kan gemmes på et kontrolkort.

```
NoOfControlActivityRecords ::= INTEGER(0.. 2^16-1)
```

Tilordnet værdi: se tillæg 2.

2.109. **NoOfEventsPerType**

Antal hændelser af hver hændelsestype, som kan gemmes på et kort.

```
NoOfEventsPerType ::= INTEGER(0..255)
```

Tilordnet værdi: se tillæg 2.

2.110. **NoOfFaultsPerType**

Antal fejl af hver fejltype, som kan gemmes på et kort.

```
NoOfFaultsPerType ::= INTEGER(0..255)
```

Tilordnet værdi: se tillæg 2.

▼B

2.111. **NoOfGNSSCDRecords**

Anden generation:

Antal GNSS-poster for sammenhængende køretid, som kan gemmes på et kort.

```
NoOfGNSSCDRecords ::= INTEGER(0..2^16-1)
```

Tilordnet værdi: se tillæg 2.

2.112. **NoOfSpecificConditionRecords**

Anden generation:

Antal poster vedrørende særlige omstændigheder, som kan gemmes på et kort.

```
NoOfSpecificConditionRecords ::= INTEGER(0..2^16-1)
```

Tilordnet værdi: se tillæg 2.

2.113. **OdometerShort**

Køretøjets kilometerstand i kortform.

```
OdometerShort ::= INTEGER(0..2^24-1)
```

Tilordnet værdi: Binær uden fortegn. Værdi i km inden for området 0 til 9 999 999 km.

2.114. **OdometerValueMidnight**

Køretøjets kilometerstand ved midnat i et givet døgn (bilag 1B, krav 090, og bilag 1C, krav 113).

```
OdometerValueMidnight ::= OdometerShort
```

Tilordnet værdi: Ikke yderligere angivet.

2.115. **OdometerValueMidnightRecordArray**

Anden generation:

OdometerValueMidnight plus metadata, der anvendes i protokollen for dataoverførsel.

```
OdometerValueMidnightRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF
                                       OdometerValueMidnight
}
```

recordType angiver postens type (OdometerValueMidnight). **Tilordnet værdi**: Se RecordType.

recordSize er størrelsen af OdometerValueMidnight i bytes.

noOfRecords er antallet af poster i mængden af poster.

records er mængden af OdometerValueMidnight-poster.

▼B

2.116. **OverspeedNumber**

Antal hændelser med overskridelse af tilladt hastighed siden seneste kontrol for overskridelse af tilladt hastighed.

```
OverspeedNumber ::= INTEGER(0..255)
```

Tilordnet værdi: 0 betyder, at der ikke er forekommet hændelser med overskridelse af tilladt hastighed siden seneste kontrol for overskridelse af tilladt hastighed, 1 betyder, at der har været én hændelse med overskridelse af tilladt hastighed siden seneste kontrol for overskridelse af tilladt hastighed, … 255 betyder, at der har været 255 eller flere hændelser med overskridelse af tilladt hastighed siden seneste kontrol for overskridelse af tilladt hastighed.

2.117. **PlaceRecord**

Oplysninger vedrørende et sted, hvor en daglig arbejdsperiode begynder eller slutter (bilag 1C, krav 108, 271, 296, 324 og 347).

Første generation:

```
PlaceRecord ::= SEQUENCE {
   entryTime                              TimeReal,
   entryTypeDailyWorkPeriod               EntryTypeDailyWorkPeriod,
   dailyWorkPeriodCountry                 NationNumeric,
   dailyWorkPeriodRegion                  RegionNumeric,
   vehicleOdometerValue                   OdometerShort
}
```

entryTime er en dato og et klokkeslæt knyttet til indlæsningen.

entryTypeDailyWorkPeriod er indlæsningens type.

dailyWorkPeriodCountry er det indlæste land.

dailyWorkPeriodRegion er den indlæste region.

vehicleOdometerValue er kilometerstanden på tidspunktet for indlæsning af stedet.

Anden generation:

```
PlaceRecord ::= SEQUENCE {
   entryTime                              TimeReal,
   entryTypeDailyWorkPeriod               EntryTypeDailyWorkPeriod,
   dailyWorkPeriodCountry                 NationNumeric,
   dailyWorkPeriodRegion                  RegionNumeric,
   vehicleOdometerValue                   OdometerShort,
   entryGNSSPlaceRecord                   GNSSPlaceRecord
}
```

Ud over parametrene for første generation anvendes følgende parameter:

entryGNSSPlaceRecord er det registrerede sted og tidspunkt.

▼B

2.118. **PreviousVehicleInfo**

Oplysninger vedrørende det foregående køretøj, som føreren anvendte, da han satte sit kort i en køretøjsenhed (bilag 1B, krav 081, og bilag 1C, krav 102).

Første generation:

```
PreviousVehicleInfo ::= SEQUENCE {
   vehicleRegistrationIdentification      VehicleRegistrationIdentification,
   cardWithdrawalTime                     TimeReal
}
```

vehicleRegistrationIdentification er indregistreringsnummer og registrerende medlemsstat for køretøjet.

cardWithdrawalTime er dato og klokkeslæt for udtagning af kortet.

Anden generation:

```
PreviousVehicleInfo ::= SEQUENCE {
   vehicleRegistrationIdentification      VehicleRegistrationIdentification,
   cardWithdrawalTime                     TimeReal,
   vuGeneration                           Generation
}
```

Ud over dataelementerne for første generation anvendes følgende dataelement:

vuGeneration angiver køretøjsenhedens generation.

2.119. **PublicKey**

Første generation:

En offentlig RSA-nøgle.

```
PublicKey ::= SEQUENCE {
   rsaKeyModulus                          RSAKeyModulus,
   rsaKeyPublicExponent                   RSAKeyPublicExponent
}
```

rsaKeyModulus er nøgleparrets modulus.

rsaKeyPublicExponent er nøgleparrets offentlige eksponent.

2.120. **RecordType**

Anden generation:

Henvisning til en posttype. Denne datatype bruges i RecordArrays.

```
RecordType ::= OCTET STRING(SIZE(1))
```

▼B

Tilordnet værdi:

'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	Fabrikantspecifik.

2.121. **RegionAlpha**

Alfabetisk henvisning til en region i en given stat.

```
RegionAlpha ::= IA5STRING(SIZE(3))
```

Første generation:

Tilordnet værdi:

' '	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

Anden generation:

RegionAlpha-koderne skal være opført på en liste på webstedet for det laboratorium, som er udpeget til at udføre interoperabilitetsprøverne.

2.122. **RegionNumeric**

Numerisk henvisning til en region i en given stat.

```
RegionNumeric ::= OCTET STRING (SIZE(1))
```

Første generation:

Tilordnet værdi:

```
'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
```

Anden generation:

RegionNumeric-koderne skal være opført på en liste på webstedet for det laboratorium, som er udpeget til at udføre interoperabilitetsprøverne.

2.123. **RemoteCommunicationModuleSerialNumber**

Anden generation:

Serienummeret på modulet til fjernkommunikation

```
RemoteCommunicationModuleSerialNumber ::= ExtendedSerialNumber
```

2.124. **RSAKeyModulus**

Første generation:

Modulus for et RSA-nøglepar.

```
RSAKeyModulus ::= OCTET STRING (SIZE(128))
```

Tilordnet værdi: Uspecificeret.

2.125. **RSAKeyPrivateExponent**

Første generation:

Den private eksponent for et RSA-nøglepar.

```
RSAKeyPrivateExponent ::= OCTET STRING (SIZE(128))
```

Tilordnet værdi: Uspecificeret.

▼B

2.126. **RSAKeyPublicExponent**

Første generation:

Den offentlige eksponent for et RSA-nøglepar.

```
RSAKeyPublicExponent ::= OCTET STRING (SIZE(8))
```

Tilordnet værdi: Uspecificeret.

2.127. **RtmData**

Anden generation:

En definition af denne datatype findes i tillæg 14.

2.128. **SealDataCard**

Anden generation:

Denne datatype, som lagrer oplysninger om de plomber, der er fastgjort til de forskellige komponenter i et køretøj, er beregnet til lagring på et kort. Denne datatype er knyttet til bilag 1C, krav 337.

```
SealDataCard ::= SEQUENCE {
   noOfSealRecords                    INTEGER(1..5),
   sealRecords                        SET SIZE(noOfSealRecords) OF SealRecord
}
```

noOfSealRecords er antallet af poster i SealRecords.

sealRecords er mængden af plombeposter.

2.129. **SealDataVu**

Anden generation:

Denne datatype, som lagrer oplysninger om de plomber, der er fastgjort til de forskellige komponenter i et køretøj, er beregnet til lagring i en køretøjsenhed.

```
SealDataVu ::= SEQUENCE SIZE(5) OF {
   sealRecords                        SealRecord
}
```

sealRecords er mængden af plombeposter. Hvis der er mindre end fem plomber til rådighed, skal værdien af EquipmentType i alle ikke-anvendte sealRecords sættes til 16, dvs. ikke anvendt.

2.130. **SealRecord**

Anden generation:

Denne datatype lagrer oplysninger om en plombe, der er fastgjort til en komponent. Denne datatype er knyttet til bilag 1C, krav 337.

```
SealRecord ::= SEQUENCE {
   equipmentType                      EquipmentType,
   extendedSealIdentifier             ExtendedSealIdentifier
}
```

equipmentType angiver den udstyrstype, som plomben er fastgjort til.

extendedSealIdentifier er datanavnet på den plombe, der er fastgjort til udstyret.

▼B

2.131. **SensorApprovalNumber**

Følerens typegodkendelsesnummer.

Første generation:

```
SensorApprovalNumber ::= IA5String(SIZE(8))
```

Tilordnet værdi: Uspecificeret.

Anden generation:

```
SensorApprovalNumber ::= IA5String(SIZE(16))
```

Tilordnet værdi:

Godkendelsesnummeret skal tilvejebringes som offentliggjort på Europa-Kommissionens relevante websted, dvs. f.eks. med eventuelle bindestreger. Godkendelsesnummeret skal være venstrejusteret.

2.132. **SensorExternalGNSSApprovalNumber**

Anden generation:

Typegodkendelsesnummeret på det eksterne GNSS-udstyr.

```
SensorExternalGNSSApprovalNumber ::= IA5String(SIZE(16))
```

Tilordnet værdi:

Godkendelsesnummeret skal tilvejebringes som offentliggjort på Europa-Kommissionens relevante websted, dvs. f.eks. med eventuelle bindestreger. Godkendelsesnummeret skal være venstrejusteret.

2.133. **SensorExternalGNSSCoupledRecord**

Anden generation:

Oplysninger, gemt på en køretøjsenhed, til identifikation af det eksterne GNSS-udstyr, som er koblet sammen med køretøjsenheden (bilag 1C, krav 100).

```
SensorExternalGNSSCoupledRecord ::= SEQUENCE {
   sensorSerialNumber                  SensorGNSSSerialNumber,
   sensorApprovalNumber                SensorExternalGNSSApprovalNumber,
   sensorCouplingDate                  SensorGNSSCouplingDate
}
```

sensorSerialNumber er serienummeret på det eksterne GNSS-udstyr, som er koblet sammen med køretøjsenheden.

sensorApprovalNumber er godkendelsesnummeret på det pågældende eksterne GNSS-udstyr.

sensorCouplingDate er datoen for det pågældende eksterne GNSS-udstyrs kobling med køretøjsenheden.

2.134. **SensorExternalGNSSIdentification**

Anden generation:

Oplysninger til identifikation af det eksterne GNSS-udstyr (bilag 1C, krav 98).

▼B

```
SensorExternalGNSSIdentification ::= SEQUENCE {
   sensorSerialNumber                    SensorGNSSSerialNumber,
   sensorApprovalNumber                  SensorExternalGNSSApprovalNumber,
   sensorSCIdentifier                    SensorExternalGNSSSCIdentifier,
   sensorOSIdentifier                    SensorExternalGNSSOSIdentifier
}
```

sensorSerialNumber er det udvidede serienummer på det eksterne GNSS-udstyr.

sensorApprovalNumber er godkendelsesnummeret på det eksterne GNSS-udstyr.

sensorSCIdentifier er datanavnet på det eksterne GNSS-udstyrs sikkerhedskomponent.

sensorOSIdentifier er datanavnet på det eksterne GNSS-udstyrs operativsystem.

2.135. **SensorExternalGNSSInstallation**

Anden generation:

Oplysninger, der er lagret i eksternt GNSS-udstyr, om montering af det eksterne GNSS-udstyrs føler (bilag 1C, krav 123).

```
SensorExternalGNSSInstallation ::= SEQUENCE {
   sensorCouplingDateFirst               SensorGNSSCouplingDate,
   firstVuApprovalNumber                 VuApprovalNumber,
   firstVuSerialNumber                   VuSerialNumber,
   sensorCouplingDateCurrent             SensorGNSSCouplingDate,
   currentVuApprovalNumber               VuApprovalNumber,
   currentVUSerialNumber                 VuSerialNumber
}
```

sensorCouplingDateFirst er datoen for den første sammenkobling af det eksterne GNSS-udstyr med en køretøjsenhed.

firstVuApprovalNumber er godkendelsesnummeret på den første køretøjsenhed, som blev koblet sammen med det eksterne GNSS-udstyr.

firstVuSerialNumber er serienummeret på den første køretøjsenhed, som er samparret med det eksterne GNSS-udstyr.

sensorCouplingDateCurrent er datoen for den aktuelle sammenkobling af det eksterne GNSS-udstyr med en køretøjsenhed.

currentVuApprovalNumber er godkendelsesnummeret på den køretøjsenhed, som aktuelt er koblet sammen med det eksterne GNSS-udstyr.

currentVUSerialNumber er serienummeret på den køretøjsenhed, som aktuelt er koblet sammen med det eksterne GNSS-udstyr.

▼B

2.136. **SensorExternalGNSSOSIdentifier**

Anden generation:

Datanavnet på det eksterne GNSS-udstyrs operativsystem.

```
SensorOSIdentifier ::= IA5String(SIZE(2))
```

Tilordnet værdi: fabrikantspecifik.

2.137. **SensorExternalGNSSSCIdentifier**

Anden generation:

Denne type anvendes f.eks. til at identificere det eksterne GNSS-udstyrs kryptografiske modul.

Datanavnet på det eksterne GNSS-udstyrs sikkerhedskomponent.

```
SensorExternalGNSSSCIdentifier ::= IA5String(SIZE(8))
```

Tilordnet værdi: specifik for komponentfabrikanten.

2.138. **SensorGNSSCouplingDate**

Anden generation:

Dato for en sammenkobling af det eksterne GNSS-udstyr med en køretøjsenhed.

```
SensorGNSSCouplingDate ::= TimeReal
```

Tilordnet værdi: Uspecificeret.

2.139. **SensorGNSSSerialNumber**

Anden generation:

Denne type bruges til at lagre GNSS-modtagerens serienummer, både når den sidder i køretøjsenheden, og når den sidder uden for enheden.

GNSS-modtagerens serienummer.

```
SensorGNSSSerialNumber ::= ExtendedSerialNumber
```

2.140. **SensorIdentification**

Oplysninger, gemt på en bevægelsessensor, til identifikation af bevægelsessensoren (bilag 1B, krav 077, og bilag 1C, krav 95).

```
SensorIdentification ::= SEQUENCE {
   sensorSerialNumber                SensorSerialNumber,
   sensorApprovalNumber              SensorApprovalNumber,
   sensorSCIdentifier                SensorSCIdentifier,
   sensorOSIdentifier                SensorOSIdentifier
}
```

sensorSerialNumber er det udvidede serienummer på bevægelsessensoren (hvori reservedelsnummer og fabrikantkode indgår).

sensorApprovalNumber er godkendelsesnummeret på bevægelsessensoren.

sensorSCIdentifier er datanavnet på bevægelsessensorens sikkerhedskomponent.

▼B

sensorOSIdentifier er datanavnet på bevægelsessensorens styresystem.

2.141. **SensorInstallation**

Oplysninger, gemt på en bevægelsessensor, vedrørende montering af bevægelsessensoren (bilag 1B, krav 099, og bilag 1C, krav 122).

```
SensorInstallation ::= SEQUENCE {
   sensorPairingDateFirst                SensorPairingDate,
   firstVuApprovalNumber                 VuApprovalNumber,
   firstVuSerialNumber                   VuSerialNumber,
   sensorPairingDateCurrent              SensorPairingDate,
   currentVuApprovalNumber               VuApprovalNumber,
   currentVUSerialNumber                 VuSerialNumber
}
```

sensorPairingDateFirst er datoen for første samparring af bevægelsessensoren med en køretøjsenhed.

firstVuApprovalNumber er godkendelsesnummeret på den første køretøjsenhed, som er samparret med bevægelsessensoren.

firstVuSerialNumber er serienummeret på den første køretøjsenhed, som er samparret med bevægelsessensoren.

sensorPairingDateCurrent er datoen for den aktuelle samparring af bevægelsessensoren med en køretøjsenhed.

currentVuApprovalNumber er godkendelsesnummeret på den køretøjsenhed, som aktuelt er samparret med bevægelsessensoren.

currentVUSerialNumber er serienummeret på den køretøjsenhed, som aktuelt er samparret med bevægelsessensoren.

2.142. **SensorInstallationSecData**

Oplysninger, gemt på et værkstedskort, vedrørende sikkerhedsdata, som er nødvendige til samparring af bevægelsessensorer med køretøjsenheder (bilag 1C, krav 308 og 331).

Første generation:

```
SensorInstallationSecData ::= TdesSessionKey
```

Tilordnet værdi: I henhold til ISO 16844-3.

Anden generation:

Som beskrevet i tillæg 11 skal et værkstedskort kunne lagre op til tre nøgler til parring af køretøjsenhed og bevægelsessensor. Disse nøgler har forskellige versioner.

```
SensorInstallationSecData ::= SEQUENCE {
   kMWCKey1                              KMWCKey,
   kMWCKey2                              KMWCKey OPTIONAL,
   kMWCKey3                              KMWCKey OPTIONAL
}
```

▼B

2.143. **SensorOSIdentifier**

Datanavn på bevægelsessensorens styresystem.

```
SensorOSIdentifier ::= IA5String(SIZE(2))
```

Tilordnet værdi: fabrikantspecifik.

2.144. **SensorPaired**

Første generation:

Oplysninger, gemt på en køretøjsenhed, til identifikation af den bevægelsessensor, som er samparret med køretøjsenheden (bilag 1B, krav 079, og bilag 1C, krav 97).

```
SensorPaired ::= SEQUENCE {
   sensorSerialNumber                    SensorSerialNumber,
   sensorApprovalNumber                  SensorApprovalNumber,
   sensorPairingDateFirst                SensorPairingDate
}
```

sensorSerialNumber er serienummeret på den bevægelsessensor, som aktuelt er samparret med køretøjsenheden.

sensorApprovalNumber er godkendelsesnummeret på den bevægelsessensor, som aktuelt er samparret med køretøjsenheden.

sensorPairingDateFirst er datoen for første samparring mellem en køretøjsenhed og den bevægelsessensor, som aktuelt er samparret med køretøjsenheden.

2.145. **SensorPairedRecord**

Anden generation:

Oplysninger, der er lagret i en køretøjsenhed, vedrørende identifikationen af en bevægelsessensor der parres med køretøjsenheden (bilag 1C, krav 97)

```
SensorPairedRecord ::= SEQUENCE {
   sensorSerialNumber                    SensorSerialNumber,
   sensorApprovalNumber                  SensorApprovalNumber,
   sensorPairingDate                     SensorPairingDate
}
```

sensorSerialNumber er serienummeret på en bevægelsessensor, der er samparret med køretøjsenheden.

sensorApprovalNumber er typegodkendelsesnummeret for den pågældende bevægelsessensor.

sensorPairingDate er datoen, hvor den pågældende bevægelsessensor er samparret med køretøjsenheden.

2.146. **SensorPairingDate**

Datoen for samparring af bevægelsessensoren med en køretøjsenhed.

```
SensorPairingDate ::= TimeReal
```

Tilordnet værdi: Uspecificeret.

▼B

2.147. **SensorSCIdentifier**

Datanavnet på bevægelsessensorens sikkerhedskomponent.

```
SensorSCIdentifier ::= IA5String(SIZE(8))
```

Tilordnet værdi: specifik for komponentfabrikanten.

2.148. **SensorSerialNumber**

Serienummeret på bevægelsessensoren.

```
SensorSerialNumber ::= ExtendedSerialNumber
```

2.149. **Signature**

En digital underskrift.

Første generation:

```
Signature ::= OCTET STRING (SIZE(128))
```

i overensstemmelse med tillæg 11 (fælles sikkerhedsmekanismer).

Anden generation:

```
Signature ::= OCTET STRING (SIZE(64..132))
```

Tilordnet værdi: i overensstemmelse med tillæg 11, Fælles sikkerhedsmekanismer.

2.150. **SignatureRecordArray**

Anden generation:

En mængde af underskrifter plus metadata, der bruges i protokollen for dataoverførsel.

```
SignatureRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF Signature
}
```

recordType er postens type (Signature). **Tilordnet værdi**: Se RecordType.

recordSize er størrelsen af Signature i bytes.

noOfRecords er antallet af poster i mængden af poster. Værdien skal sættes til 1, da underskrifterne kan have forskellig længde.

records er mængden af underskrifter.

2.151. **SimilarEventsNumber**

Antal tilsvarende hændelser for ét givet døgn (bilag 1B, krav 094, og bilag 1C, krav 117).

```
SimilarEventsNumber ::= INTEGER(0..255)
```

Tilordnet værdi: 0 anvendes ikke, 1 betyder, at der det pågældende døgn kun er indtruffet og registreret én hændelse af den pågældende type, 2 betyder, at der er registreret to hændelser af den pågældende type (kun én er registreret), … 255 betyder, at der er registreret 255 eller flere hændelser af den pågældende type den pågældende dag.

▼B

2.152. **SpecificConditionRecord**

Oplysninger, gemt på et førerkort, et værkstedskort eller en køretøjsenhed der vedrører en særlig omstændighed (bilag 1C, krav 130, 276, 301, 328 og 355).

```
SpecificConditionRecord ::= SEQUENCE {
   entryTime                              TimeReal,
   specificConditionType                  SpecificConditionType
}
```

entryTime er dato og klokkeslæt for indlæsningen.

specificConditionType er den kode, som identificerer den særlige omstændighed.

2.153. **SpecificConditions**

Oplysninger, gemt på et førerkort, et værkstedskort eller en køretøjsenhed, der vedrører en særlig omstændighed (bilag 1C, krav 131, 277, 302, 329 og 356).

Anden generation:

```
SpecificConditions := SEQUENCE {
   conditionPointerNewestRecord          INTEGER(0..NoOfSpecificConditionRecords-1),
   specificConditionRecords              SET SIZE(NoOfSpecificConditionRecords) OF
                                         SpecificConditionRecord
}
```

conditionPointerNewestRecord er indekset på den senest opdaterede post vedrørende særlige omstændigheder.

Tilordnet værdi: Tal svarende til tælleren i posten vedrørende særlige omstændigheder, begyndende med '0' for første forekomst af posten vedrørende særlige omstændigheder i strukturen.

specificConditionRecords er den mængde poster, der indeholder oplysninger om de registrerede særlige omstændigheder.

2.154. **SpecificConditionType**

Kode, som identificerer en særlig omstændighed (bilag 1B, krav 050b, 105a, 212a og 230a, og bilag 1C, krav 62).

```
SpecificConditionType ::= INTEGER(0..255)
```

Første generation:

Tilordnet værdi:

'00'H	RFU
'01'H	Uden for gyldighedsområde — Start
'02'H	Uden for gyldighedsområde — Slut
'03'H	Overfart med færge/tog
'04'H .. 'FF'H	RFU

Anden generation:

Tilordnet værdi:

'00'H	RFU
'01'H	Uden for gyldighedsområde — Start
'02'H	Uden for gyldighedsområde — Slut
'03'H	Overfart med færge/tog — Start
'04'H	Overfart med færge/tog — Slut
'05'H .. 'FF'H	RFU

▼B

2.155. **Speed**

Køretøjets hastighed (km/t).

```
Speed ::= INTEGER(0..255)
```

Tilordnet værdi: kilometer i timen inden for området 0 til 220 km/t.

2.156. **SpeedAuthorised**

Maksimal tilladelig hastighed for køretøjet (definition bb)).

```
SpeedAuthorised ::= Speed
```

2.157. **SpeedAverage**

Gennemsnitshastighed i en forud fastlagt periode (km/t).

```
SpeedAverage ::= Speed
```

2.158. **SpeedMax**

Maksimumhastighed målt i et forud fastlagt tidsrum.

```
SpeedMax ::= Speed
```

2.159. **TachographPayload**

Anden generation:

En definition af denne datatype findes i tillæg 14.

2.160. **TachographPayloadEncrypted**

Anden generation:

Det DER-TLV-krypterede takografindhold, dvs. de krypterede data, der er sendt i RTM-meddelelsen. For så vidt angår krypteringen henvises til tillæg 11, del B, afsnit 13.

```
TachographPayloadEncrypted ::= SEQUENCE {
   tag                                  OCTET STRING(SIZE(1)),
   length                               OCTET STRING(SIZE(1..2)),
   paddingContentIndicatorByte          OCTET STRING(SIZE(1)),
   encryptedData                        OCTET STRING(SIZE(16..192))
}
```

tag er en del af DER-TLV-kodningen og skal være sat til '87' (se tillæg 11, del B, afsnit 13).

length er en del af DER-TLV-kodningen og skal kode længden af følgende paddingContentIndicatorByte og encryptedData.

paddingContentIndicatorByte skal sættes til '00'.

encryptedData er krypteret tachographPayload som anført i tillæg 11, del B, afsnit 13. Længden af disse data i oktetter skal altid være et multiplum af 16.

2.161. **TDesSessionKey**

Første generation:

En tredobbelt DES-sessionsnøgle.

```
TDesSessionKey ::= SEQUENCE {
   tDesKeyA                             OCTET STRING (SIZE(8)),
   tDesKeyB                             OCTET STRING (SIZE(8))
}
```

Tilordnet værdi: Ikke yderligere angivet.

▼B

2.162. **TimeReal**

Kode for et kombineret dato- og klokkeslætfelt, hvor dato og klokkeslæt er angivet som sekunder siden 00h.00m.00s. den 1. januar 1970 GMT.

```
TimeReal{INTEGER:TimeRealRange} ::= INTEGER(0..TimeRealRange)
```

Tilordnet værdi — Oktet udsluttet: Antal sekunder siden midnat den 1. januar 1970 GMT.

Den maksimale værdi af dato/klokkeslæt er året 2106.

2.163. **TyreSize**

Dækdimensionsbetegnelser.

```
TyreSize ::= IA5String(SIZE(15))
```

Tilordnet værdi: i overensstemmelse med direktiv 92/23 (EØF) af 31. marts 1992, EFT L129, s. 95.

2.164. **VehicleIdentificationNumber**

Køretøjets identifikationsnummer med henvisning til køretøjet som helhed, normalt chassisnummeret.

```
VehicleIdentificationNumber ::= IA5String(SIZE(17))
```

Tilordnet værdi: Som defineret i ISO 3779.

2.165. **VehicleIdentificationNumberRecordArray**

Anden generation:

VIN plus metadata, der anvendes i protokollen for dataoverførsel.

```
VehicleIdentificationNumberRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF
                                       VehicleIdentificationNumber
}
```

recordType er postens type (VehicleIdentificationNumber). **Tilordnet værdi**: Se RecordType.

recordSize er størrelsen af VehicleIdentificationNumber i bytes.

noOfRecords er antallet af poster i mængden af poster.

records er mængden af VIN-numre.

2.166. **VehicleRegistrationIdentification**

Identifikation af et køretøj, entydig for Europa (indregistreringsnummer og medlemsstat).

```
VehicleRegistrationIdentification ::= SEQUENCE {
   vehicleRegistrationNation            NationNumeric,
   vehicleRegistrationNumber            VehicleRegistrationNumber
}
```

vehicleRegistrationNation er den stat, hvor køretøjet er indregistreret.

▼B

vehicleRegistrationNumber er køretøjets indregistreringsnummer (VRN).

2.167. **VehicleRegistrationNumber**

Køretøjets indregistreringsnummer (VRN). Indregistreringsnummeret tildeles af registreringsmyndigheden.

```
VehicleRegistrationNumber ::= SEQUENCE {
   codePage                              INTEGER (0..255),
   vehicleRegNumber                      OCTET STRING (SIZE(13))
}
```

codePage angiver et tegnsæt, der er defineret i afsnit 4.

vehicleRegNumber er et indregistreringsnummer, som er indkodet med det angivne tegnsæt.

Tilordnet værdi: Landespecifik.

2.168. **VehicleRegistrationNumberRecordArray**

Anden generation:

VRN plus metadata, der anvendes i protokollen for dataoverførsel.

```
VehicleRegistrationNumberRecordArray ::= SEQUENCE {
   recordType                            RecordType,
   recordSize                            INTEGER(1..65535),
   noOfRecords                           INTEGER(0..65535),
   records                               SET SIZE(noOfRecords) OF
                                         VehicleRegistrationNumber
}
```

recordType er postens type (VehicleRegistrationNumber). **Tilordnet værdi**: Se RecordType.

recordSize er størrelsen af VehicleRegistrationNumber i bytes.

noOfRecords er antallet af poster i mængden af poster.

records er mængden af VRN-numre.

2.169. **VuAbility**

Anden generation:

Oplysninger, gemt i en køretøjsenhed, vedrørende køretøjsenhedens mulighed for at bruge takografkort af første generation (bilag 1C, krav 121).

```
VuAbility ::= OCTET STRING (SIZE(1))
```

Tilordnet værdi — Oktet udsluttet: 'xxxxxxxa'B (8 bit)

For muligheden for at understøtte første generation:

'a'B	Mulighed for at understøtte takografkort af første generation:
	'0'B Første generation understøttes
	'1'B Generation1 understøttes ikke
'xxxxxxx'B	RFU

▼B

2.170. **VuActivityDailyData**

Første generation:

Oplysninger, gemt på en køretøjsenhed, vedrørende skift af aktivitet og/eller skift af kørestatus og/eller skift af kortstatus for en given kalenderdag (bilag 1B, krav 084, og bilag 1C, krav 105, 106 og 107), samt kortlæserstatus kl. 00:00 den pågældende dag.

```
VuActivityDailyData ::= SEQUENCE {
   noOfActivityChanges                  INTEGER SIZE(0..1440),
   activityChangeInfos                  SET SIZE(noOfActivityChanges) OF
                                        ActivityChangeInfo
}
```

noOfActivityChanges er antallet af ActivityChangeInfo-ord i mængden activityChangeInfos.

activityChangeInfos er den mængde ActivityChangeInfo-ord, som for det pågældende døgn er gemt i køretøjsenheden. Den omfatter altid to ActivityChangeInfo-ord, som angiver status for de to kortlæsere kl. 00:00 den pågældende dag.

2.171. **VuActivityDailyRecordArray**

Anden generation:

Oplysninger, gemt på en køretøjsenhed, vedrørende skift af aktivitet og/eller skift af kørestatus og/eller skift af kortstatus for en given kalenderdag (bilag 1C, krav 105, 106 og 107), samt kortlæserstatus kl. 00:00 den pågældende dag.

```
VuActivityDailyRecordArray ::= SEQUENCE {
   recordType                           RecordType,
   recordSize                           INTEGER(1..65535),
   noOfRecords                          INTEGER(0..65535),
   records                              SET SIZE(noOfRecords) OF ActivityChangeInfo
}
```

recordType er postens type (ActivityChangeInfo). **Tilordnet værdi**: Se RecordType.

recordSize er størrelsen af ActivityChangeInfo i bytes.

noOfRecords er antallet af poster i mængden af poster.

records er den mængde ActivityChangeInfo-ord, som for det pågældende døgn er gemt i køretøjsenheden. Den omfatter altid to ActivityChangeInfo-ord, som angiver status for de to kortlæsere kl. 00:00 den pågældende dag.

2.172. **VuApprovalNumber**

Køretøjsenhedens typegodkendelsesnummer.

Første generation:

```
VuApprovalNumber ::= IA5String(SIZE(8))
```

Tilordnet værdi: Uspecificeret.

Anden generation:

```
VuApprovalNumber ::= IA5String(SIZE(16))
```

▼B

Tilordnet værdi:

Godkendelsesnummeret skal tilvejebringes som offentliggjort på Europa-Kommissionens relevante websted, dvs. f.eks. med eventuelle bindestreger. Godkendelsesnummeret skal være venstrejusteret.

2.173. **VuCalibrationData**

Første generation:

Oplysninger, gemt på en køretøjsenhed, vedrørende kalibreringerne af kontrolapparatet (bilag 1B, krav 098).

```
VuCalibrationData ::= SEQUENCE {
   noOfVuCalibrationRecords                INTEGER(0..255),
   vuCalibrationRecords                    SET SIZE(noOfVuCalibrationRecords) OF
                                           VuCalibrationRecord
}
```

noOfVuCalibrationRecords er antallet af poster indeholdt i vuCalibrationRecords-mængden.

vuCalibrationRecords er mængden af kalibreringsposter.

2.174. **VuCalibrationRecord**

Oplysninger, gemt på en køretøjsenhed, vedrørende en kalibrering af kontrolapparatet (bilag 1B, krav 098, og bilag 1C, krav 119 og 120).

Første generation:

```
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 er formålet med kalibreringen.

workshopName, workshopAddresser værkstedets navn og adresse.

workshopCardNumber identificerer det værkstedskort, der er anvendt ved kalibreringen.

workshopCardExpiryDate er kortets udløbsdato.

vehicleIdentificationNumber er køretøjets identifikationsnummer.

▼B

vehicleRegistrationIdentification indeholder køretøjets indregistreringsnummer og den indregistrerende medlemsstat.

wVehicleCharacteristicConstant er køretøjets vejdrejetal.

kConstantOfRecordingEquipment er kontrolapparatets konstant.

lTyreCircumference er den effektive dækperiferi.

tyreSize er dimensionsbetegnelsen for de dæk, der er monteret på køretøjet.

authorisedSpeed er køretøjets tilladte hastighed.

oldOdometerValue, newOdometerValue er gammel og ny kilometerstand.

oldTimeValue, newTimeValue er gammel og ny værdi af dato og klokkeslæt.

nextCalibrationDate er datoen for næste kalibrering af den type, som i CalibrationPurpose foreskrives at skulle udføres af kontrolmyndigheden.

Anden generation:

```
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
}
```

Ud over dataelementerne for første generation anvendes følgende dataelement:

sealDataVu angiver oplysninger om de plomber, der er fastgjort til forskellige komponenter på køretøjet.

2.175. **VuCalibrationRecordArray**

Anden generation:

Oplysninger, gemt på en køretøjsenhed, vedrørende kalibreringerne af kontrolapparatet (bilag 1C, krav 119 og 120).

▼B

```
VuCalibrationRecordArray ::= SEQUENCE {
   recordType                              RecordType,
   recordSize                              INTEGER(1..65535),
   noOfRecords                             INTEGER(0..65535),
   records                                 SET SIZE(noOfRecords) OF
                                           VuCalibrationRecord
}
```

recordType er postens type (VuCalibrationRecord). **Tilordnet værdi**: Se RecordType.

recordSize er størrelsen af VuCalibrationRecord i bytes.

noOfRecords er antallet af poster i mængden af poster.

records er mængden af kalibreringsposter.

2.176. **VuCardIWData**

Første generation:

Oplysninger, gemt på en køretøjsenhed, vedrørende cyklusser med isætning/udtagning af førerkort eller værkstedskort i køretøjsenheden (bilag 1B, krav 081, og bilag 1C, krav 103).

```
VuCardIWData ::= SEQUENCE {
   noOfIWRecords                        INTEGER(0..2^16-1),
   vuCardIWRecords                      SET SIZE(noOfIWRecords) OF VuCardIWRecord
}
```

noOfIWRecords er antallet af poster i mængden af vuCardIWRecords.

vuCardIWRecords er mængden af poster, som vedrører cyklusser med isætning/udtagning af kort.

2.177. **VuCardIWRecord**

Oplysninger, gemt på en køretøjsenhed, vedrørende cyklusser med isætning/udtagning af et førerkort eller et værkstedskort i køretøjsenheden (bilag 1B, krav 081, og bilag 1C, krav 102).

Første generation:

```
VuCardIWRecord ::= SEQUENCE {
   cardHolderName                       HolderName,
   fullCardNumber                       FullCardNumber,
   cardExpiryDate                       TimeReal,
   cardInsertionTime                    TimeReal,
   vehicleOdometerValueAtInsertion      OdometerShort,
   cardSlotNumber                       CardSlotNumber,
   cardWithdrawalTime                   TimeReal,
   vehicleOdometerValueAtWithdrawal     OdometerShort,
   previousVehicleInfo                  PreviousVehicleInfo,
   manualInputFlag                      ManualInputFlag
}
```

cardHolderName er efternavn og fornavn(e) på indehaveren af fører- eller værkstedskortet, som gemt på kortet.

fullCardNumber er kortets type, den medlemsstat, som har udstedt kortet, samt kortets nummer, som gemt på kortet.

▼B

cardExpiryDate er kortets udløbsdato, som gemt på kortet.

cardInsertionTime er isætningsdato og -klokkeslæt.

vehicleOdometerValueAtInsertion er køretøjets kilometerstand ved isætning af kortet.

cardSlotNumber er den kortplads, som kortet sidder i.

cardWithdrawalTime er dato og klokkeslæt for udtagning af kortet.

vehicleOdometerValueAtWithdrawal er køretøjets kilometerstand ved udtagning af kortet.

previousVehicleInfo indeholder oplysninger om det foregående køretøj, føreren har anvendt, som gemt på kortet.

manualInputFlag er et flag, som angiver, om kortindehaveren manuelt har eller ikke har indlæst føreraktiviteter ved isætning af kortet.

Anden generation:

```
VuCardIWRecord ::= SEQUENCE {
   cardHolderName                          HolderName,
   fullCardNumberAndGeneration             FullCardNumberAndGeneration,
   cardExpiryDate                          TimeReal,
   cardInsertionTime                       TimeReal,
   vehicleOdometerValueAtInsertion         OdometerShort,
   cardSlotNumber                          CardSlotNumber,
   cardWithdrawalTime                      TimeReal,
   vehicleOdometerValueAtWithdrawal        OdometerShort,
   previousVehicleInfo                     PreviousVehicleInfo,
   manualInputFlag                         ManualInputFlag
}
```

I stedet for fullCardNumber anvendes følgende dataelement i datastrukturen af anden generation.

fullCardNumberAndGeneration er kortets type, den medlemsstat, som har udstedt kortet, samt kortets nummer og generation, som gemt på kortet.

2.178. **VuCardIWRecordArray**

Anden generation:

Oplysninger, gemt på en køretøjsenhed, vedrørende cyklusser med isætning/udtagning af førerkort eller værkstedskort i køretøjsenheden (bilag 1C, krav 103).

```
VuCardIWRecordArray ::= SEQUENCE {
   recordType                              RecordType,
   recordSize                              INTEGER(1..65535),
   noOfRecords                             INTEGER(0..65535),
   records                                 SET SIZE(noOfRecords) OF VuCardIWRecord
}
```

recordType er postens type (VuCardIWRecord). **Tilordnet værdi**: Se RecordType.

recordSize er størrelsen af VuCardIWRecord i bytes.

▼B

noOfRecords er antallet af poster i mængden af poster.

records er mængden af poster, som vedrører cyklusser med isætning/udtagning af kort.

2.179. **VuCardRecord**

Anden generation:

Oplysninger, gemt på en køretøjsenhed, vedrørende et anvendt takografkort (bilag 1C, krav 132).

```
VuCardRecord ::= SEQUENCE {
   cardExtendedSerialNumber            ExtendedSerialNumber,
   cardPersonaliserID                  OCTET STRING(SIZE(1)),
   typeofTachographCardID              EquipmentType,
   cardStructureVersion                CardStructureVersion,
   cardNumber                          CardNumber
}
```

cardExtendedSerialNumber, aflæst fra filen EF_ICC under kortets hovedfil.

cardPersonaliserID, aflæst fra filen EF_ICC under kortets hovedfil.

typeOfTachographCardId, aflæst fra filen EF_Application_Identification under DF_Tachograph_G2.

cardStructureVersion, aflæst fra filen EF_Application_Identification under DF_Tachograph_G2.

cardNumber, aflæst fra filen EF_Identification under DF_Tachograph_G2.

2.180. **VuCardRecordArray**

Anden generation:

Oplysninger, gemt på en køretøjsenhed, vedrørende de takografkort, der er anvendt sammen med køretøjsenheden. Disse oplysninger er beregnet til analyse af problemer med køretøjsenhed og kort (bilag 1C, krav 132).

```
VuCardRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF VuCardRecord
}
```

recordType er postens type (VuCardRecord). **Tilordnet værdi**: Se RecordType.

recordSize er størrelsen af VuCardRecord i bytes.

noOfRecords er antallet af poster i mængden af poster.

records er mængden af poster, som vedrører de takografkort, der er anvendt sammen med køretøjsenheden.

▼B

2.181. **VuCertificate**

Certifikat for en køretøjsenheds offentlige nøgle.

```
VuCertificate ::= Certificate
```

2.182. **VuCertificateRecordArray**

Anden generation:

Certifikatet for køretøjsenheden plus metadata, der anvendes i protokollen for dataoverførsel.

```
VuCertificateRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF VuCertificate
}
```

recordType er postens type (VuCertificate). **Tilordnet værdi**: Se RecordType.

recordSize er størrelsen af VuCertificate i bytes.

noOfRecords er antallet af poster i mængden af poster. Værdien skal sættes til 1, da certifikaterne kan have forskellig længde.

records er mængden af certifikater for køretøjsenheder.

2.183. **VuCompanyLocksData**

Første generation:

Oplysninger, gemt på en køretøjsenhed, der vedrører virksomhedslåse (bilag 1B, krav 104).

```
VuCompanyLocksData ::= SEQUENCE {
   noOfLocks                           INTEGER(0..255),
   vuCompanyLocksRecords               SET SIZE(noOfLocks) OF VuCompanyLocksRecord
}
```

noOfLocks er antallet af låse, som er opført i vuCompanyLocksRecords.

vuCompanyLocksRecords er mængden af poster vedrørende virksomhedslåse.

2.184. **VuCompanyLocksRecord**

Oplysninger, gemt på en køretøjsenhed, der vedrører én virksomhedslås (bilag 1B, krav 104, og bilag 1C, krav 128).

Første generation:

```
VuCompanyLocksRecord ::= SEQUENCE {
   lockInTime                          TimeReal,
   lockOutTime                         TimeReal,
   companyName                         Name,
   companyAddress                      Address,
   companyCardNumber                   FullCardNumber
}
```

▼B

lockInTime, lockOutTime er dato og klokkeslæt for lås-ind og lås-ud.

companyName, companyAddress er navn og adresse på den virksomhed, der er knyttet til den pågældende lås-ind.

companyCardNumber identificerer det kort, der er anvendt ved lås-ind.

Anden generation:

```
VuCompanyLocksRecord ::= SEQUENCE {
   lockInTime                          TimeReal,
   lockOutTime                         TimeReal,
   companyName                         Name,
   companyAddress                      Address,
   companyCardNumberAndGeneration      FullCardNumberAndGeneration
}
```

I stedet for companyCardNumber anvendes følgende dataelement i datastrukturen af anden generation.

companyCardNumberAndGeneration identificerer det kort, der er anvendt ved lås-ind, og kortets generation.

2.185. **VuCompanyLocksRecordArray**

Anden generation:

Oplysninger, gemt på en køretøjsenhed, der vedrører virksomhedslåse (bilag 1C, krav 128).

```
VuCompanyLocksRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF
                                       VuCompanyLocksRecord
}
```

recordType er postens type (VuCompanyLocksRecord). **Tilordnet værdi**: Se RecordType.

recordSize er størrelsen af VuCompanyLocksRecord i bytes.

noOfRecords er antallet af poster i mængden af poster. Værdi 0..255.

records er mængden af poster vedrørende virksomhedslåse.

2.186. **VuControlActivityData**

Første generation:

Oplysninger, gemt på en køretøjsenhed, vedrørende kontroller foretaget ved hjælp af denne køretøjsenhed (bilag 1B, krav 102).

```
VuControlActivityData ::= SEQUENCE {
   noOfControls                        INTEGER(0..20),
   vuControlActivityRecords            SET SIZE(noOfControls) OF
                                       VuControlActivityRecord
}
```

▼B

noOfControls er antallet af kontroller, som er opført i vuControlActivityRecords.

vuControlActivityRecords er mængden af kontrolaktivitetsposter.

2.187. **VuControlActivityRecord**

Oplysninger, gemt på en køretøjsenhed, vedrørende en kontrol foretaget ved hjælp af denne køretøjsenhed (bilag 1B, krav 102, og bilag 1C, krav 126).

Første generation:

```
VuControlActivityRecord ::= SEQUENCE {
   controlType                          ControlType,
   controlTime                          TimeReal,
   controlCardNumber                    FullCardNumber,
   downloadPeriodBeginTime              TimeReal,
   downloadPeriodEndTime                TimeReal
}
```

controlType er kontrollens type.

controlTime er dato og klokkeslæt for kontrollen.

controlCardNumber identificerer det kontrolkort, som er anvendt til kontrollen.

downloadPeriodBeginTime er begyndelsestidspunktet for dataoverførsel, når en sådan har fundet sted.

downloadPeriodEndTime er sluttidspunktet for dataoverførsel, når en sådan har fundet sted.

Anden generation:

```
VuControlActivityRecord ::= SEQUENCE {
   controlType                          ControlType,
   controlTime                          TimeReal,
   controlCardNumberAndGeneration       FullCardNumberAndGeneration,
   downloadPeriodBeginTime              TimeReal,
   downloadPeriodEndTime                TimeReal
}
```

I stedet for controlCardNumber anvendes følgende dataelement i datastrukturen af anden generation.

controlCardNumberAndGeneration identificerer det kontrolkort, som er anvendt til kontrollen, og kortets generation.

2.188. **VuControlActivityRecordArray**

Anden generation:

Oplysninger, gemt på en køretøjsenhed, vedrørende kontroller foretaget ved hjælp af denne køretøjsenhed (bilag 1C, krav 126).

▼B

```
VuControlActivityRecordArray ::= SEQUENCE {
   recordType                              RecordType,
   recordSize                              INTEGER(1..65535),
   noOfRecords                             INTEGER(0..65535),
   records                                 SET SIZE(noOfRecords) OF
                                           VuControlActivityRecord
}
```

recordType er postens type (VuControlActivityRecord). **Tilordnet værdi**: Se RecordType.

recordSize er størrelsen af VuControlActivityRecord i bytes.

noOfRecords er antallet af poster i mængden af poster.

records er mængden af kontrolaktivitetsposter for køretøjsenheden.

2.189. **VuDataBlockCounter**

Tæller, som er gemt på et kort, og som sekventielt identificerer cyklusserne med isætning/udtagning af kortet i køretøjsenheder.

```
VuDataBlockCounter ::= BCDString(SIZE(2))
```

Tilordnet værdi: Fortløbende nummer, som, efter at have nået maksimumværdien 9 999, begynder forfra fra 0.

2.190. **VuDetailedSpeedBlock**

Oplysninger, gemt på en køretøjsenhed, der detaljeret angiver køretøjets hastighed i et minut, i hvilket køretøjet har bevæget sig (bilag 1B, krav 093, og bilag 1C, krav 116).

```
VuDetailedSpeedBlock ::= SEQUENCE {
   speedBlockBeginDate    TimeReal,
   speedsPerSecond        SEQUENCE SIZE(60) OF Speed
}
```

speedBlockBeginDate er dato og klokkeslæt for den første hastighedsværdi inden for blokken.

speedsPerSecond er den kronologiske sekvens af målte hastigheder hvert sekund for det minut, der begynder på speedBlockBeginDate (inklusive).

2.191. **VuDetailedSpeedBlockRecordArray**

Anden generation:

Oplysninger, gemt på en køretøjsenhed, vedrørende køretøjets detaljerede hastighed.

```
VuDetailedSpeedBlockRecordArray ::= SEQUENCE {
   recordType                              RecordType,
   recordSize                              INTEGER(1..65535),
   noOfRecords                             INTEGER(0..65535),
   records                                 SET SIZE(noOfRecords) OF
                                           VuDetailedSpeedBlock
}
```

recordType er postens type (VuDetailedSpeedBlock). **Tilordnet værdi**: Se RecordType.

▼B

recordSize er størrelsen af VuDetailedSpeedBlock i bytes.

noOfRecords er antallet af poster i mængden af poster.

records er mængden af detaljerede hastighedsblokke.

2.192. **VuDetailedSpeedData**

Første generation:

Oplysninger, gemt på en køretøjsenhed, vedrørende køretøjets detaljerede hastighed.

```
VuDetailedSpeedData ::= SEQUENCE {
   noOfSpeedBlocks                         INTEGER(0..2^16-1),
   vuDetailedSpeedBlocks                   SET SIZE(noOfSpeedBlocks) OF
                                           VuDetailedSpeedBlock
}
```

noOfSpeedBlocks er antallet af hastighedsblokke i mængden vuDetailedSpeedBlocks.

vuDetailedSpeedBlocks er mængden af detaljerede hastighedsblokke.

2.193. **VuDownloadablePeriod**

Ældste og nyeste dato, for hvilke en køretøjsenhed lagrer data vedrørende førerens aktiviteter (bilag 1B, krav 081, 084 eller 087, og bilag 1C, krav 102, 105 og 108).

```
VuDownloadablePeriod ::= SEQUENCE {
   minDownloadableTime                     TimeReal
   maxDownloadableTime                     TimeReal
}
```

minDownloadableTime er ældste dato og klokkeslæt, som i køretøjsenheden er gemt vedrørende isætning af kort, aktivitetsskift eller indlæsning af sted.

maxDownloadableTime er nyeste dato og klokkeslæt, som i køretøjsenheden er gemt vedrørende udtagning af kort, aktivitetsskift eller indlæsning af sted.

2.194. **VuDownloadablePeriodRecordArray**

Anden generation:

VUDownloadablePeriod plus metadata, der anvendes i protokollen for dataoverførsel.

```
VuDownloadablePeriodRecordArray ::= SEQUENCE {
   recordType                              RecordType,
   recordSize                              INTEGER(1..65535),
   noOfRecords                             INTEGER(0..65535),
   records                                 SET SIZE(noOfRecords) OF
                                           VuDownloadablePeriod
}
```

recordType er postens type (VuDownloadablePeriod). **Tilordnet værdi**: Se RecordType.

▼B

recordSize er størrelsen af VuDownloadablePeriod i bytes.

noOfRecords er antallet af poster i mængden af poster.

records er mængden af VuDownloadablePeriod-poster.

2.195. **VuDownloadActivityData**

Oplysninger, gemt på en køretøjsenhed, der vedrører dens sidste overførsel (bilag 1B, krav 105, og bilag 1C, krav 129).

Første generation:

```
VuDownloadActivityData ::= SEQUENCE {
   downloadingTime                        TimeReal,
   fullCardNumber                         FullCardNumber,
   companyOrWorkshopName                  Name
}
```

downloadingTime er dato og klokkeslæt for dataoverførslen.

fullCardNumber identificerer det kort, der er anvendt til at muliggøre dataoverførslen.

companyOrWorkshopName er virksomhedens eller værkstedets navn.

Anden generation:

```
VuDownloadActivityData ::= SEQUENCE {
   downloadingTime                        TimeReal,
   fullCardNumberAndGeneration            FullCardNumberAndGeneration,
   companyOrWorkshopName                  Name
}
```

I stedet for fullCardNumber anvendes følgende dataelement i datastrukturen af anden generation.

fullCardNumberAndGeneration identificerer det kort, der er anvendt til at muliggøre dataoverførslen, og kortets generation.

2.196. **VuDownloadActivityDataRecordArray**

Anden generation:

Oplysninger om den sidste overførsel for køretøjsenheden (bilag 1C, krav 129).

```
VuDownloadActivityDataRecordArray ::= SEQUENCE {
   recordType                             RecordType,
   recordSize                             INTEGER(1..65535),
   noOfRecords                            INTEGER(0..65535),
   records                                SET SIZE(noOfRecords) OF VuDownloadActivityData
}
```

recordType er postens type (VuDownloadActivityData). **Tilordnet værdi**: Se RecordType.

recordSize er størrelsen af VuDownloadActivityData i bytes.

noOfRecords er antallet af poster i mængden af poster.

▼B

records er mængden af dataposter vedrørende dataoverførsel.

2.197. **VuEventData**

Første generation:

Oplysninger, gemt på en køretøjsenhed, vedrørende hændelser (bilag 1B, krav 094, bortset fra overskridelser af tilladt hastighed).

```
VuEventData ::= SEQUENCE {
   noOfVuEvents                          INTEGER(0..255),
   vuEventRecords                        SET SIZE(noOfVuEvents) OF VuEventRecord
}
```

noOfVuEvents er antallet af hændelser på listen over hændelser i mængden vuEventRecords.

vuEventRecords er mængden af hændelsesposter.

2.198. **VuEventRecord**

Oplysninger, gemt på en køretøjsenhed, vedrørende en hændelse (bilag 1B, krav 094, og bilag 1C, krav 117, bortset fra overskridelse af tilladt hastighed).

Første generation:

```
VuEventRecord ::= SEQUENCE {
   eventType                             EventFaultType,
   eventRecordPurpose                    EventFaultRecordPurpose,
   eventBeginTime                        TimeReal,
   eventEndTime                          TimeReal,
   cardNumberDriverSlotBegin             FullCardNumber,
   cardNumberCodriverSlotBegin           FullCardNumber,
   cardNumberDriverSlotEnd               FullCardNumber,
   cardNumberCodriverSlotEnd             FullCardNumber,
   similarEventsNumber                   SimilarEventsNumber
}
```

eventType er hændelsens type.

eventRecordPurpose er det formål, hændelsen er registreret til.

eventBeginTime er hændelsens startdato og -klokkeslæt.

eventEndTime er hændelsens slutdato og -klokkeslæt.

cardNumberDriverSlotBegin identificerer det kort, der er sat i førerens kortplads ved hændelsens start.

cardNumberCodriverSlotBegin identificerer det kort, der sad i medchaufførens kortplads ved hændelsens start.

cardNumberDriverSlotEnd identificerer det kort, der sad i førerens kortplads ved hændelsens slutning.

cardNumberCodriverSlotEnd identificerer det kort, der sad i medchaufførens kortplads ved hændelsens slutning.

similarEventsNumber er antallet af tilsvarende hændelser samme døgn.

Denne sekvens kan anvendes til alle hændelser, bortset fra overskridelser af tilladt hastighed.

▼B

Anden generation:

```
VuEventRecord ::= SEQUENCE {
   eventType                              EventFaultType,
   eventRecordPurpose                     EventFaultRecordPurpose,
   eventBeginTime                         TimeReal,
   eventEndTime                           TimeReal,
   cardNumberAndGenDriverSlotBegin        FullCardNumberAndGeneration,
   cardNumberAndGenCodriverSlotBegin      FullCardNumberAndGeneration,
   cardNumberAndGenDriverSlotEnd          FullCardNumberAndGeneration,
   cardNumberAndGenCodriverSlotEnd        FullCardNumberAndGeneration,
   similarEventsNumber                    SimilarEventsNumber,
   manufacturerSpecificEventFaultData   ManufacturerSpecificEventFaultData
}
```

Ud over dataelementerne for første generation anvendes følgende dataelementer:

manufacturerSpecificEventFaultData indeholder yderligere fabrikantspecifikke oplysninger om hændelsen.

I stedet for cardNumberDriverSlotBegin, cardNumberCodriverSlotBegin, cardNumberDriverSlotEnd og cardNumberCodriverSlotEnd anvendes følgende dataelementer i datastrukturen af anden generation:

cardNumberAndGenDriverSlotBegin identificerer det kort, der sad i førerens kortplads ved hændelsens start, og kortets generation.

cardNumberAndGenCodriverSlotBegin identificerer det kort, der sad i medchaufførens kortplads ved hændelsens start, og kortets generation.

cardNumberAndGenDriverSlotEnd identificerer det kort, der sad i førerens kortplads ved hændelsens afslutning, og kortets generation.

cardNumberAndGenCodriverSlotEnd identificerer det kort, der sad i medchaufførens kortplads ved hændelsens afslutning, og kortets generation.

Hvis hændelsen er en tidskonflikt, skal eventBeginTime og eventEndTime fortolkes som følger:

eventBeginTime er kontrolapparatets dato og klokkeslæt.

cardWithdrawalTime er GNSS-udstyrets dato og klokkeslæt.

2.199. **VuEventRecordArray**

Anden generation:

Oplysninger, gemt på en køretøjsenhed, vedrørende hændelser (bilag 1C, krav 117, bortset fra overskridelser af tilladt hastighed).

```
VuEventRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF VuEventRecord
}
```

recordType er postens type (VuEventRecord). **Tilordnet værdi**: Se RecordType.

▼B

recordSize er størrelsen af VuEventRecord i bytes.

noOfRecords er antallet af poster i mængden af poster.

records er mængden af hændelsesposter.

2.200. **VuFaultData**

Første generation:

Oplysninger, gemt på en køretøjsenhed, vedrørende fejl (bilag 1B, krav 096).

```
VuFaultData ::= SEQUENCE {
   noOfVuFaults                          INTEGER(0..255),
   vuFaultRecords                        SET SIZE(noOfVuFaults) OF VuFaultRecord
}
```

noOfVuFaults er antallet af fejl opført i vuFaultRecords-mængden.

vuFaultRecords er mængden af fejlposter.

2.201. **VuFaultRecord**

Oplysninger, gemt på en køretøjsenhed, der vedrører en fejl (bilag 1B, krav 096, og bilag 1C, krav 118).

Første generation:

```
VuFaultRecord ::= SEQUENCE {
   faultType                             EventFaultType,
   faultRecordPurpose                    EventFaultRecordPurpose,
   faultBeginTime                        TimeReal,
   faultEndTime                          TimeReal,
   cardNumberDriverSlotBegin             FullCardNumber,
   cardNumberCodriverSlotBegin           FullCardNumber,
   cardNumberDriverSlotEnd               FullCardNumber,
   cardNumberCodriverSlotEnd             FullCardNumber
}
```

faultType er typen af den pågældende fejl ved kontrolapparatet.

faultRecordPurpose er det formål, til hvilket fejlen er blevet registreret.

faultBeginTime er fejlens startdato og -klokkeslæt.

faultEndTime er fejlens slutdato og -klokkeslæt.

cardNumberDriverSlotBegin identificerer det kort, der sad i førerens kortplads ved fejlens begyndelse.

cardNumberCodriverSlotBegin identificerer det kort, der sad i medchaufførens kortplads ved fejlens begyndelse.

cardNumberDriverSlotEnd identificerer det kort, der sad i førerens kortplads ved fejlens slutning.

cardNumberCodriverSlotEnd identificerer det kort, der sad i medchaufførens kortplads ved fejlens slutning.

▼B

Anden generation:

```
VuFaultRecord ::= SEQUENCE {
   faultType                              EventFaultType,
   faultRecordPurpose                     EventFaultRecordPurpose,
   faultBeginTime                         TimeReal,
   faultEndTime                           TimeReal,
   cardNumberAndGenDriverSlotBegin        FullCardNumberAndGeneration,
   cardNumberAndGenCodriverSlotBegin      FullCardNumberAndGeneration,
   cardNumberAndGenDriverSlotEnd          FullCardNumberAndGeneration,
   cardNumberAndGenCodriverSlotEnd        FullCardNumberAndGeneration,
   manufacturerSpecificEventFaultData   ManufacturerSpecificEventFaultData
}
```

Ud over dataelementerne for første generation anvendes følgende dataelement:

manufacturerSpecificEventFaultData indeholder yderligere fabrikantspecifikke oplysninger om fejlen.

I stedet for cardNumberDriverSlotBegin, cardNumberCodriverSlotBegin, cardNumberDriverSlotEnd og cardNumberCodriverSlotEnd anvendes følgende dataelementer i datastrukturen af anden generation:

cardNumberAndGenDriverSlotBegin identificerer det kort, der sad i førerens kortplads ved fejlens start, og kortets generation.

cardNumberAndGenCodriverSlotBegin identificerer det kort, der sad i medchaufførens kortplads ved fejlens start, og kortets generation.

cardNumberAndGenDriverSlotEnd identificerer det kort, der sad i førerens kortplads ved fejlens afslutning, og kortets generation.

cardNumberAndGenCodriverSlotEnd identificerer det kort, der sad i medchaufførens kortplads ved fejlens afslutning, og kortets generation.

2.202. **VuFaultRecordArray**

Anden generation:

Oplysninger, gemt på en køretøjsenhed, vedrørende fejl (bilag 1C, krav 118).

```
VuFaultRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF VuFaultRecord
}
```

recordType er postens type (VuFaultRecord). **Tilordnet værdi**: Se RecordType.

recordSize er størrelsen af VuFaultRecord i bytes.

noOfRecords er antallet af poster i mængden af poster.

records er mængden af fejlposter.

▼B

2.203. **VuGNSSCDRecord**

Anden generation:

Oplysninger, gemt på en køretøjsenhed, vedrørende køretøjets GNSS-position, hvis førerens sammenhængende køretid når op på et multiplum af tre timer (bilag 1C, krav 108, 110).

```
VuGNSSCDRecord ::= SEQUENCE {
   timeStamp                              TimeReal,
   cardNumberAndGenDriverSlot             FullCardNumberAndGeneration,
   cardNumberAndGenCodriverSlot           FullCardNumberAndGeneration,
   gnssPlaceRecord                        GNSSPlaceRecord
}
```

timeStamp er den dato og det klokkeslæt, hvor kortindehaverens sammenhængende køretid når op på et multiplum af tre timer.

cardNumberAndGenDriverSlot identificerer det kort, der sad i førerens kortplads, og kortets generation.

cardNumberAndGenCodriverSlot identificerer det kort, der sad i medchaufførens kortplads, og kortets generation.

gnssPlaceRecord indeholder oplysninger om køretøjets position.

2.204. **VuGNSSCDRecordArray**

Anden generation:

Oplysninger, gemt på en køretøjsenhed, vedrørende køretøjets GNSS-position, hvis førerens sammenhængende køretid når op på et multiplum af tre timer (bilag 1C, krav 108 og 110).

```
VuGNSSCDRecordArray  ::= SEQUENCE {
   recordType                             RecordType,
   recordSize                             INTEGER(1..65535),
   noOfRecords                            INTEGER(0..65535),
   records                                SET SIZE(noOfRecords) OF VuGNSSCDRecord
}
```

recordType er postens type (VuGNSSCDRecord). **Tilordnet værdi**: Se RecordType.

recordSize er størrelsen af VuGNSSCDRecord i bytes.

noOfRecords er antallet af poster i mængden af poster.

records er mængden af GNSS-poster for sammenhængende køretid.

2.205. **VuIdentification**

Oplysninger, gemt på en køretøjsenhed, til identifikation af køretøjsenheden (bilag 1B, krav 075, og bilag 1C, krav 93 og 121).

▼B

Første generation:

```
VuIdentification ::= SEQUENCE {
   vuManufacturerName                    VuManufacturerName,
   vuManufacturerAddress                 VuManufacturerAddress,
   vuPartNumber                          VuPartNumber,
   vuSerialNumber                        VuSerialNumber,
   vuSoftwareIdentification              VuSoftwareIdentification,
   vuManufacturingDate                   VuManufacturingDate,
   vuApprovalNumber                      VuApprovalNumber
}
```

vuManufacturerName er navnet på fabrikanten af køretøjsenheden.

vuManufacturerAddress er adressen på fabrikanten af køretøjsenheden.

vuPartNumber er reservedelsnummeret på køretøjsenheden.

vuSerialNumber er serienummeret på køretøjsenheden.

vuSoftwareIdentification identificerer det programmel, der anvendes i køretøjsenheden.

vuManufacturingDate er køretøjsenhedens fabrikationsdato.

vuApprovalNumber er køretøjsenhedens typegodkendelsesnummer.

Anden generation:

```
VuIdentification ::= SEQUENCE {
   vuManufacturerName                    VuManufacturerName,
   vuManufacturerAddress                 VuManufacturerAddress,
   vuPartNumber                          VuPartNumber,
   vuSerialNumber                        VuSerialNumber,
   vuSoftwareIdentification              VuSoftwareIdentification,
   vuManufacturingDate                   VuManufacturingDate,
   vuApprovalNumber                      VuApprovalNumber,
   vuGeneration                          Generation,
   vuAbility                             VuAbility
}
```

Ud over dataelementerne for første generation anvendes følgende dataelementer:

vuGeneration angiver køretøjsenhedens generation.

vuAbility rummer oplysninger om, hvorvidt køretøjsenheden understøtter takografkort af første generation eller ej.

2.206. **VuIdentificationRecordArray**

Anden generation:

VuIdentification plus metadata, der anvendes i protokollen for dataoverførsel.

▼B

```
VuIdentificationRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF VuIdentification
}
```

recordType er postens type (VuIdentification). **Tilordnet værdi**: Se RecordType.

recordSize er størrelsen af VuIdentification i bytes.

noOfRecords er antallet af poster i mængden af poster.

records er mængden af VuIdentification-poster.

2.207. **VuITSConsentRecord**

Anden generation:

Oplysninger, gemt på en køretøjsenhed, vedrørende en førers samtykke om at anvende intelligente transportsystemer.

```
VuITSConsentRecord ::= SEQUENCE {
   cardNumberAndGen                    FullCardNumberAndGeneration,
   consent                             BOOLEAN
}
```

cardNumberAndGen identificerer kortet, herunder dets generation. Dette skal være et førerkort eller et værkstedskort.

consent er et flag, som angiver, om føreren har givet sit samtykke til at bruge intelligente transportsystemer sammen med køretøjet/køretøjsenheden.

Tilordnet værdi:

TRUE	angiver, at føreren har givet sit samtykke til at bruge intelligente transportsystemer.
FALSE	angiver, at føreren ikke har givet sit samtykke til at bruge intelligente transportsystemer.

2.208. **VuITSConsentRecordArray**

Anden generation:

Oplysninger, gemt på en køretøjsenhed, vedrørende føreres samtykke til brug af intelligente transportsystemer (bilag 1C, krav 200).

```
VuITSConsentRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF VuITSConsentRecord
}
```

recordType er postens type (VuITSConsentRecord). **Tilordnet værdi**: Se RecordType.

recordSize er størrelsen af VuITSConsentRecord i bytes.

noOfRecords er antallet af poster i mængden af poster.

records er mængden af poster om samtykke til brug af ITS.

▼B

2.209. **VuManufacturerAddress**

Adressen på fabrikanten af køretøjsenheden.

```
VuManufacturerAddress ::= Address
```

Tilordnet værdi: Uspecificeret.

2.210. **VuManufacturerName**

Navnet på fabrikanten af køretøjsenheden.

```
VuManufacturerName ::= Name
```

Tilordnet værdi: Uspecificeret.

2.211. **VuManufacturingDate**

Fabrikationsdatoen for køretøjsenheden.

```
VuManufacturingDate ::= TimeReal
```

Tilordnet værdi: Uspecificeret.

2.212. **VuOverSpeedingControlData**

Oplysninger, gemt på en køretøjsenhed, vedrørende de overskridelser af tilladt hastighed, som har fundet sted siden seneste kontrol med overskridelse af tilladt hastighed (bilag 1B, krav 095, og bilag 1C, krav 117).

```
VuOverSpeedingControlData ::= SEQUENCE {
   lastOverspeedControlTime             TimeReal,
   firstOverspeedSince                  TimeReal,
   numberOfOverspeedSince               OverspeedNumber
}
```

lastOverspeedControlTime er dato og klokkeslæt for seneste kontrol med overskridelse af tilladt hastighed.

firstOverspeedSince er dato og klokkeslæt for første overskridelse af tilladt hastighed siden denne kontrol med overskridelse af tilladt hastighed.

numberOfOverspeedSince er antallet af hændelser med overskridelse af tilladt hastighed siden seneste kontrol med overskridelse af tilladt hastighed.

2.213. **VuOverSpeedingControlDataRecordArray**

Anden generation:

VuOverSpeedingControlData plus metadata, der anvendes i protokollen for dataoverførsel.

```
VuOverSpeedingControlDataRecordArray ::= SEQUENCE {
   recordType                           RecordType,
   recordSize                           INTEGER(1..65535),
   noOfRecords                          INTEGER(0..65535),
   records                              SET SIZE(noOfRecords) OF
                                        VuOverSpeedingControlData
}
```

▼B

recordType er postens type (VuOverSpeedingControlData). **Tilordnet værdi**: Se RecordType.

recordSize er størrelsen af VuOverSpeedingControlData i bytes.

noOfRecords er antallet af poster i mængden af poster.

records er mængden af dataposter om kontrol med overskridelse af tilladt hastighed.

2.214. **VuOverSpeedingEventData**

Første generation:

Oplysninger, gemt på en køretøjsenhed, vedrørende hændelser med overskridelse af tilladt hastighed (bilag 1B, krav 094).

```
VuOverSpeedingEventData ::= SEQUENCE {
   noOfVuOverSpeedingEvents              INTEGER(0..255),
   vuOverSpeedingEventRecords            SET SIZE(noOfVuOverSpeedingEvents) OF
                                         VuOverSpeedingEventRecord
}
```

noOfVuOverSpeedingEvents er antal hændelser opført i listen over hændelser i mængden vuOverSpeedingEventRecords.

vuOverSpeedingEventRecords er mængden af poster vedrørende hændelser med overskridelse af tilladt hastighed.

2.215. **VuOverSpeedingEventRecord**

Første generation:

Oplysninger, gemt på en køretøjsenhed, vedrørende overskridelse af tilladt hastighed (bilag 1B, krav 094, og bilag 1C, krav 117).

```
VuOverSpeedingEventRecord ::= SEQUENCE {
   eventType                             EventFaultType,
   eventRecordPurpose                    EventFaultRecordPurpose,
   eventBeginTime                        TimeReal,
   eventEndTime                          TimeReal,
   maxSpeedValue                         SpeedMax,
   averageSpeedValue                     SpeedAverage,
   cardNumberDriverSlotBegin             FullCardNumber,
   similarEventsNumber                   SimilarEventsNumber
}
```

eventType er hændelsens type.

eventRecordPurpose er det formål, hændelsen er registreret til.

eventBeginTime er hændelsens startdato og -klokkeslæt.

eventEndTime er hændelsens slutdato og -klokkeslæt.

maxSpeedValue er den højeste hastighed målt under hændelsen.

averageSpeedValue er den aritmetiske gennemsnitshastighed målt under hændelsen.

▼B

cardNumberDriverSlotBegin identificerer det kort, der er sat i førerens kortplads ved hændelsens start.

similarEventsNumber er antallet af tilsvarende hændelser samme døgn.

Anden generation:

Oplysninger, gemt på en køretøjsenhed, vedrørende overskridelse af tilladt hastighed (bilag 1B, krav 094, og bilag 1C, krav 117).

```
VuOverSpeedingEventRecord ::= SEQUENCE {
   eventType                              EventFaultType,
   eventRecordPurpose                     EventFaultRecordPurpose,
   eventBeginTime                         TimeReal,
   eventEndTime                           TimeReal,
   maxSpeedValue                          SpeedMax,
   averageSpeedValue                      SpeedAverage,
   cardNumberAndGenDriverSlotBegin        FullCardNumberAndGeneration,
   similarEventsNumber                    SimilarEventsNumber
}
```

I stedet for cardNumberDriverSlotBegin benytter datastrukturen for anden generation følgende dataelement:

cardNumberAndGenDriverSlotBegin identificerer det kort, inklusive generation, der er sat i førerens kortplads ved hændelsens start.

2.216. **VuOverSpeedingEventRecordArray**

Anden generation:

Oplysninger, gemt på en køretøjsenhed, vedrørende hændelser med overskridelse af tilladt hastighed (bilag 1C, krav 117).

```
VuOverSpeedingEventRecordArray ::= SEQUENCE {
   recordType                             RecordType,
   recordSize                             INTEGER(1..65535),
   noOfRecords                            INTEGER(0..65535),
   records                                SET SIZE(noOfRecords) OF
                                          VuOverSpeedingEventRecord
}
```

recordType er postens type (VuOverSpeedingEventRecord). **Tilordnet værdi**: Se RecordType.

recordSize er størrelsen af VuOverSpeedingEventRecord i bytes.

noOfRecords er antallet af poster i mængden af poster.

records er mængden af poster vedrørende hændelser med overskridelse af tilladt hastighed.

2.217. **VuPartNumber**

Serienummeret på køretøjsenheden.

```
VuPartNumber ::= IA5String(SIZE(16))
```

Tilordnet værdi: Specifik for fabrikanten af køretøjsenheden.

▼B

2.218. **VuPlaceDailyWorkPeriodData**

Første generation:

Oplysninger, gemt på en køretøjsenhed, vedrørende de steder, hvor føreren begynder eller afslutter den daglige arbejdstid (bilag 1B, krav 087, og bilag 1C, krav 108 og 110).

```
VuPlaceDailyWorkPeriodData ::= SEQUENCE {
   noOfPlaceRecords                    INTEGER(0..255),
   vuPlaceDailyWorkPeriodRecords       SET SIZE(noOfPlaceRecords) OF
                                       VuPlaceDailyWorkPeriodRecord
}
```

noOfPlaceRecords er antallet af poster i mængden vuPlaceDailyWorkPeriodRecords.

vuPlaceDailyWorkPeriodRecords er mængden af poster vedrørende steder.

2.219. **VuPlaceDailyWorkPeriodRecord**

Første generation:

Oplysninger, gemt på en køretøjsenhed, vedrørende et sted, hvor føreren begynder eller afslutter den daglige arbejdstid (bilag 1B, krav 087, og bilag 1C, krav 108 og 110).

```
VuPlaceDailyWorkPeriodRecord ::= SEQUENCE {
   fullCardNumber                      FullCardNumber,
   placeRecord                         PlaceRecord
}
```

fullCardNumber er førerens korttype, den kortudstedende medlemsstat og kortets nummer.

placeRecord indeholder oplysningerne om det indlæste sted.

Anden generation:

Oplysninger, gemt på en køretøjsenhed, vedrørende et sted, hvor føreren begynder eller afslutter den daglige arbejdstid (bilag 1B, krav 087, og bilag 1C, krav 108 og 110).

```
VuPlaceDailyWorkPeriodRecord ::= SEQUENCE {
   fullCardNumberAndGeneration         FullCardNumberAndGeneration,
   placeRecord                         PlaceRecord
}
```

I stedet for fullCcardNumber benytter datastrukturen for anden generation følgende dataelement:

fullCardNumberAndGeneration angiver korttypen, den udstedende medlemsstat, kortnummeret og kortets generation, som gemt på kortet.

▼B

2.220. **VuPlaceDailyWorkPeriodRecordArray**

Anden generation:

Oplysninger, gemt på en køretøjsenhed, vedrørende de steder, hvor føreren begynder eller afslutter den daglige arbejdstid (bilag 1C, krav 108 og 110).

```
VuPlaceDailyWorkPeriodRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF
                                       VuPlaceDailyWorkPeriodRecord
}
```

recordType er postens type (VuPlaceDailyWorkPeriodRecord).
Tilordnet værdi: Se RecordType.

recordSize er størrelsen af VuPlaceDailyWorkPeriodRecord i bytes.

noOfRecords er antallet af poster i mængden af poster.

records er mængden af poster vedrørende steder.

2.221. **VuPrivateKey**

Første generation:

Køretøjsenhedens private nøgle.

```
VuPrivateKey ::= RSAKeyPrivateExponent
```

2.222. **VuPublicKey**

Første generation:

Køretøjsenhedens offentlige nøgle.

```
VuPublicKey ::= PublicKey
```

2.223. **VuSerialNumber**

Køretøjsenhedens serienummer (bilag 1B, krav 075, og bilag 1C, krav 93).

```
VuSerialNumber ::= ExtendedSerialNumber
```

2.224. **VuSoftInstallationDate**

Dato for installation af den programmelversion, som anvendes i køretøjsenheden.

```
VuSoftInstallationDate ::= TimeReal
```

Tilordnet værdi: Uspecificeret.

▼B

2.225. **VuSoftwareIdentification**

Oplysninger, gemt på en køretøjsenhed, vedrørende det installerede programmel.

```
VuSoftwareIdentification ::= SEQUENCE {
   vuSoftwareVersion                    VuSoftwareVersion,
   vuSoftInstallationDate               VuSoftInstallationDate
}
```

vuSoftwareVersion er versionsnummeret på det programmel, der anvendes i køretøjsenheden.

vuSoftInstallationDate er datoen for installation af den pågældende version af programmellet.

2.226. **VuSoftwareVersion**

Versionsnummeret på det programmel, der anvendes i køretøjsenheden.

```
VuSoftwareVersion ::= IA5String(SIZE(4))
```

Tilordnet værdi: Uspecificeret.

2.227. **VuSpecificConditionData**

Første generation:

Oplysninger, gemt på en køretøjsenhed, vedrørende særlige omstændigheder.

```
VuSpecificConditionData ::= SEQUENCE {
   noOfSpecificConditionRecords         INTEGER(0..2^16-1)
   specificConditionRecords             SET SIZE (noOfSpecificConditionRecords) OF
                                        SpecificConditionRecord
}
```

noOfSpecificConditionRecords er det antal poster, som er indeholdt i specificConditionRecords-mængden.

specificConditionRecords er mængden af poster vedrørende særlige omstændigheder.

2.228. **VuSpecificConditionRecordArray**

Anden generation:

Oplysninger, gemt på en køretøjsenhed, vedrørende særlige omstændigheder (bilag 1C, krav 130).

```
VuSpecificConditionRecordArray ::= SEQUENCE {
   recordType                           RecordType,
   recordSize                           INTEGER(1..65535),
   noOfRecords                          INTEGER(0..65535),
   records                              SET SIZE(noOfRecords) OF
                                        SpecificConditionRecord
}
```

recordType er postens type (SpecificConditionRecord). **Tilordnet værdi**: Se RecordType.

recordSize er størrelsen af SpecificConditionRecord i bytes.

noOfRecords er antallet af poster i mængden af poster.

records er mængden af poster vedrørende særlige omstændigheder.

▼B

2.229. **VuTimeAdjustmentData**

Første generation:

Oplysninger, gemt på en køretøjsenhed, vedrørende tidsjusteringer, som har fundet sted uden for rammerne af en planmæssig kalibrering (bilag 1B, krav 101).

```
VuTimeAdjustmentData ::= SEQUENCE {
   noOfVuTimeAdjRecords                  INTEGER(0..6),
   vuTimeAdjustmentRecords               SET SIZE(noOfVuTimeAdjRecords) OF
                                         VuTimeAdjustmentRecord
}
```

noOfVuTimeAdjRecords er antallet af poster i vuTimeAdjustmentRecords-mængden.

vuTimeAdjustmentRecords er mængden af tidsjusteringsposter.

2.230. **VuTimeAdjustmentGNSSRecord**

Anden generation:

Oplysninger, gemt på en køretøjsenhed, vedrørende tidsjustering, som er baseret på tidsdata fra GNSS (bilag 1C, krav 124 og 125).

```
VuTimeAdjustmentGNSSRecord ::= SEQUENCE {
   oldTimeValue                          TimeReal,
   newTimeValue                          TimeReal
}
```

oldTimeValue, newTimeValue er gammel og ny værdi af dato og klokkeslæt.

2.231. **VuTimeAdjustmentGNSSRecordArray**

Anden generation:

Oplysninger, gemt på en køretøjsenhed, vedrørende tidsjustering, som er baseret på tidsdata fra GNSS (bilag 1C, krav 124 og 125).

```
VuTimeAdjustmentGNSSRecordArray ::= SEQUENCE {
   recordType                            RecordType,
   recordSize                            INTEGER(1..65535),
   noOfRecords                           INTEGER(0..65535),
   records                               SET SIZE(noOfRecords) OF
                                         VuTimeAdjustmentGNSSRecord
}
```

recordType er postens type (VuTimeAdjustmentGNSSRecord).
Tilordnet værdi: Se RecordType.

recordSize er størrelsen af VuTimeAdjustmentGNSSRecord i bytes.

noOfRecords er antallet af poster i mængden af poster.

records er mængden af poster vedrørende GNSS-tidsjustering.

▼B

2.232. **VuTimeAdjustmentRecord**

Oplysninger, gemt på en køretøjsenhed, vedrørende en tidsjustering, som har fundet sted uden for rammerne af en planmæssig kalibrering (bilag 1B, krav 101, og bilag 1C, krav 124 og 125).

Første generation:

```
VuTimeAdjustmentRecord ::= SEQUENCE {
   oldTimeValue                         TimeReal,
   newTimeValue                         TimeReal,
   workshopName                         Name,
   workshopAddress                      Address,
   workshopCardNumber                   FullCardNumber
}
```

oldTimeValue, newTimeValue er gammel og ny værdi af dato og klokkeslæt.

workshopName, workshopAddresser værkstedets navn og adresse.

workshopCardNumber identificerer det værkstedskort, der er brugt til at foretage tidsjustering.

Anden generation:

```
VuTimeAdjustmentRecord ::= SEQUENCE {
   oldTimeValue                         TimeReal,
   newTimeValue                         TimeReal,
   workshopName                         Name,
   workshopAddress                      Address,
   workshopCardNumberAndGeneration      FullCardNumberAndGeneration
}
```

I stedet for workshopCardNumber anvendes følgende dataelement i datastrukturen af anden generation:

workshopCardNumberAndGeneration identificerer det værkstedskort, der er brugt til at foretage tidsjustering, og kortets generation.

2.233. **VuTimeAdjustmentRecordArray**

Anden generation:

Oplysninger, gemt på en køretøjsenhed, vedrørende tidsjusteringer, som har fundet sted uden for rammerne af en planmæssig kalibrering (bilag 1C, krav 124 og 125).

```
VuTimeAdjustmentRecordArray ::= SEQUENCE {
   recordType                           RecordType,
   recordSize                           INTEGER(1..65535),
   noOfRecords                          INTEGER(0..65535),
   records                              SET SIZE(noOfRecords) OF
                                        VuTimeAdjustmentRecord
}
```

recordType er postens type (VuTimeAdjustmentRecord). **Tilordnet værdi**: Se RecordType.

recordSize er størrelsen af VuTimeAdjustmentRecord i bytes.

▼B

noOfRecords er antallet af poster i mængden af poster.

records er mængden af poster vedrørende tidsjustering.

2.234. **WorkshopCardApplicationIdentification**

Oplysninger, gemt på et værkstedskort, til identifikation af kortets applikation (bilag 1C, krav 307 og 330).

Første generation:

```
WorkshopCardApplicationIdentification ::= SEQUENCE {
   typeOfTachographCardId               EquipmentType,
   cardStructureVersion                 CardStructureVersion,
   noOfEventsPerType                    NoOfEventsPerType,
   noOfFaultsPerType                    NoOfFaultsPerType,
   activityStructureLength              CardActivityLengthRange,
   noOfCardVehicleRecords               NoOfCardVehicleRecords,
   noOfCardPlaceRecords                 NoOfCardPlaceRecords,
   noOfCalibrationRecords               NoOfCalibrationRecords
}
```

typeOfTachographCardId angiver den implementerede korttype.

cardStructureVersion angiver den version af strukturen, som er implementeret i kortet.

noOfEventsPerType er antallet af hændelser af hver hændelsestype, som kan gemmes på kortet.

noOfFaultsPerType er antal fejl af hver fejltype, som kan gemmes på kortet.

activityStructureLength angiver antal bytes til rådighed til lagring af aktivitetsposter.

noOfCardVehicleRecords er antallet af køretøjsposter, som kan gemmes på kortet.

noOfCardPlaceRecords er antallet af steder, som kan gemmes på kortet.

noOfCalibrationRecords er antallet af kalibreringsposter, som kan gemmes på kortet.

Anden generation:

```
WorkshopCardApplicationIdentification ::= SEQUENCE {
   typeOfTachographCardId               EquipmentType,
   cardStructureVersion                 CardStructureVersion,
   noOfEventsPerType                    NoOfEventsPerType,
   noOfFaultsPerType                    NoOfFaultsPerType,
   activityStructureLength              CardActivityLengthRange,
   noOfCardVehicleRecords               NoOfCardVehicleRecords,
   noOfCardPlaceRecords                 NoOfCardPlaceRecords,
   noOfCalibrationRecords               NoOfCalibrationRecords,
   noOfGNSSCDRecords                    NoOfGNSSCDRecords,
   noOfSpecificConditionRecords         NoOfSpecificConditionRecords
}
```

Ud over dataelementerne for første generation anvendes følgende dataelementer:

noOfGNSSCDRecords er det antal GNSS-poster for sammenhængende køretid, som kan gemmes på kortet.

▼B

noOfSpecificConditionRecords er det antal poster vedrørende særlige omstændigheder, som kan gemmes på kortet.

2.235. **WorkshopCardCalibrationData**

Oplysninger, gemt på et værkstedskort, vedrørende de aktiviteter, der er udført med kortet (bilag 1C, krav 314, 316, 337 og 339).

```
WorkshopCardCalibrationData ::= SEQUENCE {
   calibrationTotalNumber               INTEGER(0 .. 2^16-1),
   calibrationPointerNewestRecord       INTEGER(0 .. NoOfCalibrationRecords-1),
   calibrationRecords                   SET SIZE(NoOfCalibrationRecords) OF
                                        WorkshopCardCalibrationRecord
}
```

calibrationTotalNumber er det samlede antal kalibreringer, som er udført med kortet.

calibrationPointerNewestRecord er indekset for den senest opdaterede kalibreringspost.

Tilordnet værdi: Tal svarende til tælleren i kalibreringsposten, begyndende med '0' for den første forekomst af kalibreringsposterne i strukturen.

calibrationRecords er den mængde poster, der indeholder oplysninger om kalibrering og/eller tidsjustering.

2.236. **WorkshopCardCalibrationRecord**

Oplysninger, gemt på et værkstedskort, vedrørende en kalibrering, der er udført med kortet (bilag 1C, krav 314 og 337).

Første generation:

```
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 er formålet med kalibreringen.

vehicleIdentificationNumber er køretøjets identifikationsnummer.

vehicleRegistration indeholder køretøjets indregistreringsnummer og den indregistrerende medlemsstat.

wVehicleCharacteristicConstant er køretøjets vejdrejetal.

▼B

kConstantOfRecordingEquipment er kontrolapparatets konstant.

lTyreCircumference er den effektive dækperiferi.

tyreSize er dimensionsbetegnelsen for de dæk, der er monteret på køretøjet.

authorisedSpeed er køretøjets tilladte hastighed.

oldOdometerValue, newOdometerValue er gammel og ny kilometerstand.

oldTimeValue, newTimeValue er gammel og ny værdi af dato og klokkeslæt.

nextCalibrationDate er datoen for næste kalibrering af den type, som i CalibrationPurpose foreskrives at skulle udføres af kontrolmyndigheden.

vuPartNumber, **vuSerialNumber** og **sensorSerialNumber** er de dataelementer, som identificerer kontrolapparatet.

Anden generation:

```
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
}
```

Ud over dataelementerne for første generation anvendes følgende dataelementer:

sensorGNSSSerialNumber, som identificerer eksternt GNSS-udstyr.

rcmSerialNumber, som identificerer et modul til fjernkommunikation.

sealDataCard angiver oplysninger om de plomber, der er fastgjort til forskellige komponenter på køretøjet.

▼B

2.237. **WorkshopCardHolderIdentification**

Oplysninger, gemt på et værkstedskort, til identifikation af kortindehaveren (bilag 1C, krav 311 og 334).

```
WorkshopCardHolderIdentification ::= SEQUENCE {
   workshopName                          Name,
   workshopAddress                       Address,
   cardHolderName                        HolderName,
   cardHolderPreferredLanguage           Language
}
```

workshopName er navnet på kortindehaverens værksted.

workshopAddress er adressen på kortindehaverens værksted.

cardHolderName er efternavn og fornavn(e) på indehaveren (f.eks. navnet på mekanikeren).

cardHolderPreferredLanguage er det af kortindehaveren foretrukne sprog.

2.238. **WorkshopCardPIN**

Det personlige identifikationsnummer på værkstedskortet (bilag 1C, krav 309 og 332).

```
WorkshopCardPIN ::= IA5String(SIZE(8))
```

Tilordnet værdi: Den PIN-kode, som kendes af kortindehaveren, udfyldt mod højre med sideskiftbytes indtil 8 bytes.

2.239. **W-VehicleCharacteristicConstant**

Køretøjets vejdrejetal (definition k)).

```
W-VehicleCharacteristicConstant ::= INTEGER(0..2^16-1))
```

Tilordnet værdi: Impulser pr. kilometer inden for området 0 til 64 255 impulser/km.

2.240. **VuPowerSupplyInterruptionRecord**

Anden generation:

Oplysninger, gemt i en køretøjsenhed, om begivenheder med afbrydelse af strømforsyningen (bilag 1C, krav 117).

```
VuPowerSupplyInterruptionRecord ::= SEQUENCE {
   eventType                             EventFaultType,
   eventRecordPurpose                    EventFaultRecordPurpose,
   eventBeginTime                        TimeReal,
   eventEndTime                          TimeReal,
   cardNumberAndGenDriverSlotBegin       FullCardNumberAndGeneration,
   cardNumberAndGenDriverSlotEnd         FullCardNumberAndGeneration,
   cardNumberAndGenCodriverSlotBegin     FullCardNumberAndGeneration,
   cardNumberAndGenCodriverSlotEnd       FullCardNumberAndGeneration,
   similarEventsNumber                   SimilarEventsNumber
}
```

eventType er begivenhedstypen.

eventRecordPurpose er det formål, til hvilket begivenheden registreres.

eventBeginTime er dato og tidspunkt for begivenhedens begyndelse.

▼B

eventEndTime er dato og tidspunkt for begivenhedens afslutning.

cardNumberAndGenDriverSlotBegin identificerer det kort, inklusive generation, der er isat førerens kortplads ved begivenhedens begyndelse.

cardNumberAndGenDriverSlotEnd identificerer det kort, inklusive generation, der er isat førerens kortplads ved begivenhedens afslutning.

cardNumberAndGenCodriverSlotBegin identificerer det kort, inklusive generation, der er isat medchaufførens kortplads ved begivenhedens begyndelse.

cardNumberAndGenCodriverSlotEnd identificerer det kort, inklusive generation, der er isat medchaufførens kortplads ved begivenhedens afslutning.

similarEventsNumber er antallet af lignende begivenheder den pågældende dag.

2.241. **VuPowerSupplyInterruptionRecordArray**

Anden generation:

Oplysninger, gemt i en køretøjsenhed, om begivenheder med afbrydelse af strømforsyningen (bilag 1C, krav 117).

```
VuPowerSupplyInterruptionRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF
                                       VuPowerSupplyInterruptionRecord
}
```

recordType er postens type (VuPowerSupplyInterruptionRecord). **Tilordnet værdi**: Se RecordType.

recordSize er størrelsen af VuPowerSupplyInterruptionRecord i bytes.

noOfRecords er antallet af poster i mængden af poster.

records er mængden af poster vedrørende afbrydelse af strømforsyningen.

2.242. **VuSensorExternalGNSSCoupledRecordArray**

Generation 2:

En mængde af SensorExternalGNSSCoupledRecord plus metadata, der anvendes i protokollen for dataoverførsel.

```
VuSensorExternalGNSSCoupledRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF
                                       SensorExternalGNSSCoupledRecord
}
```

recordType er postens type (SensorExternalGNSSCoupledRecord). **Tilordnet værdi**: Se RecordType.

▼B

recordSize er størrelsen af SensorExternalGNSSCoupledRecord i bytes.

noOfRecords er antallet af poster i mængden af poster.

records er mængden af poster vedrørende sensoren sammenkoblet med det eksterne GNSS-udstyr

2.243. **VuSensorPairedRecordArray**

Anden generation:

En mængde af SensorPairedRecord plus metadata, der anvendes i protokollen for dataoverførsel.

```
VuSensorPairedRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF SensorPairedRecord
}
```

recordType er postens type (SensorPairedRecord). **Tilordnet værdi**: Se RecordType

recordSize er størrelsen af SensorPairedRecord i byte.

noOfRecords er antallet af poster i mængden af poster.

records er en mængde poster om sensorens samparring.

3. DEFINITIONER AF VÆRDI- OG STØRRELSESOMRÅDE

Definition af de variabelværdier, der er anvendt til definitionerne i punkt 2.

```
TimeRealRange ::= 2^32-1
```

4. TEGNSÆT

Til IA5Strings anvendes ASCII-tegnsættet som defineret i ISO/IEC 8824-1. Af hensyn til letlæselighed og overskuelighed er de tilordnede værdier gengivet nedenfor. Ved eventuel uoverensstemmelse har ISO/IEC 8824-1 forrang for denne bemærkning.

```
  ! " # $ % & ' ( ) * + , - . / 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 { | } ~
```

I andre tegnstrenge (Address, Name, VehicleRegistrationNumber) anvendes herudover tegn fra decimalkodeområdet 161-255 i de følgende 8-bit standardtegnsæt, angivet ved Code Page-nummeret: Standardtegnsæt	Code Page (Decimal)
ISO/IEC 8859-1 Latin-1 Vesteuropæisk	1
ISO/IEC 8859-2 Latin-2 Centraleuropæisk	2
ISO/IEC 8859-3 Latin-3 Sydeuropæisk	3
ISO/IEC 8859-5 Latin/Kyrillisk	5
ISO/IEC 8859-7 Latin/Græsk	7
ISO/IEC 8859-9 Latin-5 Tyrkisk	9

▼B

I andre tegnstrenge (Address, Name, VehicleRegistrationNumber) anvendes herudover tegn fra decimalkodeområdet 161-255 i de følgende 8-bit standardtegnsæt, angivet ved Code Page-nummeret: Standardtegnsæt	Code Page (Decimal)
ISO/IEC 8859-13 Latin-7 Det baltiske område	13
ISO/IEC 8859-15 Latin-9	15
ISO/IEC 8859-16 Latin-10 Sydøsteuropæisk	16
KOI8-R Latin/Kyrillisk	80
KOI8-U Latin/Kyrillisk	85

5. KODNING

Ved kodning efter ASN.1-kodningsreglerne skal alle de definerede datatyper være kodet i overensstemmelse med ISO/IEC 8825-2, justeret variant.

6. OBJEKTIDENTIFIKATORER OG APPLIKATIONSIDENTIFIKATORER

6.1. **Objektidentifikatorer**

Objektidentifikatorerne i dette afsnit er kun relevante for anden generation. De beskrives nærmere i TR-03110-3 og gentages her for fuldstændighedens skyld. De er indeholdt i undertræet af bsi-de:

```
bsi-de OBJECT IDENTIFIER ::= {
   itu-t(0) identified-organization(4) etsi(0)
   reserved(127) etsi-identified-organization(0) 7
}
```

Datanavne på protokoller til ægthedsbekræftelse af køretøjsenheder

```
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}
```

Eksempel: Hvis ægthedsbekræftelse af en køretøjsenhed skal foretages med SHA-384, skal objektidentifikatoren `bsi-de protocols(2) smartcard(2) 2 2 4` anvendes (i ASN.1-notation). Værdien af denne objektidentifikator i punktnotation er `0.4.0.127.0.7.2.2.2.2.4`.

	Punktnotation	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

Datanavne på protokoller til ægthedsbekræftelse af chips

```
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}
```

Eksempel: Ægthedsbekræftelse af chips skal foretages med ECDH-algoritmen, så der fremkommer en AES-sessionsnøgle med en længde på 128 bit. Denne sessionsnøgle anvendes efterfølgende i CBC-funktionstilstand til at sikre datafortrolighed, og CMAC-algoritmen anvendes for at sikre dataægthed. Derfor skal objektidentifikatoren `bsi-de protocols(2) smartcard(2) 3 2 2` anvendes (i ASN.1-notation). Værdien af denne objektidentifikator i punktnotation er `0.4.0.127.0.7.2.2.3.2.2`.

	Punktnotation	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. **Applikationsidentifikatorer**

Anden generation:

Applikationsidentifikatoren (AID) for det eksterne GNSS-udstyr (anden generation) er ‘FF 44 54 45 47 4D’. Dette er en beskyttet AID i overensstemmelse med ISO/IEC 7816-4.

Bemærk: De sidste fem bytes koder DTEGM for intelligente takografers eksterne GNSS-udstyr.

Applikationsidentifikatoren for takografkortapplikationer af anden generation er ‘FF 53 4D 52 44 54’. Dette er en beskyttet AID i overensstemmelse med ISO/IEC 7816-4.

▼B

Tillæg 2

SPECIFIKATION AF TAKOGRAFKORT

INDHOLDSFORTEGNELSE

1. INDLEDNING

1.1. Forkortelser

1.2. Referencer

2. ELEKTRISKE OG FYSISKE EGENSKABER

2.1. Forsyningsspænding og strømforbrug

2.2. Programmeringsspænding V_{pp}

2.3. Klokgenerering og -frekvens

2.4. I/O-kontakt

2.5. Kortets tilstande

3. HARDWARE OG KOMMUNIKATION

3.1. Indledning

3.2. Transmissionsprotokol

3.2.1 Protokoller

3.2.2 ATR

3.2.3 PTS

3.3. Adgangsregler

3.4. Oversigt over kommandoer og fejlkoder

3.5. Kommandobeskrivelser

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. TAKOGRAFKORTENES STRUKTUR

4.1. Hovedfil (Master file — MF)

4.2. Førerkortapplikationer

4.2.1 Førerkortapplikation af første generation

4.2.2 Førerkortapplikation af anden generation

4.3. Værkstedskortapplikationer

4.3.1 Værkstedskortsapplikation af første generation

4.3.2 Værkstedskortsapplikation af anden generation

4.4. Kontrolkortapplikationer

4.4.1 Kontrolkortapplikation af første generation

4.4.2 Kontrolkortapplikation af anden generation

4.5. Virksomhedskortapplikationer

4.5.1 Virksomhedskortapplikation af første generation

4.5.2 Virksomhedskortapplikation af anden generation

1. INDLEDNING

1.1. **Forkortelser**

I dette tillæg anvendes følgende forkortelser:

AC	Betingelser for adgang til faciliteten
AES	Avanceret krypteringsstandard (Advanced Encryption Standard)
AID	Applikationsidentifikator (Application Identifier)
ALW	Altid (Always)
APDU	Dataenhed i applikationsprotokol (struktur i kommando) (Application Protocol Data Unit)
ATR	Svar på reset (Answer to Reset)
AUT	Identitetsbekræftet (Authenticated)
C6, C7	Kortets kontakt nr. 6 og 7 som beskrevet i ISO/IEC 7816-2
cc	Klokcyklusser (clock cycles)
CHV	Information til verifikation af kortindehaver (Card holder verification information)
CLA	Klassebyte i APDU-kommando (Class byte of an APDU command)

▼B

DSRC	Dedikeret kortdistancekommunikation (Dedicated Short Range Communication)
DF	Dedikeret fil En DF kan indeholde andre filer (EF eller DF)
ECC	Elliptisk kurvekryptografi (Elliptic Curve Cryptography)
EF	Elementærfil (Elementary File)
etu	Elementær tidsenhed (elementary time unit)
G1	Første generation
G2	Anden generation
IC	Integreret kredsløb
ICC	Chipkort (Integrated Circuit Card)
ID	Identifikator
IFD	Kortlæser (interface device)
IFS	Længde af informationsfelt (information field size)
IFSC	Længde af informationsfelt til kort (information field size for the card)
IFSD	Informationsfeltlængde for kortlæser (information field size device)
INS	Ordrebyte i APDU-kommando (instruction byte)
Lc	Længde af inddata til APDU-kommando
Le	Længde af forventede data (uddata til en kommando)
MF	Hovedfil (dedikeret rodfil) (Master file)
NAD	Knudepunktadresse i en T = 1 protokol (Node address)
NEV	Aldrig
P1-P2	Parameterbytes
PIN	Personligt identifikationsnummer
PRO SM	Beskyttet med sikker meddelelsesoverførsel (protected with secure messaging)
PTS	Valgt transmissionsprotokol (protocol transmission selection)
RFU	Forbeholdt fremtidig brug
RST	Nulstilling (af et kort) (Reset)
SFID	Kort id for elementærfil
SM	Sikker meddelelsesoverførsel
SW1-SW2	Statusbytes
TS	Initialt tegn i ATR (svar på nulstilling)
VPP	Programmeringsspænding
VU	Køretøjsenhed
XXh	Størrelsen XX i hexadecimal notation
‘XXh’	Størrelsen XX i hexadecimal notation
||	Sammenkædningssymbol (03||04 = 0304)

▼B

1.2. **Referencer**

I dette tillæg henvises til følgende referencer:

ISO/IEC 7816-2 Identification cards — Integrated circuit cards — Part 2: Dimensions and location of the contacts. ISO/IEC 7816-2:2007.

ISO/IEC 7816-3 Identification cards — Integrated circuit cards — Part 3: Electrical interface and transmission protocols. ISO/IEC 7816-3:2006.

ISO/IEC 7816-4 Identification cards — Integrated circuit cards — Part 4: Organization, security and commands for interchange. ISO/IEC 7816-4:2013 + Cor 1: 2014.

ISO/IEC 7816-6 Identification cards — Integrated circuit cards — Part 6: Interindustry data elements for interchange. ISO/IEC 7816-6:2004 + Cor 1: 2006.

ISO/IEC 7816-8 Identification cards — Integrated circuit cards — 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. ELEKTRISKE OG FYSISKE EGENSKABER

TCS_01 Alle elektroniske signaler skal overholde ISO/IEC 7816-3, medmindre andet er angivet.

TCS_02 Placering og dimensioner af kortets kontakter skal være i overensstemmelse med ISO/IEC 7816-2.

2.1. **Forsyningsspænding og strømforbrug**

TCS_03 Kortet skal fungere i henhold til specifikationerne inden for de forbrugsgrænser, der foreskrives i ISO/IEC 7816-3.

TCS_04 Kortet skal fungere ved Vcc = 3 V (± 0,3 V) eller Vcc = 5 V (± 0,5 V).

Valg af spænding skal ske i overensstemmelse med ISO/IEC 7816-3.

2.2. **Programmeringsspænding V_{pp}**

TCS_05 Kortet behøver ingen programmeringsspænding på pin C6. Det forventes, at klemme C6 ikke tilsluttes en kortlæser. Kontakt C6 kan være tilsluttet Vcc i kortet, men må ikke stelforbindes. Denne spænding må ikke i noget tilfælde tolkes.

2.3. **Klokgenerering og -frekvens**

TCS_06 Kortet skal arbejde i et frekvensområde fra 1 til 5 MHz og kan understøtte højere frekvenser. Inden for én kortsession kan klokfrekvensen variere ± 2 %. Klokfrekvensen genereres af køretøjsenheden, ikke af kortet selv. Arbejdscyklussen kan variere mellem 40 og 60 %.

TCS_07 Under de betingelser, der er indeholdt i kortfilen EF ICC, kan den eksterne klokke standses. Den første byte i kroppen af filen EF ICC koder for betingelserne i Clock-stop-funktionstilstand:

▼B

Lavt	Højt		
Bit 3	Bit 2	Bit 1	
0	0	1	Clockstop tilladt, intet foretrukket niveau
0	1	1	Clockstop tilladt, højt niveau foretrukket
1	0	1	Clockstop tilladt, lavt niveau foretrukket
0	0	0	Clockstop ikke tilladt
0	1	0	Clockstop kun tilladt på højt niveau
1	0	0	Clockstop kun tilladt på lavt niveau

Bit 4 til 8 ubenyttet.

2.4. **I/O-kontakt**

TCS_08 I/O-kontakten C7 anvendes til at modtage og overføre data fra og til kortlæseren. Under funktion må kun enten kortet eller kortlæseren være i dataoverførselstilstand. Hvis begge enheder er i overførselstilstand, må det ikke kunne medføre skade på kortet. Medmindre kortet overfører data, skal det skifte til modtagetilstand.

2.5. **Kortets tilstande**

TCS_09 Kortet arbejder i to tilstande, mens forsyningsspændingen tilføres:

i driftstilstand, mens det udfører kommandoer eller er koblet til den digitale enhed

i hviletilstand på alle andre tidspunkter; i denne tilstand skal alle data ligge på kortet.

3. HARDWARE OG KOMMUNIKATION

3.1. **Indledning**

Dette afsnit beskriver de funktioner, der som minimum kræves af takografkort og køretøjsenheder for at sikre korrekt funktion og interoperabilitet.

Takografkort opfylder så vidt muligt de foreliggende gældende ISO/IEC-normer (specielt ISO/IEC 7816). Dog beskrives kommandoer og protokoller fuldt ud for at specificere visse indskrænkninger i brugen eller visse forskelle, når sådanne findes. De foreskrevne kommandoer er fuldt forenelige med de anførte normer, medmindre andet er angivet.

3.2. **Transmissionsprotokol**

TCS_10 Transmissionsprotokollen skal være i overensstemmelse med ISO/IEC 7816-3 for T = 0 og T = 1. Specielt skal køretøjsenheden anerkende udvidelser af ventetid, som sendes af kortet.

3.2.1 *Protokoller*

TCS_11 Kortet skal give mulighed både for protokol **T = 0** og protokol **T = 1**. Derudover kan kortet understøtte andre kontaktrelaterede protokoller.

TCS_12 T = 0 er standardprotokol, hvorfor der kræves en **PTS**-kommando for at ændre protokol til T = 1.

▼B

TCS_13 Enheder skal understøtte **direkte konvention** i begge protokoller:

TCS_14 Ved ATR præsenteres **Information Field Size Card**-byten i TA3. Denne værdi skal være mindst 'F0h' (= 240 bytes).

For protokollerne gælder følgende begrænsninger:

TCS_15 **T = 0**

— Kortlæseren skal understøtte et svar på I/O efter begyndelsen af signalet på nulstilling fra 400 cc.

— Kortlæseren skal kunne læse tegn, som er adskilt af 12 etu.

— Kortlæseren skal læse en forkert karakter og dens gentagelse, hvis de er adskilt af 13 etu. Hvis der registreres en forkert karakter, kan fejlsignalet på I/O optræde mellem 1 etu og 2 etu. Kortlæseren skal understøtte en forsinkelse på 1 etu.

— Kortlæseren skal acceptere et svar på nulstilling (ATR) på 33 bytes (TS + 32).

— Hvis det pågældende ATR indeholder et TC1, skal den ekstra beskyttelsestid gælde for tegn sendt af kortlæseren, dog kan tegn sendt af kortet stadig være adskilt af 12 etu. Dette gælder også for ACK-tegnet sendt af kortet efter, at der er afgivet et P3-tegn af kortlæseren.

— Kortlæseren skal tage hensyn til et NUL-tegn afsendt fra kortet.

— Kortlæseren skal acceptere den supplerende funktionstilstand for ACK.

— Kommandoen GET RESPONSE kan ikke bruges i kædningsfunktion til at hente data, hvis længde eventuelt er over 255 bytes.

TCS_16 **T = 1**

— NAD-byte: ikke anvendt (NAD skal sættes til '00').

— S-block ABORT: Ikke anvendt.

— S-block VPP state fejl: Ikke anvendt.

— Den totale kædningslængde for et datafelt er ikke over 255 bytes (skal sikres af kortlæseren).

— Informationsfeltstørrelse for kortlæser (IFSD) skal angives af kortlæseren umiddelbart efter svar på nulstilling: Kortlæseren skal overføre S-blokkens IFS-forespørgsel efter svar på nulstilling (ATR), og kortet skal tilbagemelde S-blokkens IFS. Den anbefalede værdi for IFSD er 254 bytes.

— Kortet anmoder ikke om efterjustering af IFS.

▼B

3.2.2 *ATR*

TCS_17 Kortlæseren kontrollerer ATR-bytes (svar på nulstilling) i henhold til ISO/IEC 7816-3. Der skal ikke foretages kontrol af historiske ATR-tegn.

Eksempel på grundlæggende biprotokollær ATR i henhold til ISO/IEC 7816-3

Karakter	Værdi	Bemærkninger
TS	'3Bh'	Angiver direkte konvention
T0	'85h'	TD1 foreligger; 5 historiske bytes til stede
TD1	'80h'	TD1 foreligger; T = 0 skal anvendes
TD2	'11h'	TA3 foreligger; T = 1 skal anvendes
TA3	'XXh' (mindst 'F0h')	Størrelse af informationsfelt på kort (IFSC)
TH1 til TH5	'XXh'	Historiske tegn
TCK	'XXh'	Kontroltegn (eksklusive OR)

TCS_18 Efter Answer To Reset (ATR) er hovedfilen (MF) valgt automatisk og bliver den aktuelle mappe.

3.2.3 *PTS*

TCS_19 Standardprotokollen er T = 0. For at vælge protokol T = 1 skal der sendes en PTS (også benævnt PPS) til kortet fra kortlæseren.

TCS_20 Da protokollerne T = 0 og T = 1 begge er påbudte for kortet, er det grundlæggende valg af transmissionsprotokol (PTS) for protokolskift påbudt for kortet.

Som angivet i ISO/IEC 7816-3 kan PTS benyttes til at skifte til en højere transmissionshastighed end den standardhastighed, som vælges af kortet i svar på nulstilling (ATR), hvis der er nogen (TA(1)) bytes til stede.

Højere transmissionshastigheder er valgfri for kortet.

TCS_21 Hvis ingen anden transmissionshastighed end standardhastigheden understøttes (eller den valgte transmissionshastighed ikke understøttes), skal kortet svare korrekt på protokoltransmissionsvalget (PTS) i henhold til ISO/IEC 7816-3 ved at udelade PPS1-byten.

Følgende er eksempler på grundlæggende PTS til protokolvalg:

Karakter	Værdi	Bemærkninger
PPSS	'FFh'	Starttegn
PPS0	'00h' eller '01h'	PPS1 til PPS3 findes ikke; '00h' for at vælge T0, '01h' for at vælge T1.
PK	'XXh'	Kontroltegn: 'Xh' = 'FFh', hvis PPS0 = '00h' 'XXh' = 'FEh', hvis PPS0 = '01h'

▼B

3.3. **Adgangsregler**

TCS_22 I en adgangsregel specificeres sikkerhedsbetingelserne for en adgangstilstand, dvs. en kommando. Hvis disse sikkerhedsbetingelser er opfyldt, behandles den tilsvarende kommando.

TCS_23 Følgende sikkerhedsbetingelser bruges for takografkortet:

Forkortelse	Betydning
ALW	Operationen er altid mulig og kan udføres uden begrænsning. APDU-kommandoer og -svar sendes som almindelig tekst, dvs. uden sikker meddelelsesoverførsel.
NEV	Operationen er aldrig mulig.
PLAIN-C	Kommandoen APDU sendes som almindelig tekst, dvs. uden sikker meddelelsesoverførsel.
PWD	Handlingen kan kun udføres, hvis værkstedskortets PIN-kode er blevet kontrolleret med tilfredsstillende resultat, dvs. hvis kortets interne sikkerhedsstatus ”PIN_Verified” er angivet. Kommandoen skal sendes uden sikker meddelelsesoverførsel.
EXT-AUT-G1	Handlingen kan kun udføres, hvis kommandoen External Authenticate for ægthedsbekræftelse (første generation) (se også tillæg 11, del A) er gennemført med tilfredsstillende resultat.
SM-MAC-G1	APDU (kommando og svar) skal anvendes ved sikker meddelelsesoverførsel (første generation) i ”authentication-only”-tilstand (se tillæg 11, del A).
SM-C-MAC-G1	Kommandoen APDU skal anvendes ved sikker meddelelsesoverførsel (første generation) i ”authentication-only”-tilstand (se tillæg 11, del A).
SM-R-ENC-G1	Svaret APDU skal anvendes ved sikker meddelelsesoverførsel (første generation) i krypteringstilstand (se tillæg 11, del A), dvs. der tilbagemeldes ingen meddelelsesgodkendelseskode.
SM-R-ENC-MAC-G1	Kommandoen APDU skal anvendes ved sikker meddelelsesoverførsel (første generation) i ”encrypt-then-authenticate”-tilstand (se tillæg 11, del A).
SM-MAC-G2	APDU (kommando og svar) skal anvendes ved sikker meddelelsesoverførsel (anden generation) i ”authentication-only”-tilstand (se tillæg 11, del B).
SM-C-MAC-G2	Kommandoen APDU skal anvendes ved sikker meddelelsesoverførsel (anden generation) i ”authentication-only”-tilstand (se tillæg 11, del B).
SM-R-ENC-MAC-G2	Kommandoen APDU skal anvendes ved sikker meddelelsesoverførsel (anden generation) i ”encrypt-then-authenticate”-tilstand (se tillæg 11, del A).

TCS_24 Disse sikkerhedsbetingelser kan kædes sammen på følgende måder:

AND: Alle sikkerhedsbetingelser skal være opfyldt

OR: Mindst én sikkerhedsbetingelse skal være opfyldt

Adgangsreglerne for filsystemet, dvs. kommandoerne SELECT, READ BINARY og UPDATE BINARY, er nærmere beskrevet i afsnit 4. Adgangsreglerne for de resterende kommandoer er nærmere beskrevet i følgende tabeller.

▼B

TCS_25 I applikationen DF Tachograph G1 anvendes følgende adgangsregler:

Kommando	Førerkort	Værkstedskort	Kontrolkort	Virksomheds-kort
External Authenticate				
— For ægthedsbekræftelse (første generation)	ALW	ALW	ALW	ALW
— For ægthedsbekræftelse (anden generation)	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	Ikke relevant	Ikke relevant	Ikke relevant	Ikke relevant
PSO: Compute Digital Signature	ALW OR SM-MAC-G2	ALW OR SM-MAC-G2	Ikke relevant	Ikke relevant
PSO: Hash	Ikke relevant	Ikke relevant	ALW	Ikke relevant
PSO: Hash of File	ALW OR SM-MAC-G2	ALW OR SM-MAC-G2	Ikke relevant	Ikke relevant
PSO: Verify Certificate	ALW	ALW	ALW	ALW
PSO: Verify Digital Signature	Ikke relevant	Ikke relevant	ALW	Ikke relevant
Verify	Ikke relevant	ALW	Ikke relevant	Ikke relevant

TCS_26 I applikationen DF Tachograph_G2 anvendes følgende adgangsregler:

Kommando	Førerkort	Værkstedskort	Kontrolkort	Virksomheds-kort
External Authenticate				
— For ægthedsbekræftelse (første generation)	Ikke relevant	Ikke relevant	Ikke relevant	Ikke relevant
— For ægthedsbekræftelse (anden generation)	ALW	PWD	ALW	ALW
Internal Authenticate	Ikke relevant	Ikke relevant	Ikke relevant	Ikke relevant

▼B

Kommando	Førerkort	Værkstedskort	Kontrolkort	Virksomheds-kort
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	Ikke relevant	ALW	ALW	Ikke relevant
PSO: Compute Digital Signature	ALW OR SM-MAC-G2	ALW OR SM-MAC-G2	Ikke relevant	Ikke relevant
PSO: Hash	Ikke relevant	Ikke relevant	ALW	Ikke relevant
PSO: Hash of File	ALW OR SM-MAC-G2	ALW OR SM-MAC-G2	Ikke relevant	Ikke relevant
PSO: Verify Certificate	ALW	ALW	ALW	ALW
PSO: Verify Digital Signature	Ikke relevant	Ikke relevant	ALW	Ikke relevant
Verify	Ikke relevant	ALW	Ikke relevant	Ikke relevant

TCS_27 I hovedfilen anvendes følgende adgangsregler:

Kommando	Førerkort	Værkstedskort	Kontrolkort	Virksomheds-kort
External Authenticate				
— For ægthedsbekræftelse (første generation)	Ikke relevant	Ikke relevant	Ikke relevant	Ikke relevant
— For ægthedsbekræftelse (anden generation)	ALW	PWD	ALW	ALW
Internal Authenticate	Ikke relevant	Ikke relevant	Ikke relevant	Ikke relevant
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	Ikke relevant	Ikke relevant	Ikke relevant	Ikke relevant

▼B

Kommando	Førerkort	Værkstedskort	Kontrolkort	Virksomheds-kort
PSO: Compute Digital Signature	Ikke relevant	Ikke relevant	Ikke relevant	Ikke relevant
PSO: Hash	Ikke relevant	Ikke relevant	Ikke relevant	Ikke relevant
PSO: Hash of File	Ikke relevant	Ikke relevant	Ikke relevant	Ikke relevant
PSO: Verify Certificate	ALW	ALW	ALW	ALW
Verify	Ikke relevant	ALW	Ikke relevant	Ikke relevant

TCS_28 Et takografkort kan enten acceptere en kommando med et højere sikkerhedsniveau end niveauet i sikkerhedsbetingelserne eller ikke gøre det. Hvis sikkerhedsbetingelsen er ALW (eller PLAIN-C), kan kortet således acceptere en kommando med sikker meddelelsesoverførsel (kryptering og/eller ægthedsbekræftelsestilstand). Hvis sikkerhedsbetingelsen kræver sikker meddelelsesoverførsel i ægthedsbekræftelsestilstand, kan takografkortet acceptere en kommando med sikker meddelelsesoverførsel af samme generation i ægthedsbekræftelses- og krypteringstilstand.

Bemærk: I kommandobeskrivelserne findes der flere oplysninger om, ihvilket omfang kommandoerne understøtter de forskellige takografkorttyper og dedikerede filer.

3.4. **Oversigt over kommandoer og fejlkoder**

Kommandoer og filorganisation er afledt af og i overensstemmelse med ISO/IEC 78164.

I dette afsnit beskrives følgende APDU-kommando-svar-par. De kommandovarianter, der understøttes af en applikation af første eller anden generation, er nærmere beskrevet i de tilsvarende kommandobeskrivelser.

Kommando	INS
SELECT	‘A4h’
READ BINARY	‘B0h’, ‘B1h’
UPDATE BINARY	‘D6h’, ‘D7h’
GET CHALLENGE	‘84h’
VERIFY	‘20h’
GET RESPONSE	‘C0h’
PERFORM SECURITY OPERATION	‘2Ah’

▼B

Kommando	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 Statusordene SW1 SW2 tilbagemeldes sammen med enhver svarmeddelelse og angiver behandlingsstatus for kommandoen.

SW1	SW2	Betydning
90	00	Normal behandling af data.
61	XX	Normal behandling af data. XX = antal svarbytes til rådighed
62	81	Advarselsbehandling. En del af svardata kan være beskadiget
63	00	Ægthedsbekræftelse mislykkedes (advarsel)
63	CX	Forkert CHV (kortindehaververifikation, PIN). Indholdet i tæller for resterende forsøg tilbagemeldes med ‘X’
64	00	Kørselsfejl — Status for ikke-flygtigt lager uændret. Integritetsfejl.
65	00	Kørselsfejl — Status for ikke-flygtigt lager ændret.
65	81	Kørselsfejl — Status for ikke-flygtigt lager ændret. Hukommelsesfejl
66	88	Sikkerhedsfejl: forkert kryptografisk kontrolsum (ved sikker meddelelsesoverførsel) eller forkert certifikat (ved verifikation af certifikat) eller forkert kryptogram (ved ekstern ægthedsbekræftelse) eller forkert underskrift (ved verifikation af underskrift)
67	00	Forkert længde (forkert Lc eller Le)

▼B

SW1	SW2	Betydning
68	82	Sikker overførsel understøttes ikke
68	83	Sidste kommando i den forventede kæde
69	00	Forbudt kommando (intet svar foreligger i T = 0)
69	82	Sikkerhedsstatus ikke tilfredsstillet
69	83	Ægthedsbekræftelse blokeret
69	85	Betingelser for anvendelse ikke opfyldt
69	86	Kommando ikke tilladt (ingen aktuel elementærfil)
69	87	Forventede dataobjekter for sikker meddelelsesoverførsel mangler
69	88	Ukorrekte dataobjekter for sikker meddelelsesoverførsel
6A	80	Ukorrekte parametre i datafelt
6A	82	Filer ikke fundet
6A	86	Forkerte parametre P1-P2
6A	88	De adresserede data kunne ikke findes
6B	00	Forkerte parametre (adressetillæg uden for elementærfil)
6C	XX	Forkert længde, SW2 angiver eksakt længde. Intet datafelt tilbagemeldes
6D	00	Operationskode ikke understøttet eller ugyldig
6E	00	Klasse ikke understøttet
6F	00	Andre kontrolfejl

TCS_30 Hvis mere end én fejlbetingelse er opfyldt i en kommando-APDU kan kortet tilbagemelde ethvert af de passende statusord.

3.5. **Kommandobeskrivelser**

Påbudte kommandoer for takografkort er beskrevet i dette kapitel.

Supplerende relevante enkeltheder om de anvendte kryptografiske operationer er givet i tillæg 11 (fælles sikkerhedsmekanismer) for takografer af første og anden generation.

Alle kommandoer beskrives uafhængigt af den anvendte protokol (T = 0 eller T = 1). APDU-bytene CLA, INS, P1, P2, Lc og Le bliver altid angivet. Hvis Lc eller Le ikke er nødvendig for den beskrevne kommando, er den tilhørende længde, værdi og beskrivelse tomme.

TCS_31 Anmodes der om begge længdebytes (Lc og Le), skal den beskrevne kommando deles i to dele, hvis kortlæseren bruger protokol T = 0: Kortlæseren sender kommandoen som beskrevet ved hjælp af P3 = Lc + data og sender derefter en GET RESPONSE (se punkt 3.5.6) kommando med P3 = Le.

TCS_32 Anmodes der om begge længdebytes, og Le = 0 (sikker meddelelsesoverførsel):

▼B

— når der bruges protokol T = 1, skal kortet svare på Le = 0 ved at sende alle tilgængelige uddata

— når protokol T = 0 anvendes, skal kortlæseren sende den første kommando med P3 = Lc + data, kortet skal (på det implicitte Le = 0) svare med statusbytes '**61La**', hvor La er antal svarbytes til rådighed. Kortlæseren skal derefter generere en GET RESPONSE-kommando med P3 = La for at læse data.

TCS_33 Takografkort kan understøtte felter med udvidet længde i overensstemmelse med ISO/IEC 7816-4 som en valgfri funktion. Et takografkort, som understøtter felter med udvidet længde, skal

— angive, at felter med udvidet længde understøttes, i ATR

— angive de understøttede bufferstørrelser ved hjælp af oplysningerne med udvidet længde i elementærfilen ATR/INFO, se TCS_146

— angive, om det understøtter felter med udvidet længde for T = 1 og/eller T = 0, i elementærfilen Extended Length, se TCS_147

— understøtte felter med udvidet længde for takografapplikationer af første og anden generation.

Bemærkninger:

Alle kommandoer beskrives nærmere for felter med kort længde. Brug af APDU'er med udvidet længde beskrives i ISO/IEC 7816-4.

Generelt anføres kommandoerne for ordinær funktionstilstand, dvs. uden sikker meddelelsesoverførsel, da laget til sikker meddelelsesoverførsel er nærmere beskrevet i tillæg 11. Det fremgår klart af adgangsreglerne for en kommando, om kommandoen skal understøtte sikker meddelelsesoverførsel eller ej, og om den skal understøtte sikker meddelelsesoverførsel for første og/eller anden generation. En række kommandovarianter beskrives med hensyn til sikker meddelelsesoverførsel for at illustrere brugen af sikker meddelelsesoverførsel.

TCS_34 Køretøjsenheden skal gennemføre hele den fælles ægthedsbekræftelsesprotokol for køretøjsenheder og kort af anden generation for en session, herunder (om nødvendigt) certifikatverificeringen — enten i DF Tachograph, DF Tachograph_G2 eller hovedfilen.

3.5.1 *SELECT*

Denne kommando overholder ISO/IEC 7816-4, men har begrænset anvendelse i forhold til den i normen definerede kommando.

SELECT-kommandoen anvendes:

— til at vælge en applikationsdedikeret fil (skal vælges med navn)

— til at vælge en elementærfil svarende til det forelagte filnavn.

3.5.1.1 Valg ved navn (AID)

Med denne kommando kan der vælges en applikationsdedikeret fil på kortet.

TCS_35 Denne kommando kan udføres fra et vilkårligt sted i filstrukturen (efter svar på nulstilling (ATR) eller på et vilkårligt tidspunkt).

▼B

TCS_36 Når der vælges en applikation, bliver det aktuelle sikkerhedsmiljø nulstillet. Efter valget af applikationen er der ikke længere valgt nogen aktuel offentlig nøgle. Adgangsbetingelsen EXT-AUT-G1 mistes ligeledes. Hvis kommandoen blev udført uden sikker meddelelsesoverførsel, er de tidligere sessionsnøgler til sikker meddelelsesoverførsel ikke længere til rådighed.

TCS_37 **Kommandomeddelelse**

Byte	Længde	Værdi	Beskrivelse
CLA	1	‘00h’	
INS	1	‘A4h’	
P1	1	‘04h’	Valg ved navn (AID)
P2	1	‘0Ch’	Intet svar forventet
Lc	1	‘NNh’	Antal byte sendt til kortet (længde af AID): ‘06h’ for takografapplikationen
#6-#(5+NN)	NN	‘XX..XXh’	AID: ‘FF 54 41 43 48 4F’ for takografapplikationen af første generation AID: ‘FF 53 4D 52 44 54’ for takografapplikationen af anden generation

Der kræves intet svar på kommandoen SELECT (Le findes ikke i T = 1, eller der anmodes ikke om svar i T = 0).

TCS_38 **Svarmeddelelse (der er ikke anmodet om svar)**

Byte	Længde	Værdi	Beskrivelse
SW	2	‘XXXXh’	Statusord (SW1, SW2)

— Giver kommandoen resultat, tilbagemelder kortet ‘**9000**’.

— Hvis den applikation, som svarer til applikationsnavnet, ikke findes, tilbagemeldes status ‘**6A82**’.

— Hvis byten Le er til stede i T = 1, tilbagemeldes status ‘**6700**’.

— Hvis der i T = 0 anmodes om et svar efter SELECT-kommandoen, tilbagemeldes status ‘**6900**’.

— Hvis den valgte applikation anses for beskadiget (der er fundet integritetsfejl i filattributterne), tilbagemeldes status ‘**6400**’ eller ‘**6581**’.

3.5.1.2 Valg af en elementærfil ved hjælp af filnavnet

TCS_39 **Kommandomeddelelse**

TCS_40 Takografkort skal understøtte sikker meddelelsesoverførsel (anden generation) som foreskrevet i tillæg 11, del B for denne kommandovariant.

Byte	Længde	Værdi	Beskrivelse
CLA	1	‘00h’	
INS	1	‘A4h’	
P1	1	‘02h’	Valg af en elementærfil under den aktuelle dedikerede fil

▼B

Byte	Længde	Værdi	Beskrivelse
P2	1	‘0Ch’	Intet svar forventet
Lc	1	‘02h’	Antal bytes sendt til kortet
#6-#7	2	‘XXXXh’	Filnavn

Der kræves intet svar på kommandoen SELECT (Le findes ikke i T = 1, eller der anmodes ikke om svar i T = 0).

TCS_41 **Svarmeddelelse (der er ikke anmodet om svar)**

Byte	Længde	Værdi	Beskrivelse
SW	2	‘XXXXh’	Statusord (SW1, SW2)

— Giver kommandoen resultat, tilbagemelder kortet ‘**9000**’.

— Hvis filen svarende til det pågældende filnavn ikke findes, tilbagemeldes status ‘**6A82**’.

— Hvis byten Le er til stede i T = 1, tilbagemeldes status ‘**6700**’.

— Hvis der i T = 0 anmodes om et svar efter SELECT-kommandoen, tilbagemeldes status ‘**6900**’.

— Hvis den valgte fil anses for beskadiget (der er fundet integritetsfejl i filattributterne), tilbagemeldes status ‘**6400**’ eller ‘**6581**’.

3.5.2 *READ BINARY*

Denne kommando overholder ISO/IEC 7816-4, men har begrænset anvendelse i forhold til den i normen definerede kommando.

Kommandoen READ BINARY anvendes til at læse data fra en transparent fil.

Kortets svar består i at tilbagemelde de læste data, om ønsket indkapslet i en sikker meddelelsesstruktur.

3.5.2.1 Kommando med forskydning i P1-P2

Denne kommando giver kortlæseren mulighed for uden sikker meddelelsesoverførsel at læse data fra den aktuelt valgte elementærfil.

Bemærk: Denne kommando uden sikker meddelelsesoverførsel kan kun bruges til at læse en fil, som understøtter sikkerhedsbetingelsen ALW for læseadgangstilstand.

TCS_42 **Kommandomeddelelse**

Byte	Længde	Værdi	Beskrivelse
CLA	1	‘00h’	
INS	1	‘B0h’	Read Binary
P1	1	‘XXh’	Forskydning i bytes fra filens begyndelse: Mest betydende byte

▼B

Byte	Længde	Værdi	Beskrivelse
P2	1	'XXh'	Forskydning i bytes fra filens begyndelse: Mindst betydende byte
Le	1	'XXh'	Forventet datalængde. Antal bytes, som skal læses.

Bemærk: bit 8 af P1 skal være sat til 0.

TCS_43 **Svarmeddelelse**

Byte	Længde	Værdi	Beskrivelse
#1-#X	X	'XX..XXh'	Data læst
SW	2	'XXXXh'	Statusord (SW1, SW2)

— Giver kommandoen resultat, tilbagemelder kortet '**9000**'.

— Vælges ingen elementærfil, tilbagemeldes behandlingsstatus '**6986**'.

— Er sikkerhedsbetingelserne for den valgte fil ikke opfyldt, afbrydes kommandoen med '**6982**'.

— Er forskydningen ikke forenelig med elementærfilens størrelse (forskydning > størrelse af EF), tilbagemeldes status '**6B00**'.

— Er størrelsen af de data, der skal læses, ikke forenelig med elementærfilens størrelse (forskydning + Le > størrelsen af EF), tilbagemeldes status '**6700**' eller '**6Cxx**', hvor 'xx' er den eksakte længde.

— Konstateres der en integritetsfejl i filattributterne, skal kortet anse filen for uoprettelig beskadiget, og den tilbagemeldte behandlingsstatur er '**6400**' eller '**6581**'.

— Konstateres der en integritetsfejl i de lagrede data, skal kortet tilbagemelde de ønskede data, og der tilbagemeldes status '**6281**'.

3.5.2.1.1 Kommando med sikker meddelelsesoverførsel (eksempler)

Denne kommando giver IDF mulighed for at læse data fra den aktuelt valgte elementærfil med sikkert meddelelsessystem, med det formål at efterprøve identiteten af de modtagne data og beskytte fortroligheden af data, hvis sikkerhedsbetingelsen SM-R-ENC-MAC-G1 (første generation) eller SM-R-ENC-MAC-G2 (anden generation) gælder.

TCS_44 **Kommandomeddelelse**

Byte	Længde	Værdi	Beskrivelse
CLA	1	'0Ch'	Der er anmodet om sikker meddelelsesoverførsel
INS	1	'B0h'	Read Binary
P1	1	'XXh'	P1 (forskydning i bytes fra filens begyndelse): Mest betydende byte
P2	1	'XXh'	P2 (forskydning i bytes fra filens begyndelse): Mindst betydende byte

▼B

Byte	Længde	Værdi	Beskrivelse
Lc	1	'XXh'	Længde af inddata til sikker meddelelse
#6	1	'97h'	T_{LE}: Etiket for angivelse af forventet længde
#7	1	'01h'	L_{LE}: Forventet længde
#8	1	'NNh'	Angivelse af forventet længde (oprindelig Le): Antal bytes, som skal læses
#9	1	'8Eh'	T_{CC}: Etiket for kryptografisk kontrolsum
#10	1	'XXh'	L_{CC}: Længde af efterfølgende kryptografiske kontrolsum '04h' for sikker meddelelsesoverførsel (første generation) (se tillæg 11, del A) '08h', '0Ch' eller '10h' afhængigt af AES-nøglelængden for sikker meddelelsesoverførsel (anden generation) (se tillæg 11, del B)
#11-#(10+L)	L	'XX..XXh'	Kryptografisk kontrolsum
Le	1	'00h'	Som foreskrevet i ISO/IEC 7816-4

TCS_45 **Svarmeddelelse, hvis SM-R-ENC-MAC-G1 (første generation) / SM-R-ENC-MAC-G2 (anden generation) ikke kræves, og hvis inddataformatet for sikker overførsel er korrekt:**

Byte	Længde	Værdi	Beskrivelse
#1	1	'99h'	Etiket til behandlingsstatus (SW1-SW2) — valgfri for sikker meddelelsesoverførsel (første generation)
#2	1	'02h'	Behandlingsstatussens længde
#3-#4	2	'XX XXh'	Behandlingsstatus for det ubeskyttede APDU-svar
#5	1	'81h'	T_{PV}: Etiket for data med ordinær værdi
#6	L	'NNh' eller '81 NNh'	L_{PV}: længde af tilbagemeldte data (= original Le). L er 2 bytes, hvis L_{PV}>127 bytes.
#(6+L)-#(5+L+NN)	NN	'XX..XXh'	Ordinær dataværdi
#(6+L+NN)	1	'8Eh'	T_{CC}: Etiket for kryptografisk kontrolsum
#(7+L+NN)	1	'XXh'	L_{CC}: Længde af efterfølgende kryptografiske kontrolsum '04h' for sikker meddelelsesoverførsel (første generation) (se tillæg 11, del A) '08h', '0Ch' eller '10h' afhængigt af AES-nøglelængden for sikker meddelelsesoverførsel (anden generation) (se tillæg 11, del B)
#(8+L+NN)-#(7+M+L+N-N)	M	'XX..XXh'	Kryptografisk kontrolsum
SW	2	'XXXXh'	Statusord (SW1, SW2)

▼B

TCS_46 **Svarmeddelelse, hvis SM-R-ENC-MAC-G1 (første generation) / SM-R-ENC-MAC-G2 (anden generation) kræves, og hvis inddataformatet for sikker overførsel er korrekt:**

Byte	Længde	Værdi	Beskrivelse
#1	1	'87h'	$T_{PI\ CG}$: Etiket for krypterede data (kryptogram)
#2	L	'MMh' eller '81 MMh'	$L_{PI\ CG}$: længde af tilbagemeldte krypterede data (afviger pga. udfyldning fra kommandoens oprindelige længde Le). L er 2 bytes, hvis $L_{PI\ CG}$ > 127 bytes.
#(2+L)-#(1+L+MM)	MM	'01XX..XXh'	Krypterede data: Udfyldningsindikator og kryptogram
#(2+L+MM)	1	'99h'	Etiket til behandlingsstatus (SW1-SW2) — valgfri for sikker meddelelsesoverførsel (første generation)
#(3+L+MM)	1	'02h'	Behandlingsstatussens længde
#(4+L+MM)-#(5+L+MM)	2	'XX XXh'	Behandlingsstatus for det ubeskyttede APDU-svar
#(6+L+MM)	1	'8Eh'	T_{CC}: Etiket for kryptografisk kontrolsum
#(7+L+MM)	1	'XXh'	L_{CC}: Længde af efterfølgende kryptografiske kontrolsum '04h' for sikker meddelelsesoverførsel (første generation) (se tillæg 11, del A) '08h', '0Ch' eller '10h' afhængigt af AES-nøglelængden for sikker meddelelsesoverførsel (anden generation) (se tillæg 11, del B)
#(8+L+MM)-#(7+N+L+MM)	N	'XX..XXh'	Kryptografisk kontrolsum
SW	2	'XXXXh'	Statusord (SW1, SW2)

Kommandoen READ BINARY kan tilbagemelde de ordinære behandlingsstatusser, der er anført i TCS_43 under etiket '99h' som beskrevet i TCS_59 ved brug af svarstrukturen for sikker meddelelsesoverførsel.

Derudover kan der optræde visse fejl, som særligt vedrører sikker meddelelsesoverførsel. I så fald tilbagemeldes behandlingsstatus simpelthen, uden at nogen struktur for sikker meddelelsesoverførsel er inddraget:

TCS_47 **Svarmeddelelse, hvis det indlæste format for sikker meddelelsesoverførsel er ukorrekt**

Byte	Længde	Værdi	Beskrivelse
SW	2	'XXXXh'	Statusord (SW1, SW2)

— Foreligger der ingen nøgle for den aktuelle session, tilbagemeldes behandlingsstatus '**6A88**'. Dette sker, hvis sessionsnøglen enten ikke er genereret i forvejen eller er blevet ugyldig (i så fald skal kortlæseren på ny udføre den gensidige ægthedsbekræftelse, så der fastsættes en ny sessionsnøgle).

▼B

— Hvis der mangler nogle forventede dataobjekter (som ovenfor specificeret) i formatet for sikker meddelelsesoverførsel, tilbagemeldes behandlingsstatus '**6987**': Denne fejl opstår, hvis der mangler en forventet etiket, eller hvis kommandoen ikke er korrekt opbygget.

— Hvis nogle dataobjekter er ukorrekte, tilbagemeldes status '**6988**': Denne fejl optræder, når alle de nødvendige etiketter er til stede, men visse af længderne ikke svarer til de forventede.

— Lykkes verifikationen af den kryptografiske kontrolsum ikke, tilbagemeldes behandlingsstatus '**6688**'.

3.5.2.2 Kommando med kort id for elementærfil

Denne kommandovariant giver kortlæseren mulighed for at vælge en elementærfil ved hjælp af et kort id for elementærfilen og læse data fra filen.

TCS_48 Et takografkort skal understøtte denne kommandovariant for alle elementærfiler med et fastsat kort id for elementærfilen. Disse korte id'er for elementærfiler er nærmere beskrevet i afsnit 4.

TCS_49 **Kommandomeddelelse**

Byte	Længde	Værdi	Beskrivelse
CLA	1	'00h'	
INS	1	'B0h'	Read Binary
P1	1	'XXh'	Bit 8 er sat til 1 Bit 7 og 6 er sat til 00 Bit 5-1 koder det korte id for den tilsvarende elementærfil
P2	1	'XXh'	Koder en forskydning fra 0 til 255 bytes i den elementærfil, som P1 henviser til
Le	1	'XXh'	Forventet datalængde. Antal bytes, som skal læses.

Bemærk: De korte id'er for elementærfiler, der anvendes til takografapplikationen af anden generation, er nærmere beskrevet i afsnit 4.

Hvis P1 koder et kort id for en elementærfil, og kommandoen giver resultat, bliver den identificerede elementærfil til den aktuelt valgte elementærfil (den aktuelle elementærfil).

TCS_50 **Svarmeddelelse**

Byte	Længde	Værdi	Beskrivelse
#1-#L	L	'XX..XXh'	Data læst
SW	2	'XXXXh'	Statusord (SW1, SW2)

— Giver kommandoen resultat, tilbagemelder kortet '**9000**'.

— Hvis filen svarende til det korte id for elementærfilen ikke findes, tilbagemeldes status '**6A82**'.

— Er sikkerhedsbetingelserne for den valgte fil ikke opfyldt, afbrydes kommandoen med '**6982**'.

▼B

— Er forskydningen ikke forenelig med elementærfilens størrelse (forskydning > størrelse af EF), tilbagemeldes status '**6B00**'.

— Er størrelsen af de data, der skal læses, ikke forenelig med elementærfilens størrelse (forskydning + Le > størrelsen af EF), tilbagemeldes status '**6700**' eller '**6Cxx**', hvor 'xx' er den eksakte længde.

— Konstateres der en integritetsfejl i filattributterne, skal kortet anse filen for uoprettelig beskadiget, og den tilbagemeldte behandlingsstatur er '**6400**' eller '**6581**'.

— Konstateres der en integritetsfejl i de lagrede data, skal kortet tilbagemelde de ønskede data, og der tilbagemeldes status '**6281**'.

3.5.2.3 Kommando med ulige ordrebyte

Denne kommandovariant giver kortlæseren mulighed for at læse data fra en elementærfil med 32 768 bytes eller derover.

TCS_51 Takografkort, som understøtter elementærfiler med 32 768 bytes eller derover, skal understøtte denne kommandovariant for disse elementærfiler. Et takografkort kan eventuelt understøtte denne kommandovariant for andre elementærfiler med undtagelse af elementærfilen Sensor_Installation_Data. Se TCS_156 og TCS_160.

TCS_52 **Kommandomeddelelse**

Byte	Længde	Værdi	Beskrivelse
CLA	1	'00h'	
INS	1	'B1h'	Read Binary
P1	1	'00h'	Aktuel elementærfil
P2	1	'00h'	
Lc	1	'NNh'	Lc Længde af forskydningsdataobjekt.
#6-#(5+NN)	NN	'XX..XXh'	Forskydningsdataobjekt: Etiket '54h' Længde '01h' eller '02h' Værdi forskudt
Le	1	'XXh'	Antal bytes, som skal læses.

Kortlæseren skal kode længden på forskydningsdataobjektet med det mindst mulige antal oktetter. For eksempel skal kortlæseren ved brug af længdebyten '01h' kode en forskydning fra 0 til 255, og ved brug af længdebyten '02h' skal den kode en forskydning fra '256' op til '65 535' bytes.

TCS_53 **Svarmeddelelse**

Byte	Længde	Værdi	Beskrivelse
#1-#L	L	'XX..XXh'	Læste data, der er indkapslet i et objekt med yderligere data med etiketten '53h'.
SW	2	'XXXXh'	Statusord (SW1, SW2)

▼B

— Giver kommandoen resultat, tilbagemelder kortet '**9000**'.

— Vælges ingen elementærfil, tilbagemeldes behandlingsstatus '**6986**'.

— Er sikkerhedsbetingelserne for den valgte fil ikke opfyldt, afbrydes kommandoen med '**6982**'.

— Er forskydningen ikke forenelig med elementærfilens størrelse (forskydning > størrelse af EF), tilbagemeldes status '**6B00**'.

— Er størrelsen af de data, der skal læses, ikke forenelig med elementærfilens størrelse (forskydning + Le > størrelsen af EF), tilbagemeldes status '**6700**' eller '**6Cxx**', hvor 'xx' er den eksakte længde.

— Konstateres der en integritetsfejl i filattributterne, skal kortet anse filen for uoprettelig beskadiget, og den tilbagemeldte behandlingsstatur er '**6400**' eller '**6581**'.

— Konstateres der en integritetsfejl i de lagrede data, skal kortet tilbagemelde de ønskede data, og der tilbagemeldes status '**6281**'.

3.5.2.3.1 Kommando med sikker meddelelsesoverførsel (eksempler)

Kommando med sikker meddelelsesoverførsel (eksempler)Følgende eksempel viser brug af sikker meddelelsesoverførsel, hvis sikkerhedsbetingelsen SM-MAC-G2 gælder.

TCS_54 Kommandomeddelelse

Byte	Længde	Værdi	Beskrivelse
CLA	1	'0Ch'	Der er anmodet om sikker meddelelsesoverførsel
INS	1	'B1h'	Read Binary
P1	1	'00h'	Aktuel elementærfil
P2	1	'00h'	
Lc	1	'XXh'	Længde af det sikrede datafelt
#6	1	'B3h'	Etiket for data med ordinær værdi, der er kodet i BER-TLV
#7	1	'NNh'	L_{PV}: længde af overførte data
#(8)-#(7+NN)	NN	'XX..XXh'	Ordinære data, der er kodet i BER-TLV, dvs. forskydningsdataobjektet med etiket '54'
#(8+NN)	1	'97h'	T_{LE}: Etiket for angivelse af forventet længde
#(9+NN)	1	'01h'	L_{LE}: Forventet længde
#(10+NN)	1	'XXh'	Angivelse af forventet længde (oprindelig Le): Antal bytes, som skal læses
#(11+NN)	1	'8Eh'	T_{CC}: Etiket for kryptografisk kontrolsum
#(12+NN)	1	'XXh'	L_{CC}: Længde af efterfølgende kryptografiske kontrolsum '08h', '0Ch' eller '10h' afhængigt af AES-nøglelængden for sikker meddelelsesoverførsel (anden generation) (se tillæg 11, del B)
#(13+NN)-#(12+M+NN)	M	'XX..XXh'	Kryptografisk kontrolsum
Le	1	'00h'	Som foreskrevet i ISO/IEC 7816-4

▼B

TCS_55 Svarmeddelelse, hvis kommandoen giver resultat

Byte	Længde	Værdi	Beskrivelse
#1	1	'B3h'	Ordinære data kodet i BER-TLV
#2	L	'NNh' eller '81 NNh'	L_{PV}: længde af tilbagemeldte data (= original Le). L er 2 bytes, hvis L_{PV} > 127 bytes.
#(2+L)-#(1+L+NN)	NN	'XX..XXh'	Ordinære data, der er kodet i BER-TLV, dvs. indlæste data, som er indkapslet i et objekt med yderligere data med etiket '53h'.
#(2+L+NN)	1	'99h'	Behandlingsstatus for det ubeskyttede APDU-svar
#(3+L+NN)	1	'02h'	Behandlingsstatussens længde
#(4+L+NN)-#(5+L+NN)	2	'XX XXh'	Behandlingsstatus for det ubeskyttede APDU-svar
#(6+L+NN)	1	'8Eh'	T_{CC}: Etiket for kryptografisk kontrolsum
#(7+L+NN)	1	'XXh'	L_{CC}: Længde af efterfølgende kryptografiske kontrolsum '08h', '0Ch' eller '10h' afhængigt af AES-nøglelængden for sikker meddelelsesoverførsel (anden generation) (se tillæg 11, del B)
#(8+L+NN)-#(7+M+L+N-N)	M	'XX..XXh'	Kryptografisk kontrolsum
SW	2	'XXXXh'	Statusord (SW1, SW2)

3.5.3 *UPDATE BINARY*

Denne kommando overholder ISO/IEC 7816-4, men har begrænset anvendelse i forhold til den i normen definerede kommando.

Med kommandomeddelelsen UPDATE BINARY igangsættes opdatering (sletning + skrivning) af de bit, der i forvejen ligger i en binær elementærfil, med de bit, der er indeholdt i kommandoen APDU.

3.5.3.1 Kommando med forskydning i P1-P2

Denne kommando giver kortlæseren mulighed for at skrive data til den aktuelt valgte elementærfil, uden at kortet kontrollerer ægtheden af de modtagne data.

Bemærk: Denne kommando uden sikker meddelelsesoverførsel kan kun bruges til at opdatere en fil, som understøtter sikkerhedsbetingelsen ALW for opdateringsadgangstilstand.

TCS_56 **Kommandomeddelelse**

Byte	Længde	Værdi	Beskrivelse
CLA	1	'00h'	
INS	1	'D6h'	Update Binary
P1	1	'XXh'	Forskydning i bytes fra filens begyndelse: Mest betydende byte
P2	1	'XXh'	Forskydning i bytes fra filens begyndelse: Mindst betydende byte

▼B

Byte	Længde	Værdi	Beskrivelse
Lc	1	'NNh'	Længde af data, som skal opdateres. Antal bytes, som skal skrives
#6-#(5+NN)	NN	'XX..XXh'	Data, som skal skrives

Bemærk: bit 8 af P1 skal være sat til 0.

TCS_57 **Svarmeddelelse**

Byte	Længde	Værdi	Beskrivelse
SW	2	'XXXXh'	Statusord (SW1, SW2)

— Giver kommandoen resultat, tilbagemelder kortet '**9000**'.

— Vælges ingen elementærfil, tilbagemeldes behandlingsstatus '**6986**'.

— Er sikkerhedsbetingelserne for den valgte fil ikke opfyldt, afbrydes kommandoen med '**6982**'.

— Er forskydningen ikke forenelig med elementærfilens størrelse (forskydning > størrelse af EF), tilbagemeldes status '**6B00**'.

— Er størrelsen af de data, der skal skrives, ikke forenelig med elementærfilens størrelse (forskydning + Lc > størrelsen af EF), tilbagemeldes status '**6700**'.

— Konstateres der en integritetsfejl i filattributterne, skal kortet anse filen for uoprettelig beskadiget, og den tilbagemeldte behandlingsstatur er '**6400**' eller '**6500**'.

— Hvis der ikke kan skrives, tilbagemeldes behandlingsstatus '**6581**'.

3.5.3.1.1 Kommando med sikker meddelelsesoverførsel (eksempler)

Denne kommando giver kortlæseren mulighed for at skrive data til den aktuelt valgte elementærfil, idet kortet kontroller ægtheden af de modtagne data. Da der ikke kræves fortrolighed, er data ikke krypteret.

TCS_58 **Kommandomeddelelse**

Byte	Længde	Værdi	Beskrivelse
CLA	1	'0Ch'	Der er anmodet om sikker meddelelsesoverførsel
INS	1	'D6h'	Update Binary
P1	1	'XXh'	Forskydning i bytes fra filens begyndelse: Mest betydende byte
P2	1	'XXh'	Forskydning i bytes fra filens begyndelse: Mindst betydende byte
Lc	1	'XXh'	Længde af det sikrede datafelt
#6	1	'81h'	T_{PV}: Etiket for data med ordinær værdi
#7	L	'NNh' eller '81 NNh'	L_{PV}: længde af overførte data L er 2 bytes, hvis L_{PV} > 127 bytes.

▼B

Byte	Længde	Værdi	Beskrivelse
#(7+L)-#(6+L+NN)	NN	'XX..XXh'	Værdi af ordinære data (data, som skal skrives)
#(7+L+NN)	1	'8Eh'	T_{CC}: Etiket for kryptografisk kontrolsum
#(8+L+NN)	1	'XXh'	L_{CC}: Længde af efterfølgende kryptografiske kontrolsum '04h' for sikker meddelelsesoverførsel (første generation) (se tillæg 11, del A) '08h', '0Ch' eller '10h' afhængigt af AES-nøglelængden for sikker meddelelsesoverførsel (anden generation) (se tillæg 11, del B)
#(9+L+NN)-#(8+M+L+N-N)	M	'XX..XXh'	Kryptografisk kontrolsum
Le	1	'00h'	Som foreskrevet i ISO/IEC 7816-4

TCS_59 **Svarmeddelelse, hvis inddata har det korrekte format til sikker meddelelsesoverførsel**

Byte	Længde	Værdi	Beskrivelse
#1	1	'99h'	T_{SW}: Etiket for statusord (skal beskyttes af CC)
#2	1	'02h'	L_{SW}: længde af tilbagemeldte statusord
#3-#4	2	'XXXXh'	Behandlingsstatus for det ubeskyttede APDU-svar
#5	1	'8Eh'	T_{CC}: Etiket for kryptografisk kontrolsum
#6	1	'XXh'	L_{CC}: Længde af efterfølgende kryptografiske kontrolsum '04h' for sikker meddelelsesoverførsel (første generation) (se tillæg 11, del A) '08h', '0Ch' eller '10h' afhængigt af AES-nøglelængden for sikker meddelelsesoverførsel (anden generation) (se tillæg 11, del B)
#7-#(6+L)	L	'XX..XXh'	Kryptografisk kontrolsum
SW	2	'XXXXh'	Statusord (SW1, SW2)

De "ordinære" behandlingsstatusser, som beskrives for kommandoen UPDATE BINARY uden sikker meddelelsesoverførsel (se punkt 3.5.3.1), kan tilbagemeldes med den svarmeddelelsesstruktur, som er beskrevet ovenfor.

Derudover kan der optræde visse fejl, som særligt vedrører sikker meddelelsesoverførsel. I så fald tilbagemeldes behandlingsstatus simpelthen, uden at nogen struktur for sikker meddelelsesoverførsel er inddraget:

TCS_60 **Svarmeddelelse ved fejl i sikker meddelelsesoverførsel**

Byte	Længde	Værdi	Beskrivelse
SW	2	'XXXXh'	Statusord (SW1, SW2)

▼B

— Foreligger der ingen nøgle for den aktuelle session, tilbagemeldes behandlingsstatus '**6A88**'.

— Hvis der mangler nogle forventede dataobjekter (som ovenfor specificeret) i formatet for sikker meddelelsesoverførsel, tilbagemeldes behandlingsstatus '**6987**': Denne fejl opstår, hvis der mangler en forventet etiket, eller hvis kommandoen ikke er korrekt opbygget.

— Hvis nogle dataobjekter er ukorrekte, tilbagemeldes status '**6988**': Denne fejl optræder, når alle de nødvendige etiketter er til stede, men visse af længderne ikke svarer til de forventede.

— Lykkes verifikationen af den kryptografiske kontrolsum ikke, tilbagemeldes behandlingsstatus '**6688**'.

3.5.3.2 Kommando med kort id for elementærfil

Denne kommandovariant giver kortlæseren mulighed for at vælge en elementærfil ved hjælp af et kort id for elementærfilen og læse data fra filen.

TCS_61 Et takografkort skal understøtte denne kommandovariant for alle elementærfiler med et fastsat kort id for elementærfilen. Disse korte id'er for elementærfiler er nærmere beskrevet i afsnit 4.

TCS_62 **Kommandomeddelelse**

Byte	Længde	Værdi	Beskrivelse
CLA	1	'00h'	
INS	1	'D6h'	Update Binary
P1	1	'XXh'	Bit 8 er sat til 1 Bit 7 og 6 er sat til 00 Bit 5-1 koder det korte id for den tilsvarende elementærfil
P2	1	'XXh'	Koder en forskydning fra 0 til 255 bytes i den elementærfil, som P1 henviser til
Lc	1	'NNh'	Længde af data, som skal opdateres. Antal bytes, som skal skrives
#6-#(5+NN)	NN	'XX..XXh'	Data, som skal skrives

TCS_63 **Svarmeddelelse**

Byte	Længde	Værdi	Beskrivelse
SW	2	'XXXXh'	Statusord (SW1, SW2)

Bemærk: De korte id'er for elementærfiler, der anvendes til takografapplikationen af anden generation, beskrives nærmere i afsnit 4.

Hvis P1 koder et kort id for en elementærfil, og kommandoen giver resultat, bliver den identificerede elementærfil til den aktuelt valgte elementærfil (den aktuelle elementærfil).

▼B

— Giver kommandoen resultat, tilbagemelder kortet '**9000**'.

— Hvis filen svarende til det korte id for elementærfilen ikke findes, tilbagemeldes status '**6A82**'.

— Er sikkerhedsbetingelserne for den valgte fil ikke opfyldt, afbrydes kommandoen med '**6982**'.

— Er forskydningen ikke forenelig med elementærfilens størrelse (forskydning > størrelse af EF), tilbagemeldes status '**6B00**'.

— Er størrelsen af de data, der skal skrives, ikke forenelig med elementærfilens størrelse (forskydning + Lc > størrelsen af EF), tilbagemeldes status '**6700**'.

— Konstateres der en integritetsfejl i filattributterne, skal kortet anse filen for uoprettelig beskadiget, og den tilbagemeldte behandlingsstatur er '**6400**' eller '**6581**'.

— Hvis der ikke kan skrives, tilbagemeldes behandlingsstatus '**6581**'.

3.5.3.3 Kommando med ulige ordrebyte

Denne kommandovariant giver kortlæseren mulighed for at skrive data til en elementærfil med 32 768 bytes eller derover.

TCS_64 Takografkort, som understøtter elementærfiler med 32 768 bytes eller derover, skal understøtte denne kommandovariant for disse elementærfiler. Et takografkort kan eventuelt understøtte denne kommandovariant for andre elementærfiler.

TCS_65 **Kommandomeddelelse**

Byte	Længde	Værdi	Beskrivelse
CLA	1	'00h'	
INS	1	'D7h'	Update Binary
P1	1	'00h'	Aktuel elementærfil
P2	1	'00h'	
Lc	1	'NNh'	Lc Længde af data i kommandodatafeltet
#6-#(5+NN)	NN	'XX..XXh'	Forskydningsdataobjekt med etiket '54h' || Objekt med yderligere data med etiket '53h', der indkapsler de data, som skal skrives

Kortlæseren skal kode længden af forskydningsdataobjektet og længden af objektet med yderligere data med det mindst mulige antal oktetter. For eksempel skal kortlæseren ved brug af længdebyten '01h' kode en forskydning/længde fra 0 til 255, og ved brug af længdebyten '02h' skal den kode en forskydning/længde fra '256' op til '65 535' bytes.

TCS_66 **Svarmeddelelse**

Byte	Længde	Værdi	Beskrivelse
SW	2	'XXXXh'	Statusord (SW1, SW2)

▼B

— Giver kommandoen resultat, tilbagemelder kortet '**9000**'.

— Vælges ingen elementærfil, tilbagemeldes behandlingsstatus '**6986**'.

— Er sikkerhedsbetingelserne for den valgte fil ikke opfyldt, afbrydes kommandoen med '**6982**'.

— Er forskydningen ikke forenelig med elementærfilens størrelse (forskydning > størrelse af EF), tilbagemeldes status '**6B00**'.

— Er størrelsen af de data, der skal skrives, ikke forenelig med elementærfilens størrelse (forskydning + Lc > størrelsen af EF), tilbagemeldes status '**6700**'.

— Konstateres der en integritetsfejl i filattributterne, skal kortet anse filen for uoprettelig beskadiget, og den tilbagemeldte behandlingsstatur er '**6400**' eller '**6500**'.

— Hvis der ikke kan skrives, tilbagemeldes behandlingsstatus '**6581**'.

3.5.3.3.1 Kommando med sikker meddelelsesoverførsel (eksempler)

Kommando med sikker meddelelsesoverførsel (eksempler)Følgende eksempel viser brug af sikker meddelelsesoverførsel, hvis sikkerhedsbetingelsen SM-MAC-G2 gælder.

TCS_67 Kommandomeddelelse

Byte	Længde	Værdi	Beskrivelse
CLA	1	'0Ch'	Der er anmodet om sikker meddelelsesoverførsel
INS	1	'D7h'	Update Binary
P1	1	'00h'	Aktuel elementærfil
P2	1	'00h'	
Lc	1	'XXh'	Længde af det sikrede datafelt
#6	1	'B3h'	Etiket for data med ordinær værdi, der er kodet i BER-TLV
#7	L	'NNh' eller '81 NNh'	L_{PV}: længde af overførte data L er 2 bytes, hvis L_{PV}>127 bytes.
#(7+L)-#(6+L+NN)	NN	'XX..XXh'	Ordinære data kodet i BER-TLV, dvs. forskydningsdataobjekt med etiket '54h' || Objekt med yderligere data med etiket '53h', der indkapsler de data, som skal skrives
#(7+L+NN)	1	'8Eh'	T_{CC}: Etiket for kryptografisk kontrolsum
#(8+L+NN)	1	'XXh'	L_{CC}: Længde af efterfølgende kryptografiske kontrolsum '08h', '0Ch' eller '10h' afhængigt af AES-nøglelængden for sikker meddelelsesoverførsel (anden generation) (se tillæg 11, del B)
#(9+L+NN)-#(8+M+L+N-N)	M	'XX..XXh'	Kryptografisk kontrolsum
Le	1	'00h'	Som foreskrevet i ISO/IEC 7816-4

▼B

TCS_68 Svarmeddelelse, hvis kommandoen giver resultat

Byte	Længde	Værdi	Beskrivelse
#1	1	'99h'	T_{SW}: Etiket for statusord (skal beskyttes af CC)
#2	1	'02h'	L_{SW}: længde af tilbagemeldte statusord
#3-#4	2	'XXXXh'	Behandlingsstatus for det ubeskyttede APDU-svar
#5	1	'8Eh'	T_{CC}: Etiket for kryptografisk kontrolsum
#6	1	'XXh'	L_{CC}: Længde af efterfølgende kryptografiske kontrolsum '08h', '0Ch' eller '10h' afhængigt af AES-nøglelængden for sikker meddelelsesoverførsel (anden generation) (se tillæg 11, del B)
#7-#(6+L)	L	'XX..XXh'	Kryptografisk kontrolsum
SW	2	'XXXXh'	Statusord (SW1, SW2)

3.5.4 *GET CHALLENGE*

Denne kommando overholder ISO/IEC 7816-4, men har begrænset anvendelse i forhold til den i normen definerede kommando.

Med GET CHALLENGE-kommandoen beder man kortet afgive en challenge for at bruge den i en sikkerhedsrelateret procedure, hvori der sendes et kryptogram eller nogle kryptograferede data til kortet.

TCS_69 Den challenge, som afgives af kortet, er kun gyldig for den næste kommando, som anvender en challenge, som sendes til kortet.

TCS_70 **Kommandomeddelelse**

Byte	Længde	Værdi	Beskrivelse
CLA	1	'00h'	
INS	1	'84h'	INS
P1	1	'00h'	P1
P2	1	'00h'	P2
Le	1	'08h'	Le (forventet længde af challenge).

TCS_71 **Svarmeddelelse**

Byte	Længde	Værdi	Beskrivelse
#1-#8	8	'XX..XXh'	Udfordring
SW	2	'XXXXh'	Statusord (SW1, SW2)

— Giver kommandoen resultat, tilbagemelder kortet '**9000**'.

— Hvis længden Le er forskellig fra '08h', er behandlingsstatus '**6700**'.

— Hvis parametrene P1-P2 er ukorrekte, er behandlingsstatus '**6A86**'.

▼B

3.5.5 *VERIFY*

Denne kommando overholder ISO/IEC 7816-4, men har begrænset anvendelse i forhold til den i normen definerede kommando.

Kun værkstedskortet kræves for at understøtte denne kommando.

Andre slags takografkort kan muligvis udføre denne kommando, men for disse kort personaliseres ingen reference-CHV. Derfor kan disse kort ikke udføre denne kommando på tilfredsstillende vis. For så vidt angår andre slags takografkort end værkstedskort ligger deres adfærd (den returnerede fejlkode) uden for anvendelsesområdet for denne specifikation, hvis denne kommando sendes.

VERIFY-kommandoen får kortet til at sammenholde de CHV(PIN)data, som sendes med kommandoen, med kortindehaverens reference-CHV, som er gemt på kortet.

TCS_72 Den PIN, der er indlæst af brugeren, skal af kortlæseren være ASCI-kodet og udfyldt mod højre med 'FFh'-bytes til en længde af 8 bytes. Se også datatypen WorkshopCardPIN i tillæg 1.

TCS_73 Takografapplikationer af første og anden generation skal bruge den samme reference-CHV.

TCS_74 Takografkortet skal kontrollere, om kommandoen er kodet korrekt. Hvis kommandoen ikke er kodet korrekt, skal kortet ikke sammenligne CHV-værdierne, ikke nedbringe tælleren for resterende CHV-forsøg og ikke nulstille sikkerhedsstatussen "PIN_Verified", men derimod afbryde kommandoen. En kommando er kodet korrekt, hvis bytene CLA, INS, P1, P2 og Lc har de fastsatte værdier, Le ikke findes, og kommandoens datafelt har den korrekte længde.

TCS_75 Hvis kommandoen giver resultat, tilbagestilles tælleren for resterende CHV-forsøg. Tælleren for resterende CHV-forsøg starter på værdien 5. Hvis kommandoen giver resultat, skal kortet sætte den interne sikkerhedsstatus til "PIN_Verified". Kortet skal nulstille denne sikkerhedsstatus, hvis kortet selv nulstilles, eller hvis den CHV-kode, der overføres i kommandoen, ikke matcher den lagrede reference-CHV.

Bemærk: Ved at bruge den samme reference-CHV og en overordnet sikkerhedsstatus slipper værkstedsmedarbejderne for at skulle genindlæse PIN-koden efter at have valgt en anden dedikeret fil for takografapplikationen.

TCS_76 Manglende overensstemmelse mellem oplysninger registreres på kortet, dvs. tælleren for resterende CHV-forsøg nedbringes med én, for at begrænse antal yderligere forsøg på benyttelse af reference-CHV.

TCS_77 **Kommandomeddelelse**

Byte	Længde	Værdi	Beskrivelse
CLA	1	'00h'	
INS	1	'20h'	INS
P1	1	'00h'	P1

▼B

Byte	Længde	Værdi	Beskrivelse
P2	1	‘00h’	P2 (det verificerede CHV kendes implicit)
Lc	1	‘08h’	Længden af den overførte CHV-kode
#6-#13	8	‘XX..XXh’	CHV

TCS_78 **Svarmeddelelse**

Byte	Længde	Værdi	Beskrivelse
SW	2	‘XXXXh’	Statusord (SW1, SW2)

— Giver kommandoen resultat, tilbagemelder kortet ‘**9000**’.

— Hvis reference-CHV'et ikke findes, tilbagemeldes status ‘**6A88**’.

— Hvis CHV'er er blokeret (tælleren for resterende forsøg for det pågældende CHV har værdien nul), tilbagemeldes behandlingsstatus ‘**6983**’. Når først CHV'et er i denne status, kan det pågældende CHV ikke længere fremvises med held.

— Stemmer oplysningerne ikke overens, bliver tælleren for resterende forsøg formindsket, og status ‘**63CX**’ tilbagemeldes (X > 0 og X er lig værdien af tælleren for resterende CHV-forsøg).

— Hvis reference-CHV anses for beskadiget, tilbagemeldes status ‘**6400**’ eller ‘**6581**’.

— Hvis længden Lc er forskellig fra ‘08h’, er behandlingsstatus ‘**6700**’.

3.5.6 *GET RESPONSE*

Denne kommando er i overensstemmelse med ISO/IEC 7816-4.

Denne kommando (som kun er nødvendig og tilgængelig for protokollen T = 0) benyttes til at overføre behandlede data fra kortet til kortlæseren (i tilfælde, hvor både Lc og Le er indgået i en kommando).

Kommandoen GET RESPONSE skal udstedes straks efter den kommando, som behandler data, ellers mistes data. Efter udførelse af kommandoen GET RESPONSE er de tidligere behandlede data ikke længere tilgængelige (medmindre fejlen ‘61xx’ eller ‘6Cxx’ optræder, se nedenfor).

TCS_79 **Kommandomeddelelse**

Byte	Længde	Værdi	Beskrivelse
CLA	1	‘00h’	
INS	1	‘C0h’	
P1	1	‘00h’	
P2	1	‘00h’	
Le	1	‘XXh’	Antal bytes forventet

▼B

TCS_80 **Svarmeddelelse**

Byte	Længde	Værdi	Beskrivelse
#1-#X	X	'XX..XXh'	Data
SW	2	'XXXXh'	Statusord (SW1, SW2)

— Giver kommandoen resultat, tilbagemelder kortet '**9000**'.

— Hvis ingen data er behandlet af kortet, tilbagemeldes status '**6900**' eller '**6F00**'.

— Hvis længden (Le) overstiger antal bytes til rådighed, eller hvis Le er nul, tilbagemeldes status '**6Cxx**', hvor 'xx' er det nøjagtige antal bytes til rådighed. I dette tilfælde er de behandlede data stadig til rådighed for en efterfølgende GET RESPONSE-kommando.

— Hvis Le ikke er nul og er mindre end antal bytes til rådighed, bliver de ønskede data sendt på normal måde af kortet, og der tilbagemeldes status '**61xx**', hvor 'xx' er antal bytes, som stadig er til rådighed ved en efterfølgende GET RESPONSE-kommando.

— Hvis kommandoen ikke understøttes (protokol T = 1), tilbagemelder kortet '**6D00**'.

3.5.7 *PSO: VERIFY CERTIFICATE*

Denne kommando overholder ISO/IEC 7816-8, men har begrænset anvendelse i forhold til den i normen definerede kommando.

VERIFY CERTIFICATE-kommandoen anvendes af kortet til at hente en offentlig nøgle udefra og kontrollere dens gyldighed.

3.5.7.1 Kommando-svar-par (første generation)

TCS_81 Denne kommandovariant understøttes kun af en takografapplikation af første generation.

TCS_82 Når en VERIFY CERTIFICATE-kommando giver resultat, bliver den offentlige nøgle gemt til fremtidig anvendelse i sikkerhedsmiljøet. Denne nøgle skal udtrykkelig være angivet til brug i sikkerhedsrelaterede kommandoer (INTERNAL AUTHENTICATE, EXTERNAL AUTHENTICATE eller VERIFY CERTIFICATE) af MSE-kommandoen (se punkt 3.5.11) med anvendelse af nøgleidentifikatoren.

TCS_83 I alle tilfælde anvender kommandoen VERIFY CERTIFICATE den offentlige nøgle, som tidligere er valgt af MSE-kommandoen til at åbne certifikatet. Denne offentlige nøgle skal tilhøre en medlemsstat eller EU.

TCS_84 **Kommandomeddelelse**

Byte	Længde	Værdi	Beskrivelse
CLA	1	'00h'	
INS	1	'2Ah'	Udfør sikkerhedsoperation
P1	1	'00h'	P1

▼B

Byte	Længde	Værdi	Beskrivelse
P2	1	'AEh'	P2: Ikke BER-TLV-kodede data (sammenkædning af dataelementer)
Lc	1	'C2h'	Lc: Certifikatets længde, 194 bytes
#6-#199	194	'XX..XXh'	Certifikat: Sammenkædning af dataelementer (som beskrevet i tillæg 11)

TCS_85 **Svarmeddelelse**

Byte	Længde	Værdi	Beskrivelse
SW	2	'XXXXh'	Statusord (SW1, SW2)

— Giver kommandoen resultat, tilbagemelder kortet '**9000**'.

— Lykkes certifikatverificeringen ikke, tilbagemeldes behandlingsstatus '**6688**'. Verifikation og udpakning af certifikatet er beskrevet i tillæg 11 for både første og anden generation.

— Findes der ingen offentlig nøgle i sikkerhedsmiljøet, tilbagemeldes '**6A88**'.

— Hvis den valgte offentlige nøgle (som benyttes til udpakning af certifikatet) anses for beskadiget, tilbagemeldes status '**6400**' eller '**6581**'.

— Kun første generation: Hvis den valgte offentlige nøgle (som anvendes til at udpakke certifikatet) har en anden CHA.LSB (`CertificateHolderAuthorisation.equipmentType`) end '00' (dvs. ikke tilhører en EU-medlemsstat), tilbagemeldes status '**6985**'.

3.5.7.2 Kommando-svar-par (anden generation)

Afhængigt af kurvestørrelsen kan ECC-certifikater være så lange, at de ikke kan sendes i en enkelt APDU. I så fald skal der anvendes kommandokædning i overensstemmelse med ISO/IEC 7816-4, og certifikatet skal sendes i to på hinanden følgende APDU'er af typen PSO: Verify Certificate.

Certifikaters opbygning og domæneparametre er fastlagt i tillæg 11.

TCS_86 Kommandoen kan udføres i hovedfilen, DF Tachograph og DF Tachograph_G2. Se også TCS_33.

TCS_87 **Kommandomeddelelse**

Byte	Længde	Værdi	Beskrivelse
CLA	1	'X0h'	CLA-byte, der indikerer kommandokædning: '00h' — den eneste eller sidste kommando i kæden '10h' — ikke den sidste kommando i kæden
INS	1	'2Ah'	Udfør sikkerhedsoperation
P1	1	'00h'	
P2	1	'BEh'	Verificer selvdeskriptivt certifikat

▼B

Byte	Længde	Værdi	Beskrivelse
Lc	1	'XXh'	Længde af kommandoens datafelt, se TCS_88 og TCS_89.
#6-#5+L	L	'XX..XXh'	DER-TLV-kodede data: dataobjekt af typen "ECC Certificate Body" som første dataobjekt sammenkædet med dataobjektet "ECC Certificate Signature" som andet dataobjekt eller en del af denne sammenkædning. Etiketten '7F21' og den tilsvarende længde skal ikke overføres. Disse dataobjekters rækkefølge ligger fast.

TCS_88 For APDU'er med kort længde gælder følgende bestemmelser: Kortlæseren skal bruge det mindste antal APDU'er, der er nødvendige for at overføre kommandoens indhold, og overføre det størst mulige antal bytes i den første kommando-APDU i overensstemmelse med værdien af Information Field Size Card-byten. Se TCS_14. Hvis kortlæseren opfører sig anderledes, er kortets adfærd uden for det gyldige område.

TCS_89 For APDU'er med udvidet længde gælder følgende bestemmelser: Hvis certifikatet ikke kan være i en enkelt APDU, skal kortet understøtte kommandokædning. Kortlæseren skal bruge det mindste antal APDU'er, der er nødvendige for at overføre kommandoens indhold, og overføre det størst mulige antal bytes i den første kommando-APDU. Hvis kortlæseren opfører sig anderledes, er kortets adfærd uden for det gyldige område.

Bemærk: Som anført i tillæg 11 lagrer kortet certifikatet eller det relevante indhold i det, hvorefter det opdaterer parameteren currentAuthenticatedTime.

Svarmeddelelsesstrukturen og statusordene er fastlagt i TCS_85.

TCS_90 Ud over de fejlkoder, der er opført i TCS_85, kan kortet tilbagemelde følgende fejlkoder:

— Hvis den valgte offentlige nøgle (som anvendes til at udpakke certifikatet) har en CHA.LSB (CertificateHolderAuthorisation.equipmentType), som ikke egner sig til certifikatverificering i overensstemmelse med tillæg 11, tilbagemeldes status '**6985**'.

— Hvis kortets currentAuthenticatedTime ligger senere end Certificate Expiration Date, tilbagemeldes behandlingsstatus '**6985**'.

— Hvis den sidste kommando i kæden er som forventet, tilbagemelder kortet '**6883**'.

— Hvis der sendes ukorrekte parametre i kommandoens datafelt, tilbagemelder kortet '**6A80**' (bruges også, hvis dataobjekterne ikke sendes i den foreskrevne rækkefølge).

▼B

3.5.8 *INTERNAL AUTHENTICATE*

Denne kommando er i overensstemmelse med ISO/IEC 7816-4.

TCS_91 Alle takografkort skal understøtte denne kommando i første generation af DF Tachograph. Kommandoen kan eventuelt være tilgængelig i hovedfilen og/eller DF Tachograph_G2. I så fald skal kommandoen afsluttes med en passende fejlkode, da kortets (Card.SK) private nøgle til ægthedsbekræftelsesprotokollen (første generation) kun er tilgængelig i første generation af DF Tachograph.

Med kommandoen INTERNAL AUTHENTICATE kan kortlæseren bekræfte kortets ægthed. Identitetsbekræftelsen er beskrevet i tillæg 11. Den indeholder følgende sætninger:

TCS_92 Kommandoen INTERNAL AUTHENTICATE anvender kortets private nøgle (som er valgt implicit) til signering af ægthedsdata, som indeholder K1 (første element i session nøgleoverensstemmelse) og RND1, og anvender den offentlige nøgle, der aktuelt er valgt (ved den seneste MSE-kommando), til at kryptere underskriften og udforme ægthedsbekræftelsestoken (nærmere detaljer i tillæg 11).

TCS_93 **Kommandomeddelelse**

Byte	Længde	Værdi	Beskrivelse
CLA	1	'00h'	CLA
INS	1	'88h'	INS
P1	1	'00h'	P1
P2	1	'00h'	P2
Lc	1	'10h'	Længde af data sendt til kortet
#6-#13	8	'XX..XXh'	Challenge anvendt til bekræftelse af kortets identitet
#14-#21	8	'XX..XXh'	VU.CHR (se tillæg 11)
Le	1	'80h'	Forventet længde af data fra kortet

TCS_94 **Svarmeddelelse**

Byte	Længde	Værdi	Beskrivelse
#1-#128	128	'XX..XXh'	Token for identifikation af kort (se tillæg 11)
SW	2	'XXXXh'	Statusord (SW1, SW2)

— Giver kommandoen resultat, tilbagemelder kortet '**9000**'.

— Findes ingen offentlig nøgle i sikkerhedsmiljøet, tilbagemeldes status '**6A88**'.

— Findes ingen privat nøgle i sikkerhedsmiljøet, tilbagemeldes status '**6A88**'.

— Hvis VU.CHR ikke svarer til navnet for den aktuelle offentlige nøgle, tilbagemeldes status '**6A88**'.

▼B

— Hvis den valgte private nøgle anses for beskadiget, tilbagemeldes status '**6400**' eller '**6581**'.

TCS_95 Hvis INTERNAL AUTHENTICATE-kommandoen giver resultat, slettes den eventuelle nøgle for den aktuelle session og er ikke længere til rådighed. For at man kan få adgang til en ny sessionsnøgle, skal kommandoen EXTERNAL AUTHENTICATE for mekanismen til ægthedsbekræftelse for første generation gennemføres med resultat.

3.5.9 *EXTERNAL AUTHENTICATE*

Denne kommando er i overensstemmelse med ISO/IEC 7816-4.

Med kommandoen EXTERNAL AUTHENTICATE kan kortet bekræfte identiteten af kortlæseren. Ægthedsbekræftelsen er beskrevet i tillæg 11 for takografer af første og anden generation (ægthedsbekræftelse for køretøjsenhed).

TCS_96 Kommandovarianten for mekanismen til gensidig ægthedsbekræftelse af første generation understøttes kun af takografapplikationer af første generation.

TCS_97 Kommandovarianten for gensidig ægthedsbekræftelse for anden generation på køretøjsenhedens kort kan udføres i hovedfilen, DF Tachograph og DF Tachograph_G2. Se også TCS_34.

TCS_98 **Kommandomeddelelse**

Byte	Længde	Værdi	Beskrivelse
CLA	1	'00h'	CLA
INS	1	'82h'	INS
P1	1	'00h'	Nøgler og algoritmer kendes implicit
P2	1	'00h'	
Lc	1	'XXh'	Lc (længde af data sendt til kortet)
#6-#(5+L)	L	'XX..XXh'	Ægthedsbekræftelse for første generation: Kryptogram (se tillæg 11, del A) Ægthedsbekræftelse for anden generation: Underskrift genereret af kortlæseren (se tillæg 11, del B)

TCS_99 **Svarmeddelelse**

Byte	Længde	Værdi	Beskrivelse
SW	2	'XXXXh'	Statusord (SW1, SW2)

— Giver kommandoen resultat, tilbagemelder kortet '**9000**'.

— Hvis CHA for den aktuelt fastsatte offentlige nøgle ikke er en sammenføjning af takografapplikationens navn (AID) og en type køretøjsenhed, tilbagemeldes status '**6F00**'.

— Hvis denne kommando ikke følger umiddelbart efter en GET CHALLENGE-kommando, tilbagemeldes status '**6985**'.

▼B

Takografapplikationen af første generation kan derudover tilbagemelde følgende fejlkoder:

— Findes der ingen offentlig nøgle i sikkerhedsmiljøet, tilbagemeldes '**6A88**'.

— Findes ingen privat nøgle i sikkerhedsmiljøet, tilbagemeldes status '**6A88**'.

— Lykkes verifikationen af den kryptografiske kontrolsum ikke, tilbagemeldes behandlingsstatus '**6688**'.

— Hvis den valgte private nøgle anses for beskadiget, tilbagemeldes status '**6400**' eller '**6581**'.

Kommandovarianten for ægthedsbekræftelse for anden generation kan desuden tilbagemelde følgende fejlkode:

— Lykkes verifikationen af underskriften ikke, tilbagemelder kortet '**6300**'.

3.5.10 *GENERAL AUTHENTICATE*

Denne kommando bruges til den protokol til ægthedsbekræftelse af chip af anden generation, der er angivet i tillæg 11, del B, og som er i overensstemmelse med ISO/IEC 7816-4.

TCS_100 Kommandoen kan udføres i hovedfilen, DF Tachograph og DF Tachograph_G2. Se også TCS_34.

TCS_101 **Kommandomeddelelse**

Byte	Længde	Værdi	Beskrivelse
CLA	1	'00h'	
INS	1	'86h'	
P1	1	'00h'	Nøgler og protokol kendes implicit
P2	1	'00h'	
Lc	1	'NNh'	Lc: længde af efterfølgende datafelt
#6-#(5+L)	L	'7Ch' + L_{7C} + '80h' + L_{80} + 'XX..XXh'	DER-TLV-kodet kortvarig værdi for offentlig nøgle (se tillæg 11) Køretøjsenheden skal sende dataobjekterne i denne rækkefølge.

TCS_102 **Svarmeddelelse**

Byte	Længde	Værdi	Beskrivelse
#1-#L	L	'7Ch' + L_{7C} + '81h' + '08h' + 'XX..XXh' + '82h' + L_{82} + 'XX..XXh'	DER-TLV-kodede dynamiske ægthedsbekræftelsesdata: nonce og ægthedsbekræftelsestoken (se tillæg 11)
SW	2	'XXXXh'	Statusord (SW1, SW2)

— Giver kommandoen resultat, tilbagemelder kortet '**9000**'.

— Kortet tilbagemelder '**6A80**' for at indikere ukorrekte parametre i datafelt.

▼B

— Kortet tilbagemelder '**6982**', hvis kommandoen External Authenticate ikke er udført med resultat

Svarobjektet for dynamisk ægthedsbekræftelse '7Ch'

— skal findes, hvis operationen giver resultat, dvs. statusordet er '**9000**'

— må ikke findes i tilfælde af en kørselsfejl eller kontrolfejl, dvs. hvis statusordene er inden for området **'6400'-'6FFF'**

— findes muligvis ikke i tilfælde af en advarsel, dvs. hvis statusordene er inden for området **'6200'-'63FF'**.

3.5.11 *MANAGE SECURITY ENVIRONMENT*

Med denne kommando fastsættes en offentlig nøgle til brug for ægthedsbekræftelse.

3.5.11.1 Kommando-svar-par (første generation)

Denne kommando er i overensstemmelse med ISO/IEC 7816-4. Brugen af denne kommando er begrænset med hensyn til den tilknyttede standard.

TCS_103 Denne kommando understøttes kun af en takografapplikation af første generation.

TCS_104 Den nøgle, der henvises til i MSE-datafeltet, er den aktuelle offentlige nøgle indtil næste korrekte MSE-kommando, indtil en dedikeret fil vælges, eller indtil kortet nulstilles.

TCS_105 Hvis den nøgle, der henvises til, ikke (allerede) er til stede på kortet, sker der ingen ændring i sikkerhedsmiljøet.

TCS_106 **Kommandomeddelelse**

Byte	Længde	Værdi	Beskrivelse
CLA	1	'00h'	CLA
INS	1	'22h'	INS
P1	1	'C1h'	P1: Den nøgle, der henvises til, er gyldig for alle kryptografiske operationer
P2	1	'B6h'	P2 (data, som der er henvist til vedrørende digital underskrift)
Lc	1	'0Ah'	Lc: længde af efterfølgende datafelt
#6	1	'83h'	Etiket bestemt til henvisning til en offentlig nøgle i asymmetriske tilfælde
#7	1	'08h'	Længde af nøglehenvisning (nøgleidentifikator)
#8-#15	8	'XX..XXh'	Nøgleidentifikator som foreskrevet i tillæg 11

TCS_107 **Svarmeddelelse**

Byte	Længde	Værdi	Beskrivelse
SW	2	'XXXXh'	Statusord (SW1, SW2)

▼B

— Giver kommandoen resultat, tilbagemelder kortet '**9000**'.

— Hvis den nøgle, der henvises til, ikke er til stede på kortet, tilbagemeldes behandlingsstatus '**6A88**'.

— Hvis visse forventede dataobjekter ikke findes i sikkert meddelelsesformat, tilbagemeldes status '**6987**'. Dette kan være tilfældet, hvis etiketten '83h' mangler.

— Hvis nogle dataobjekter er ukorrekte, tilbagemeldes status '**6988**'. Dette kan ske, hvis længden af nøgleidentifikatoren ikke er '08h.'

— Hvis den valgte nøgle anses for beskadiget, tilbagemeldes status '**6400**' eller '**6581**'.

3.5.11.2 Kommando-svar-par (anden generation)

Ved ægthedsbekræftelse af anden generation understøtter takografkortet følgende kommandoversioner af typen MSE: Set, som er i overensstemmelse med ISO/IEC 7816-4. Disse kommandoversioner understøttes ikke for ægthedsbekræftelse af første generation.

3.5.11.2.1 MSE:SET AT til ægthedsbekræftelse af chip

Følgende MSE:SET AT-kommando bruges til at vælge parametrene for den ægthedsbekræftelse af chip, som udføres af en efterfølgende General Authenticate-kommando.

TCS_108 Kommandoen kan udføres i hovedfilen, DF Tachograph og DF Tachograph_G2. Se også TCS_34.

TCS_109 **MSE:SET AT-kommandomeddelelse til ægthedsbekræftelse af chip**

Byte	Længde	Værdi	Beskrivelse
CLA	1	'00h'	
INS	1	'22h'	
P1	1	'41h'	Angives for intern ægthedsbekræftelse
P2	1	'A4h'	Ægthedsbekræftelse
Lc	1	'NNh'	Lc: længde af efterfølgende datafelt
#6-#(5+L)	L	'80h' + '0Ah' + 'XX..XXh'	DER-TLV-kodet henvisning til kryptografisk mekanisme: Objektidentifikator for ægthedsbekræftelse af chip (kun værdi, Etiket '06h' udelades). Objektidentifikatorernes værdier fremgår af tillæg 1. Byte-notation skal anvendes. I tillæg 11 findes en vejledning i udvælgelse af en af disse objektidentifikatorer.

3.5.11.2.2 MSE:SET AT til ægthedsbekræftelse af køretøjsenhed

Følgende MSE:SET AT-kommando bruges til at vælge parametrene og nøglerne for den ægthedsbekræftelse af køretøjsenheden, som udføres af en efterfølgende External Authenticate-kommando.

▼B

TCS_110 Kommandoen kan udføres i hovedfilen, DF Tachograph og DF Tachograph_G2. Se også TCS_34.

TCS_111 **MSE:SET AT-kommandomeddelelse til ægthedsbekræftelse af køretøjsenhed**

Byte	Længde	Værdi	Beskrivelse
CLA	1	'00h'	
INS	1	'22h'	
P1	1	'81h'	Angives for ekstern ægthedsbekræftelse
P2	1	'A4h'	Ægthedsbekræftelse
Lc	1	'NNh'	Lc: længde af efterfølgende datafelt
#6-#(5+L)	L	'80h' + '0Ah' + 'XX..XXh'	DER-TLV-kodet henvisning til kryptografisk mekanisme: Objektidentifikator for ægthedsbekræftelse af køretøjsenhed (kun værdi, Etiket '06h' udelades). Objektidentifikatorernes værdier fremgår af tillæg 1. Byte-notation skal anvendes. I tillæg 11 findes en vejledning i udvælgelse af en af disse objektidentifikatorer.
		'83h' + '08h' + 'XX..XXh'	DER-TLV-kodet henvisning af køretøjsenhedens offentlige nøgle foretaget af den henvisning til certifikatindehaveren, der er nævnt i nøglens certifikat.
		'91h' + L_{91} + 'XX..XXh'	DER-TLV-kodet komprimeret gengivelse af den kortvarige offentlige nøgle for køretøjsenheden, som vil blive anvendt under ægthedsbekræftelse af chip (se tillæg 11)

3.5.11.2.3 MSE:SET DST

Følgende MSE:SET DST-kommando bruges til at fastsætte en offentlig nøgle for enten

— verifikation af en underskrift, som leveres i en efterfølgende PSO: Verify Digital Signature-kommando eller

— underskriftsverifikation af et certifikat, som leveres i en efterfølgende PSO: Verify Certificate-kommando

TCS_112 Kommandoen kan udføres i hovedfilen, DF Tachograph og DF Tachograph_G2. Se også TCS_33.

TCS_113 **MSE SET DST-kommandomeddelelse**

Byte	Længde	Værdi	Beskrivelse
CLA	1	'00h'	
INS	1	'22h'	
P1	1	'81h'	Angives for verifikation
P2	1	'B6h'	Digital underskrift

▼B

Lc	1	'NNh'	Lc: længde af efterfølgende datafelt
#6-#(5+L)	L	'83h' + '08h' + 'XX..XXh'	DER-TLV-kodet henvisning af en offentlig nøgle, dvs. henvisningen til certifikatindehaveren i den offentlige nøgles certifikat (se tillæg 11)

For alle kommandoversioner er svarmeddelelsesstrukturen og statusordene givet ved:

TCS_114 **Svarmeddelelse**

Byte	Længde	Værdi	Beskrivelse
SW	2	'XXXXh'	Statusord (SW1, SW2)

— Giver kommandoen resultat, tilbagemelder kortet '**9000**'. Protokollen er valgt og initialiseret.

— '**6A80**' indikerer ukorrekte parametre i kommandoens datafelt.

— '**6A88**' indikerer, at adresserede data (dvs. en nøgle, der henvises til) ikke er tilgængelig.

3.5.12 *PSO: HASH*

Denne kommando anvendes til at overføre værdien af en hashberegning på visse data til kortet. Kommandoen bruges til verifikation af digitale underskrifter. Hashværdien lagres midlertidigt til den efterfølgende kommando PSO: Verify Digital Signature

Denne kommando er i overensstemmelse med ISO/IEC 7816-8. Brugen af denne kommando er begrænset med hensyn til den tilknyttede standard.

Kun kontrolkortet kræves for at understøtte denne kommando i DF Tachograph og DF Tachograph_G2.

Andre slags takografkort kan eventuelt udføre denne kommando. Kommandoen kan eventuelt være tilgængelig i hovedfilen.

Kontrolkortapplikationen af første generation understøtter kun SHA-1.

TCS_115 Den midlertidigt gemte hashværdi skal slettes, hvis en ny hashværdi beregnes ved hjælp af kommandoen PSO: HASH, hvis en dedikeret fil vælges, og hvis takografkortet nulstilles.

TCS_116 **Kommandomeddelelse**

Byte	Længde	Værdi	Beskrivelse
CLA	1	'00h'	CLA
INS	1	'2Ah'	Udfør sikkerhedsoperation
P1	1	'90h'	Tilbagemeld hashkode

▼B

Byte	Længde	Værdi	Beskrivelse
P2	1	‘A0h’	Etiket: Datafeltet indeholder dataobjekter, som er relevante for hashing
Lc	1	‘XXh’	Længde Lc af det efterfølgende datafelt
#6	1	‘90h’	Etiket til hashkode
#7	1	‘XXh’	Længde L af hashkoden: ‘14h’ i applikation af første generation (se tillæg 11, del A) ‘20h’, ‘30h’ eller ‘40h’ i applikation af anden generation (se tillæg 11, del B)
#8-#(7+L)	L	‘XX..XXh’	Hashkode

TCS_117 **Svarmeddelelse**

Byte	Længde	Værdi	Beskrivelse
SW	2	‘XXXXh’	Statusord (SW1, SW2)

— Giver kommandoen resultat, tilbagemelder kortet ‘**9000**’.

— Hvis nogle af de forventede dataobjekter (som angivet ovenfor) mangler, tilbagemeldes status ‘**6987**’. Dette kan ske, hvis en af etiketterne ‘90h’ mangler.

— Hvis nogle dataobjekter er ukorrekte, tilbagemeldes status ‘**6988**’. Denne fejl opstår, hvis den ønskede etiket er til stede, men har en anden længde end ‘14h’ for SHA-1, ‘20h’ for SHA-256, ‘30h’ for SHA-384 eller ‘40h’ for SHA-512 (applikation af anden generation).

3.5.13 *PERFORM HASH of FILE*

Denne kommando er ikke i overensstemmelse med ISO/IEC 7816-8. Klassebyten (CLA) i denne kommando angiver således, at der er en ophavsretligt beskyttet anvendelse af PERFORM SECURITY OPERATION/HASH.

Kun førerkortet og værkstedskortet kræves for at understøtte denne kommando i DF Tachograph og DF Tachograph_G2.

Andre slags takografkort kan eventuelt udføre denne kommando. Hvis et virksomhedskort eller kontrolkort udfører denne kommando, skal kommandoen udføres som foreskrevet i dette afsnit.

Kommandoen kan eventuelt være tilgængelig i hovedfilen. I så fald skal kommandoen udføres som foreskrevet i dette afsnit. Den må ikke muliggøre beregning af en hashværdi, men skal afsluttes med en passende fejlkode.

TCS_118 Kommandoen PERFORM HASH OF FILE anvendes til hashing af dataområdet i den aktuelt valgte transparente elementærfil.

TCS_119 Takografkort skal kun understøtte denne kommando for de elementærfiler, der er anført i afsnit 4 under DF_Tachograph og DF_Tachograph_G2 med følgende undtagelse. Takografkort må ikke understøtte kommandoen for elementærfilen Sensor_Installation_Data i DF Tachograph_G2.

▼B

TCS_120 Resultatet af hashoperationen gemmes midlertidigt på kortet. Derefter kan det benyttes til at sætte en digital underskrift på filen ved hjælp af kommandoen PSO: COMPUTE DIGITAL SIGNATURE.

TCS_121 Den midlertidigt gemte Hash of File-værdi skal slettes, hvis en ny Hash of File-værdi beregnes ved hjælp af kommandoen PSO: Hash of File, hvis en dedikeret fil vælges, og hvis takografkortet nulstilles.

TCS_122 Takografapplikationer af første generation skal understøtte SHA-1.

TCS_123 Takografapplikationer af anden generation skal understøtte SHA-1 og SHA-2 (256, 384 og 512 bit).

TCS_124 **Kommandomeddelelse**

Byte	Længde	Værdi	Beskrivelse
CLA	1	'80h'	CLA
INS	1	'2Ah'	Udfør sikkerhedsoperation
P1	1	'90h'	Etiket: Hash
P2	1	'XXh'	P2: Angiver den algoritme, som skal anvendes til hashing af dataene i den aktuelt valgte transparente fil. '00h' for SHA-1 '01h' for SHA-256 '02h' for SHA-384 '03h' for SHA-512

TCS_125 **Svarmeddelelse**

Byte	Længde	Værdi	Beskrivelse
SW	2	'XXXXh'	Statusord (SW1, SW2)

— Giver kommandoen resultat, tilbagemelder kortet '**9000**'.

— Hvis den aktuelt valgte elementærfil ikke tillader denne kommando (elementærfilen Sensor_Installation_Data i DF Tachograph_G2), tilbagemeldes status '**6985**'.

— Anses den valgte elementærfil for beskadiget, tilbagemeldes status '**6400**' eller '**6581**'.

— Er den valgte fil ikke en transparent fil, eller findes der ingen aktuelt valgt elementærfil, tilbagemeldes status '**6986**'.

3.5.14 *PSO: COMPUTE DIGITAL SIGNATURE*

Denne kommando anvendes til at beregne den digitale underskrift af en tidligere beregnet hashkode (se PERFORM HASH OF FILE, punkt 3.5.13).

Kun førerkortet og værkstedskortet kræves for at understøtte denne kommando i DF Tachograph og DF Tachograph_G2.

▼B

Andre slags takografkort kan muligvis udføre denne kommando, men de må ikke have en underskriftsnøgle. Disse kort kan derfor ikke udføre kommandoen med resultat, men skal afsluttes med en passende fejlkode.

Kommandoen kan eventuelt være tilgængelig i hovedfilen. I så fald skal kommandoen afsluttes med en passende fejlkode.

Denne kommando er i overensstemmelse med ISO/IEC 7816-8. Brugen af denne kommando er begrænset med hensyn til den tilknyttede standard.

TCS_126 Denne kommando må ikke beregne en digital underskrift for en tidligere beregnet hashkode med kommandoen PSO: HASH.

TCS_127 Kortets private nøgle anvendes til at beregne den digitale underskrift og kendes implicit af kortet.

TCS_128 Takografapplikationen af første generation udfører en digital underskrift med en udfyldningsmetode, som er i overensstemmelse med PKCS1 (se tillæg 11 for nærmere detaljer).

TCS_129 Takografapplikationen af anden generation beregner en digital underskrift, der baseret på en elliptisk kurve (se tillæg 11 for detaljer).

TCS_130 **Kommandomeddelelse**

Byte	Længde	Værdi	Beskrivelse
CLA	1	'00h'	CLA
INS	1	'2Ah'	Udfør sikkerhedsoperation
P1	1	'9Eh'	Digital underskrift, som skal tilbagemeldes
P2	1	'9Ah'	Etiket: Datafeltet indeholder data, som skal underskrives. Da der ikke indgår noget datafelt, formodes data allerede at være til stede i kortet (hash af filen)
Le	1	'NNh'	Længde af den forventede underskrift

TCS_131 **Svarmeddelelse**

Byte	Længde	Værdi	Beskrivelse
#1-#L	L	'XX..XXh'	Underskrift af den tidligere beregnede hash
SW	2	'XXXXh'	Statusord (SW1, SW2)

— Giver kommandoen resultat, tilbagemelder kortet '**9000**'.

— Hvis den implicit valgte private nøgle anses for beskadiget, tilbagemeldes status '**6400**' eller '**6581**'.

— Hvis den hashværdi, der blev beregnet ved en tidligere PERFORM HASH of FILE-kommando, ikke er tilgængelig, tilbagemeldes status '**6985**'.

▼B

3.5.15 *PSO: VERIFY DIGITAL SIGNATURE*

Denne kommando anvendes til at verificere den digitale underskrift, der tilføres som inddata for en meddelelse, for hvilken hash kendes af kortet. Underskriftsalgoritmen kendes implicit af kortet.

Denne kommando er i overensstemmelse med ISO/IEC 7816-8. Brugen af denne kommando er begrænset med hensyn til den tilknyttede standard.

Kun kontrolkortet kræves for at understøtte denne kommando i DF Tachograph og DF Tachograph_G2.

Andre slags takografkort kan eventuelt udføre denne kommando. Kommandoen kan eventuelt være tilgængelig i hovedfilen.

TCS_132 Kommandoen VERIFY DIGITAL SIGNATURE bruger altid den offentlige nøgle, der er valgt af den foregående kommando af typen Manage Security Environment MSE: Set DST, og den foregående hashkode, der er indlæst af en PSO: HASH-kommando.

TCS_133 **Kommandomeddelelse**

Byte	Længde	Værdi	Beskrivelse
CLA	1	'00h'	CLA
INS	1	'2Ah'	Udfør sikkerhedsoperation
P1	1	'00h'	
P2	1	'A8h'	Etiket: Datafeltet indeholder dataobjekter, der er relevante for verifikation
Lc	1	'83h'	Længde Lc af det efterfølgende datafelt
6	1	'9Eh'	Etiket for digital underskrift
#7-#8	2	'81 XXh'	Længde af digital underskrift: 128 bytes kodet i overensstemmelse med tillæg 11, del A, for takografapplikationer af første generation Afhængigt af den valgte kurve for takografapplikationer af anden generation (se tillæg 11, del B)
#9-#(8+L)	L	'XX..XXh'	Indhold af digital underskrift

TCS_134 **Svarmeddelelse**

Byte	Længde	Værdi	Beskrivelse
SW	2	'XXXXh'	Statusord (SW1, SW2)

— Giver kommandoen resultat, tilbagemelder kortet '**9000**'.

— Lykkes verifikationen af underskriften ikke, tilbagemeldes behandlingsstatus '**6688**'. Verifikationsprocessen er beskrevet i tillæg 11.

— Hvis der ikke er valgt nogen offentlig nøgle, tilbagemeldes status '**6A88**'.

— Hvis nogle af de forventede dataobjekter (som angivet ovenfor) mangler, tilbagemeldes status '**6987**'. Dette kan forekomme, hvis en af de ønskede etiketter mangler.

▼B

— Hvis der til behandling af kommandoen ikke er nogen hashkode til rådighed (som resultat af en forudgående PSO: HASH-kommando), tilbagemeldes status '**6985**'.

— Hvis nogle dataobjekter er ukorrekte, tilbagemeldes status '**6988**'. Dette kan forekomme, hvis længden af et af de ønskede dataobjekter er forkert.

— Hvis den valgte offentlige nøgle anses for beskadiget, tilbagemeldes status '**6400**' eller '**6581**'.

3.5.16 *PROCESS DSRC MESSAGE*

Denne kommando bruges til at verificere integriteten og ægtheden af DSRC-meddelelsen og til at dechifrere de data, som en køretøjsenhed sender til en kontrolmyndighed eller et værksted via DSRC-forbindelsen. Kortet udleder den krypteringsnøgle og den MAC-nøgle, der bruges til at sikre DSRC-meddelelsen som beskrevet i tillæg 11, del B, afsnit 13.

Kun kontrolkortet og værkstedskortet kræves for at understøtte denne kommando i DF Tachograph_G2.

Andre slags takografkort kan muligvis udføre denne kommando, men de må ikke have en DSRC-hovednøgle. Disse kort kan derfor ikke udføre kommandoen med resultat, men skal afsluttes med en passende fejlkode.

Kommandoen kan eventuelt være tilgængelig i hovedfilen og/eller DF Tachograph. I så fald skal kommandoen afsluttes med en passende fejlkode.

TCS_135 DSRC-hovednøglen er kun tilgængelig i DF Tachograph_G2. Kontrol- og værkstedskortet skal således kun understøtte udførelse af kommandoen i DF Tachograph_G2.

TCS_136 Kommandoen skal kun dekryptere DSRC-dataene og verificere den kryptografiske kontrolsum, men ikke fortolke de indlæste data.

TCS_137 Dataobjekternes rækkefølge i kommandoens datafelt er fastlagt i denne specifikation.

TCS_138 **Kommandomeddelelse**

Byte	Længde	Værdi	Beskrivelse
CLA	1	'80h'	Beskyttet CLA
INS	1	'2Ah'	Udfør sikkerhedsoperation
P1	1	'80h'	Svardata: ordinær værdi
P2	1	'B0h'	Kommandodata: ordinær værdi, der er kodet i BER-TLV og omfatter SM-dataobjekter
Lc	1	'NNh'	Længde Lc af det efterfølgende datafelt

▼B

Byte	Længde	Værdi	Beskrivelse
#6-#(5+L)	L	'87h' + L_{87} + 'XX..XXh'	DER-TLV-kodet indikatorbyte for udfyldningsindhold efterfulgt af krypteret takografindhold. For indikatorbyten for udfyldningsindhold skal værdien '00h' anvendes ("no further indication" (ingen yderligere angivelse) i henhold til ISO/IEC 7816-4:2013, tabel 52). For så vidt angår krypteringsmekanismen henvises til tillæg 11, del B, afsnit 13. De tilladte værdier for længden L_{87} er multiplerne af AES-bloklængden plus 1 for indikatorbyten for udfyldningsindhold, dvs. fra 17 bytes til og med 193 bytes. *Bemærk:* Se ISO/IEC 7816-4:2013, tabel 49, med hensyn til SM-dataobjektet med etiket '87h'.
		'81h' + '10h'	DER-TLV-kodet kontrolreferenceskabelon for fortrolighed, der indlejrer sammenkædningen af følgende dataelementer (se tillæg 1 (DSRCSecurityData) og tillæg 11, del B, afsnit 13): — tidsstempel på 4 bytes — tæller på 3 bytes — køretøjsenhedens serienummer på 8 bytes — DSRC-hovednøgleversion på 1 byte *Bemærk:* Se ISO/IEC 7816-4:2013, tabel 49, med hensyn til SM-dataobjektet med etiket '81h'.
		'8Eh' + L_{8E} + 'XX..XXh'	DER-TLV-kodet MAC over DSRC-meddelelsen. For så vidt angår MAC-algoritmen og beregning henvises til tillæg 11, del B, afsnit 13. *Bemærk:* Se ISO/IEC 7816-4:2013, tabel 49, med hensyn til SM-dataobjektet med etiket '8Eh'.

TCS_139 **Svarmeddelelse**

Byte	Længde	Værdi	Beskrivelse
#1-#L	L	'XX..XXh'	Manglende data (i tilfælde af en fejl) eller dechifrerede data (udfyldning fjernet)
SW	2	'XXXXh'	Statusord (SW1, SW2)

— Giver kommandoen resultat, tilbagemelder kortet '**9000**'.

— '**6A80**' indikerer ukorrekte parametre i kommandoens datafelt (bruges også, hvis dataobjekterne ikke sendes i den foreskrevne rækkefølge).

— '**6A88**' indikerer, at adresserede data ikke er tilgængelige (den adresserede DSRC-hovednøgle er ikke tilgængelig).

— '**6900**' indikerer, at verifikationen af den kryptografiske kontrolsum eller dekrypteringen af dataene mislykkedes.

4. TAKOGRAFKORTENES STRUKTUR

Dette afsnit angiver takografkortenes filstruktur til lagring af tilgængelige data.

▼B

Det specificerer ikke producentafhængige interne strukturer i kortet som f.eks. startetiketter på filer eller lagring og behandling af dataelementer, som udelukkende behøves til intern brug, som f.eks. `EuropeanPublicKey`, `CardPrivateKey`, `TdesSessionKey` eller `WorkshopCardPin`.

TCS_140 Takografkort af anden generation skal rumme hovedfilen og en takografapplikation af første og anden generation af samme type (f.eks. førerkortapplikationer).

TCS_141 Takografkort skal som minimum understøtte det antal poster, som er fastsat for de tilsvarende applikationer, og må ikke understøtte flere poster end det maksimale antal poster, der er fastsat for de tilsvarende applikationer.

Det højeste og laveste antal poster er nærmere beskrevet i dette afsnit for de forskellige applikationer.

For så vidt angår de sikkerhedsbetingelser, der anvendes i adgangsreglerne i hele dette afsnit, henvises til afsnit 3.3. Generelt angiver adgangstilstanden "læs" kommandoen READ BINARY med lige — og hvis de understøttes — ulige INS-byte med undtagelse af elementærfilen Sensor_Installation_Data på værkstedskortet. Se TCS_156 og TCS_160. Adgangstilstanden "opdater" angiver kommandoen Update Binary med lige — og hvis de understøttes — ulige INS-byte, mens adgangstilstanden "vælg" angiver kommandoen SELECT.

4.1. **Hovedfil (Master file — MF)**

TCS_142 Efter at hovedfilen er personaliseret, skal den have følgende permanente filstruktur og filadgangsregler:

Bemærk: Det korte id for elementærfilen (SFID) gives som decimaltal. F.eks. svarer værdien 30 til 11110 som binært tal.

			Adgangsregler	
Fil	**Fil-id**	**SFID**	**Læs/vælg**	**Opdater**
MF	'3F00h'			
├─ EF ICC	'0002h'		ALW	NEV
├─ EF IC	'0005h'		ALW	NEV
├─ EF DIR	'2F00h'	30	ALW	NEV
├─ EF ATR/INFO (betinget)	'2F01h'	29	ALW	NEV
├─ EF Extended_Length (betingen)	'0006h'	28	ALW	NEV
├─ DF Tachograph	'0500h'		SC1	
└─ DF Tachograph_G2			SC1	

Følgende forkortelse for sikkerhedsbetingelsen anvendes i denne tabel:

SC1 ALW OR SM-MAC-G2

TCS_143 Alle elementærfilers strukturer skal være transparente.

TCS_144 Hovedfilen skal have følgende datastruktur:

▼B

Fil/dataelement	Antal poster	Størrelse (bytes) Min	Max	Standard-værdier
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 Elementærfilen EF DIR skal indeholde følgende applikationsrelaterede dataobjekter: '61 08 4F 06 FF 54 41 43 48 4F 61 08 4F 06 FF 53 4D 52 44 54'

TCS_146 Elementærfilen EF ATR/INFO skal findes, hvis takografkortet i sit ATR angiver, at det understøtter felter med udvidet længde. I så fald skal elementærfilen EF ATR/INFO indeholde dataobjektet med udvidet informationslængde (DO '7F66') som foreskrevet i ISO/IEC 7816-4:2013, afsnit 12.7.1.

TCS_147 Elementærfilen EF Extended_Length skal findes, hvis takografkortet i sit ATR angiver, at det understøtter felter med udvidet længde. I så fald skal elementærfilen indeholde følgende dataobjekt: '02 01 xx', hvor værdien 'xx' angiver, om felter med udvidet længde understøttes for protokollen T = 1 og/eller T = 0.

Værdien '01' angiver, at felter med udvidet længde understøttes for protokollen T = 1.

Værdien '10' angiver, at felter med udvidet længde understøttes for protokollen T = 0.

Værdien '11' angiver, at felter med udvidet længde understøttes for protokollerne T = 1 og T = 0.

4.2. Førerkortapplikationer

4.2.1 *Førerkortapplikation af første generation*

TCS_148 Efter at førerkortapplikationen af første generation er personaliseret, skal den have følgende permanente filstruktur og filadgangsregler:

Fil	Fil-id	Adgangsregler Læs	Vælg	Opdater
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

Følgende forkortelser for sikkerhedsbetingelserne anvendes i denne tabel:

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 Alle elementærfilers strukturer skal være transparente.

TCS_150 Førerkortapplikationen af første generation skal have følgende datastruktur:

Fil/dataelement	Antal poster	Størrelse (bytes) Min	Max	Standard-værdier
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 Følgende værdier, der er anvendt som størrelsesangivelser i ovenstående tabel, er mindste og største antal poster i førerkortets datastruktur for en applikation af første generation:

		Min	Max
n_1	NoOfEventsPerType	6	12
n_2	NoOfFaultsPerType	12	24
n_3	NoOfCardVehicleRecords	84	200
n_4	NoOfCardPlaceRecords	84	112
n_6	CardActivityLengthRange	5 544 bytes (28 døgn med 93 aktivitetsskift)	13 776 bytes (28 døgn med 240 aktivitetsskift)

4.2.2 *Førerkortapplikation af anden generation*

TCS_152 Efter at førerkortapplikationen af anden generation er personaliseret, skal den have følgende permanente filstruktur og filadgangsregler:

Bemærk: Det korte id for elementærfilen (SFID) gives som decimaltal. F.eks. svarer værdien 30 til 11110 som binært tal.

			Adgangsregler	
Fil	**Fil-id**	**SFID**	**Læs/vælg**	**Opdater**
└─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

Følgende forkortelse for sikkerhedsbetingelsen anvendes i denne tabel:

SC1 ALW OR SM-MAC-G2

TCS_153 Alle elementærfilers strukturer skal være transparente.

TCS_154 Førerkortapplikationen af anden generation skal have følgende datastruktur:

▼B

Fil/dataelement	Antal poster	Størrelse (bytes) Min	Max	Standard-værdier
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 Følgende værdier, der er anvendt som størrelsesangivelser i ovenstående tabel, er mindste og største antal poster i førerkortets datastruktur for en applikation af anden generation:

		Min	Max
n_1	NoOfEventsPerType	6	12
n_2	NoOfFaultsPerType	12	24
n_3	NoOfCardVehicleRecords	84	200
n_4	NoOfCardPlaceRecords	84	112
n_6	CardActivityLengthRange	5 544 bytes (28 døgn med 93 aktivitetsskift)	13 776 Bytes (28 døgn med 240 aktivitetsskift)
n_7	NoOfCardVehicleUnitRecords	84	200
n_8	NoOfGNSSCDRecords	252	336
n_9	NoOfSpecificConditionRecords	56	112

4.3. **Værkstedskortapplikationer**

4.3.1 *Værkstedskortsapplikation af første generation*

TCS_156 Efter at værkstedskortapplikationen af første generation er personaliseret, skal den have følgende permanente filstruktur og filadgangsregler:

▼B

		Adgangsregler		
Fil	**Fil-id**	**Læs**	**Vælg**	**Opdater**
└─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

Følgende forkortelser for sikkerhedsbetingelserne anvendes i denne tabel:

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 For kommandoen READ BINARY med lige INS-byte:

(PLAIN-C AND SM-R-ENC-G1) OR (SM-C-MAC-G1 AND SM-R-ENC-MAC-G1) OR

(SM-C-MAC-G2 AND SM-R-ENC-MAC-G2)

For kommandoen READ BINARY med ulige INS-byte (hvis den understøttes): NEV

TCS_157 Alle elementærfilers strukturer skal være transparente.

TCS_158 Værkstedskortsapplikationen af første generation skal have følgende datastruktur:

▼B

Fil/dataelement	Antal poster	Størrelse (bytes) Min	Max	Standard-værdier
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 Følgende værdier, der er anvendt som størrelsesangivelser i ovenstående tabel, er mindste og største antal poster i værkstedskortets datastruktur for en applikation af første generation:

		Min	Max
n_1	NoOfEventsPerType	3	3
n_2	NoOfFaultsPerType	6	6
n_3	NoOfCardVehicleRecords	4	8
n_4	NoOfCardPlaceRecords	6	8
n_5	NoOfCalibrationRecords	88	255
n_6	CardActivityLengthRange	198 bytes (1 dag med 93 aktivitetsskift)	492 bytes (1 dag med 240 aktivitetsskift)

4.3.2 *Værkstedskortsapplikation af anden generation*

TCS_160 Efter at værkstedskortapplikationen af anden generation er personaliseret, skal den have følgende permanente filstruktur og filadgangsregler:

Bemærk: Det korte id for elementærfilen (SFID) gives som decimaltal. F.eks. svarer værdien 30 til 11110 som binært tal.

			Adgangsregler		
Fil	**Fil-id**	**SFID**	**Læs**	**Vælg**	**Opdater**
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

Følgende forkortelser for sikkerhedsbetingelserne anvendes i denne tabel:

SC1 ALW OR SM-MAC-G2

SC5 For kommandoen Read Binary med lige INS-byte: SM-C-MAC-G2 AND SM-R-ENC-MAC-G2

For kommandoen Read Binary med ulige INS-byte (hvis den understøttes): NEV

TCS_161 Alle elementærfilers strukturer skal være transparente.

TCS_162 Værkstedskortsapplikationen af anden generation skal have følgende datastruktur:

Fil/dataelement	Antal poster	Størrelse (bytes) Min	Max	Standard-værdier
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 Følgende værdier, der er anvendt som størrelsesangivelser i ovenstående tabel, er mindste og største antal poster i værkstedskortets datastruktur for en applikation af anden generation:

		Min	Max
n_1	NoOfEventsPerType	3	3
n_2	NoOfFaultsPerType	6	6
n_3	NoOfCardVehicleRecords	4	8
n_4	NoOfCardPlaceRecords	6	8
n_5	NoOfCalibrationRecords	88	255
n_6	CardActivityLengthRange	198 bytes (1 dag med 93 aktivitetsskift)	492 bytes (1 dag med 240 aktivitetsskift)
n_7	NoOfCardVehicleUnitRecords	4	8
n_8	NoOfGNSSCDRecords	18	24
n_9	NoOfSpecificConditionRecords	2	4

4.4. Kontrolkortapplikationer

4.4.1 *Kontrolkortapplikation af første generation*

TCS_164 Efter at kontrolkortapplikationen af første generation er personaliseret, skal den have følgende permanente filstruktur og filadgangsregler:

		Adgangsregler		
Fil	**Fil-id**	**Læs**	**Vælg**	**Opdater**
└─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

Følgende forkortelser for sikkerhedsbetingelserne anvendes i denne tabel:

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 Alle elementærfilers strukturer skal være transparente.

TCS_166 Kontrolkortapplikationen af første generation skal have følgende datastruktur:

▼B

Fil/dataelement	Antal poster	Størrelse (bytes) Min	Max	
DF Tachograph		*11186*	*24526*	
EF Application_Identification		*5*	*5*	
ControlCardApplicationIdentification		*5*	*5*	
typeOfTachographCardId		1	1	{00}
cardStructureVersion		2	2	{00 00}
noOfControlActivityRecords		2	2	{00 00}
EF Card_Certificate		*194*	*194*	
CardCertificate		194	194	{00..00}
EF CA_Certificate		*194*	*194*	
MemberStateCertificate		194	194	{00..00}
EF Identification		*211*	*211*	
CardIdentification		*65*	*65*	
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
cardIssuingAuthorityName		36	36	{00, 20..20}
cardIssueDate		4	4	{00..00}
cardValidityBegin		4	4	{00..00}
cardExpiryDate		4	4	{00..00}
ControlCardHolderIdentification		*146*	*146*	
controlBodyName		36	36	{00, 20..20}
controlBodyAddress		36	36	{00, 20..20}
cardHolderName				
holderSurname		36	36	{00, 20..20}
holderFirstNames		36	36	{00, 20..20}
cardHolderPreferredLanguage		2	2	{20 20}
EF Controller_Activity_Data		*10582*	*23922*	
ControlCardControlActivityData		*10582*	*23922*	
controlPointerNewestRecord		2	2	{00 00}
controlActivityRecords		*10580*	*23920*	
controlActivityRecord	n_7	*46*	*46*	
controlType		1	1	{00}
controlTime		4	4	{00..00}
controlledCardNumber				
cardType		1	1	{00}
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
controlledVehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
controlDownloadPeriodBegin		4	4	{00..00}
controlDownloadPeriodEnd		4	4	{00..00}

TCS_167 Følgende værdier, der er anvendt som størrelsesangivelser i ovenstående tabel, er mindste og største antal poster i kontrolkortets datastruktur for en applikation af første generation:

		Min	Max
n_7	NoOfControlActivityRecords	230	520

4.4.2 *Kontrolkortapplikation af anden generation*

TCS_168 Efter at kontrolkortapplikationen af anden generation er personaliseret, skal den have følgende permanente filstruktur og filadgangsregler:

Bemærk: Det korte id for elementærfilen (SFID) gives som decimaltal. F.eks. svarer værdien 30 til 11110 som binært tal.

▼B

			Adgangsregler	
Fil	**Fil-id**	**SFID**	**Læs/vælg**	**Opdater**
└─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

Følgende forkortelse for sikkerhedsbetingelsen anvendes i denne tabel:

SC1 ALW OR SM-MAC-G2

TCS_169 Alle elementærfilers strukturer skal være transparente.

TCS_170 Kontrolkortapplikationen af anden generation skal have følgende datastruktur:

Fil/dataelement	**Antal poster**	**Størrelse (bytes) Min**	**Max**	
└─DF Tachograph_G2		*11410*	*25161*	
├─EF Application_Identification		*5*	*5*	
│ └─ControlCardApplicationIdentification		*5*	*5*	
│ ├─typeOfTachographCardId		1	1	{00}
│ ├─cardStructureVersion		2	2	{00 00}
│ └─noOfControlActivityRecords		2	2	{00 00}
├─EF CardMA_Certificate		*204*	*341*	
│ └─CardMACertificate		204	341	{00..00}
├─EF CA_Certificate		*204*	*341*	
│ └─MemberStateCertificate		204	341	{00..00}
├─EF Link_Certificate		*204*	*341*	
│ └─LinkCertificate		204	341	{00..00}
├─EF Identification		*211*	*211*	
│ ├─CardIdentification		*65*	*65*	
│ │ ├─cardIssuingMemberState		1	1	{00}
│ │ ├─cardNumber		16	16	{20..20}
│ │ ├─cardIssuingAuthorityName		36	36	{00, 20..20}
│ │ ├─cardIssueDate		4	4	{00..00}
│ │ ├─cardValidityBegin		4	4	{00..00}
│ │ └─cardExpiryDate		4	4	{00..00}
│ └─ControlCardHolderIdentification		*146*	*146*	
│ ├─controlBodyName		36	36	{00, 20..20}
│ ├─controlBodyAddress		36	36	{00, 20..20}
│ ├─cardHolderName				
│ │ ├─holderSurname		36	36	{00, 20..20}
│ │ └─holderFirstNames		36	36	{00, 20..20}
│ └─cardHolderPreferredLanguage		2	2	{20 20}
└─EF Controller_Activity_Data		*10582*	*23922*	
└─ControlCardControlActivityData		*10582*	*23922*	
├─controlPointerNewestRecord		2	2	{00 00}
└─controlActivityRecords		*10580*	*23920*	
└─controlActivityRecord	n_7	*46*	*46*	
├─controlType		1	1	{00}
├─controlTime		4	4	{00..00}
├─controlledCardNumber				
│ ├─cardType		1	1	{00}
│ ├─cardIssuingMemberState		1	1	{00}
│ └─cardNumber		16	16	{20..20}
├─controlledVehicleRegistration				
│ ├─vehicleRegistrationNation		1	1	{00}
│ └─vehicleRegistrationNumber		14	14	{00, 20..20}
├─controlDownloadPeriodBegin		4	4	{00..00}
└─controlDownloadPeriodEnd		4	4	{00..00}

TCS_171 Følgende værdier, der er anvendt som størrelsesangivelser i ovenstående tabel, er mindste og største antal poster i kontrolkortets datastruktur for en applikation af anden generation:

▼B

		Min	Max
n_7	NoOfControlActivityRecords	230	520

4.5. Virksomhedskortapplikationer

4.5.1 *Virksomhedskortapplikation af første generation*

TCS_172 Efter at virksomhedskortapplikationen af første generation er personaliseret, skal den have følgende permanente filstruktur og filadgangsregler:

		Adgangsregler		
Fil	**Fil-id**	**Læs**	**Vælg**	**Opdater**
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

Følgende forkortelser for sikkerhedsbetingelserne anvendes i denne tabel:

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 Alle elementærfilers strukturer skal være transparente.

TCS_174 Virksomhedskortapplikationen af første generation skal have følgende datastruktur:

Fil/dataelement	Antal poster	Størrelse (bytes) Min	Max	Standard-værdier
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 Følgende værdier, der er anvendt som størrelsesangivelser i ovenstående tabel, er mindste og største antal poster i virksomhedskortets datastruktur for en applikation af første generation:

		Min	Max
n_8	NoOfCompanyActivityRecords	230	520

4.5.2 *Virksomhedskortapplikation af anden generation*

TCS_176 Efter at virksomhedskortapplikationen af anden generation er personaliseret, skal den have følgende permanente filstruktur og filadgangsregler:

Bemærk: Det korte id for elementærfilen (SFID) gives som decimaltal. F.eks. svarer værdien 30 til 11110 som binært tal.

			Adgangsregler	
Fil	**Fil-id**	**SFID**	**Læs/vælg**	**Opdater**
└─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

Følgende forkortelse for sikkerhedsbetingelsen anvendes i denne tabel:

SC1 ALW OR SM-MAC-G2

TCS_177 Alle elementærfilers strukturer skal være transparente.

TCS_178 Virksomhedskortapplikationen af anden generation skal have følgende datastruktur:

Fil/dataelement	**Antal poster**	**Størrelse (bytes) Min**	**Max**	**Standard-værdier**
└─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 Følgende værdier, der er anvendt som størrelsesangivelser i ovenstående tabel, er mindste og største antal poster i virksomhedskortets datastruktur for en applikation af anden generation:

		Min	Max
n_8	NoOfCompanyActivityRecords	230	520

▼B

Tillæg 3

PIKTOGRAMMER

PIC_001 Der kan til takografen anvendes følgende piktogrammer og piktogramkombinationer (eller piktogrammer og kombinationer, som svarer tilstrækkeligt til dem til at være entydigt identificerbare som dem):

1. BASISPIKTOGRAMMER

	Mennesker	**Handlinger**	**Funktionstilstande**
	Virksomhed		Virksomhedstilstand
	Tilsynsførende	Kontrol	Kontroltilstand
	Fører	Kørsel	Driftstilstand
	Værksted/prøvestation	Eftersyn/kalibrering	Kalibreringstilstand
	Fabrikant		

	Aktiviteter	**Varighed**
	Til rådighed	Aktuel rådighedsperiode
	Kørsel	Kontinuerlig køretid
	Hvile	Aktuel hvileperiode
	Andet arbejde	Aktuel arbejdsperiode
	Pause	Akkumuleret pausetid
	Ukendt	

	Udstyr	**Funktioner**
	Førerkortplads	
	Kortplads for medchauffør	
	Kort	
	Ur	
	Skærm	Visning på skærm
	Overførsel til eksternt lager	Dataoverførsel
	Strømforsyning	
	Printer/udskrift	Trykning
	Føler	
	Dækstørrelse	
	Køretøj/køretøjsenhed	
	GNSS-udstyr	
	Udstyr til fjernkommunikation	
	ITS-grænseflade	

▼B

	Særlige omstændigheder
OUT	Uden for gyldighedsområde
	Overfart med færge/tog

	Diverse		
!	Hændelser		Fejl
	Den daglige arbejdstids begyndelse		Den daglige arbejdstids afslutning
	Sted		
M	Manuel indlæsning af føreraktiviteter		
	Sikkerhed		
	Hastighed		
	Tid		
Σ	Total/sum		

	Angivelse
24t	Dagligt
I	Ugentligt
II	Hver anden uge
+	Fra eller til

2. KOMBINATIONER AF PIKTOGRAMMER

	Diverse		
	Kontrolsted		
	Sted, hvor den daglige arbejdstid begynder		Sted, hvor den daglige arbejdstid slutter
+	Fra tidspunkt	+	Til tidspunkt
+	Fra køretøj		
OUT+	Uden for gyldighedsområde (start)	+OUT	Uden for gyldighedsområde (slut)

	Kort
	Førerkort
	Virksomhedskort
	Kontrolkort
	Værkstedskort
– – –	Intet kort

	Kørsel
	Førerholdkørsel
I	Køretid for én uge
II	Køretid for to uger

▼B

	Udskrifter
	Daglig udskrift af føreraktivitet fra kort
	Daglig udskrift af føreraktivitet fra VU
	Udskrift af hændelser og fejl fra kort
	Udskrift af hændelser og fejl fra VU
	Udskrift af tekniske data
	Udskrift af overskridelse af tilladt hastighed
	Begivenheder
	Isætning af ugyldigt kort
	Kortkonflikt
	Tidsoverlapning
	Kørsel uden behørigt kort
	Isætning af kort under kørslen
	Seneste kortsession ikke korrekt afsluttet
	Overskridelse af tilladt hastighed
	Strømforsyningssvigt
	Fejl ved køredata
	Køretøjsbevægelseskonflikt
	Sikkerhedsbrud
	Justering af klokkeslæt (foretaget af værksted)
	Kontrol af overskridelse af tilladt hastighed
	Fejl
	Kortfejl (førerkortplads)
	Kortfejl (medchaufførs kortplads)
	Displayfejl
	Dataoverførselsfejl
	Printerfejl
	Følerfejl
	Intern fejl i VU
	GNSS-fejl
	Fejl ved fjernkommunikation
	Manuel indlæsning
	Stadig samme daglige arbejdsperiode?
	Slut på foregående arbejdsperiode?
	Bekræft eller indlæs sted, hvor daglig arbejdsperiode slutter
	Indlæs starttidspunkt
	Indlæs sted, hvor daglig arbejdsperiode begynder.

Bemærk: Andre kombinationer af piktogrammer, som danner udskrivningsgrupper eller datanavne for poster, er givet i tillæg 4.

▼B

Tillæg 4

UDSKRIFTER

INDHOLDSFORTEGNELSE

1. GENERELT

2. SPECIFIKATION AF DATAGRUPPER

3. SPECIFIKATION AF UDSKRIFTER

3.1. Daglig udskrift af føreraktivitet fra kort

3.2. Daglig udskrift af føreraktivitet fra køretøjsenhed

3.3. Udskrift af hændelser og fejl fra kort

3.4. Udskrift af hændelser og fejl fra køretøjsenhed

3.5. Udskrift af tekniske data

3.6. Udskrift af overskridelse af tilladt hastighed

3.7 Historik over isatte kort

1. GENERELT

Hver udskrift er opbygget ved kædning af forskellige datagrupper, om muligt identificeret med en gruppeidentifikator.

En datagruppe indeholder en eller flere poster, eventuelt identificeret ved en postidentifikator.

PRT_001 Når en gruppeidentifikator står umiddelbart foran en post-identifikator, bliver postidentifikatoren ikke udskrevet.

PRT_002 Når et dataelement er ukendt eller ikke må udskrives af grunde vedrørende dataadgang, udskrives mellemrum i stedet.

PRT_003 Hvis indholdet af en hel linje er ukendt eller ikke behøver udskrives, udelades hele linjen.

PRT_004 Numeriske datafelter udskrives højrejusteret, med mellemrum som skilletegn for tusinder og millioner, og uden foranstillede nuller.

PRT_005 Strengdatafelter udskrives venstrejusteret og udfyldt med mellemrum til dataelementets længde eller om nødvendigt afkortet til dataelementets længde (navn og adresse).

PRT_006 I tilfælde af et linjeskift på grund af et langt tekststykke, skal et specialtegn (en prik midt på linjen (i højden) ”•”) udskrives som det første tegn på den næste linje.

2. SPECIFIKATION AF DATAGRUPPER

I dette kapitel er anvendt følgende notationsregler for format:

— Tegn med **fede** typer angiver almindelig tekst, som skal udskrives (udskrives med normale tegn)

▼B

— Normale typer angiver variable (piktogrammer eller data) som ved udskrivning skal erstattes med deres værdi

— Variabelnavne er omgivet af understregningstegn for at angive den længde, som dataelementer for den pågældende variabel kan have

— Datoer angives i formatet ”dd/mm/yyyy” (dag, måned, år) Formatet ”dd.mm.yyyy” kan også anvendes

— Betegnelsen ”kortidentifikation” angiver sammensætningen af kortets type gennem en kombination af kortpiktogrammer, den kortudstedende medlemsstats kode, en normal skråstreg og kortets nummer med udskiftningsindekset og fornyelsesindekset adskilt af et mellemrum:

P	■	x	x	x	/	x	x	x	x	x	x	x	x	x	x	x	x	x		x		x
Kombination af kort og piktogram		Udstedende medlemsstats kode				De første 14 tegn i kortnummeret (eventuelt inkl. et fortløbende indeks)														Udskiftningsindeks		Fornyelsesindeks

▼B

PRT_007 Udskrifter skal anvende følgende datablokke og/eller dataposter i overensstemmelse med følgende betydninger og formater:

Datagruppe eller registreringsnummer Betydning	Dataformat
1 ***Dato og tidspunkt for udskrivning af dokumentet***	▼ dd/mm/yyyy hh:mm **(UTC)**
2 ***Udskriftens art*** Datagruppeidentifikator Piktogramkombination i udskrift (se tillæg 3), hastighedsbegrænserens indstilling (kun ved udskrivning af overskridelse af tilladt hastighed)	----------▼---------- Picto xxx **km/h**
3 ***Identifikation af kortindehaver*** Datagruppeidentifikator. P = piktogram for personer Kortindehaverens efternavn Kortindehaverens eventuelle fornavn(e) Identifikation af kort Eventuel udløbsdato for kortet og angivelse af kortgeneration (GEN 1 eller GEN 2) (*)	----------P---------- P Last_Name_____ First_Name_____ Card_Identification_____ dd/mm/yyyy – GEN 2

Er kortet ikke et personligt kort og ikke påført kortindehaverens efternavn, skal der i stedet herfor udskrives virksomhedens, værkstedets eller kontrolorganets navn.

(*) Kortgeneration kan kun udskrives af intelligente takografer.

4 ***Identifikation af køretøj*** Datagruppeidentifikator VIN Registrerende medlemsstat og køretøjets registreringsnummer	----------🚙---------- 🚙 VIN_____ Nat/VRN_____
5 ***Identifikation af køretøjsenhed*** Datagruppeidentifikator Køretøjsfabrikantens navn Reservedelsnummer for køretøjsenhed Angivelse af generation for køretøjsenhed (*)	----------⊟---------- ⊟ VU_Manufacturer_____ VU_Part_Number__ GEN 2

(*) Kortgeneration kan kun udskrives af intelligente takografer.

6 ***Seneste kalibrering af takografen*** Datagruppeidentifikator Værkstedets navn Identifikation af værkstedskort Dato for seneste kalibrering	----------🔧---------- 🔧 Last_Name_____ Card_Identification_____ 🔧 dd/mm/yyyy

▼B

7	***Seneste kontrol (ved en tilsynsførende)***	
	Datagruppeidentifikator	----------▯----------
	Identifikation af tilsynsførendes kort	Card_Identification_____
	Kontroldato, -klokkeslæt og -art	▯ dd/mm/yyyy hh:mm ppppp

Kontrollens art: Op til fem piktogrammer. Kontrollens art kan være følgende eller en kombination deraf:

▪: Dataoverførsel, kort, ↧: Dataoverførsel, køretøjsenhed, ▼: udskrivning, □: Visning på skærm, ⊤: Kalibreringskontrol ved vejsiden

8	***Føreraktiviteter, gemt på kortet, i kronologisk rækkefølge***	
	Datagruppeidentifikator	----------⊙----------
	Forespørgselsdato (kalenderdag, som udskriften omhandler) + tæller for daglig tilstedeværelse af kort	dd/mm/yyyy xxx
8a	*Betingelsen "uden for gyldighedsområde" ved den aktuelle dags begyndelse* (står tom, hvis betingelsen "uden for gyldighedsområde" ikke er åbnet)	----------OUT----------
8.1	*Periode, hvor kortet ikke var isat*	
8.1a	Postidentifikator (periodens start)	----------
8.1b	*Ukendt periode*. Starttid, varighed	? hh:mm hh**h**mm
8.1c	*Aktivitet indlæst manuelt*	A hh:mm hh**h**mm
	Aktivitetspiktogram, starttid, varighed	
8.2	*Indsætning af kort i kortplads S*	
	Postidentifikator; S = Kortpladspiktogram	---------S---------
	Registrerende medlemsstat og køretøjets registreringsnummer	Nat/VRN_____
	Køretøjets kilometerstand ved isætning af kortet	x xxx xxx **km**
8.3	*Aktivitet (mens kortet var isat)*	
	Aktivitetspiktogram, starttid, varighed, førerholdstatus (førerholdspiktogram hvis FØRERHOLD, blanke hvis ÉN FØRER)	A hh:mm hhhmm ⊙⊙
8.3a	*Særlig omstændighed*. Indlæsningstidspunkt, piktogram (eller piktogramkombination) for særlige omstændigheder.	hh:mm ---pppp---
8.4	*Udtagning af kort*	
	Køretøjets kilometerstand og tilbagelagt distance siden sidste isætning ved kendt kilometerstand	x xxx xxx **km**; x xxx **km**

9	***Føreraktiviteter, lagret i køretøjsenheden for hver kortplads i kronologisk rækkefølge***	
	Datagruppeidentifikator	----------⊙----------
	Forespørgselsdato (kalenderdag, som udskriften omhandler)	dd/mm/yyyy
	Køretøjets kilometerstand ved kl. 00:00 og 24:00	x xxx xxx - x xxx xxx **km**

10	***Aktiviteter, som er registreret i kortplads S***	
	Datagruppeidentifikator	----------S----------
10a	*Betingelsen "uden for gyldighedsområde" ved den aktuelle dags begyndelse* (står tom, hvis betingelsen "uden for gyldighedsområde" ikke er åbnet)	----------OUT----------
10.1	*Periode, hvor der ikke har været isat et kort i kortplads S*	
	Postidentifikator.	----------
	Intet kort isat	⊙▪---
	Køretøjets kilometerstand ved periodens begyndelse	x xxx xxx **km**
10.2	*Isætning af kort*	
	Postidentifikator for isætning af kort	----------
	Førerens efternavn	⊙ Last_Name_____

▼B

	Førerens fornavn	First_Name_____
	Identifikation af førerkort	Card_Identification_____
	Eventuel udløbsdato for kortet og angivelse af kortgeneration (GEN 1 eller GEN 2) (*)	dd/mm/yyyy - GEN 2
	Registrerende medlemsstat og indregistreringsnummer for det foregående køretøj, som er anvendt	Nat/VRN_____
	Dato og klokkeslæt for udtagning af kortet af det foregående køretøj	dd/mm/yyyy hh:mm
	Tom linje	
	Køretøjets kilometerstand ved isætning af kortet, manuel indlæsning af flag for føreraktivet (M for ja, blank for nej).	x xxx xxx **km** M
	Hvis der ikke er isat noget førerkort den dag, for hvilken udskriften foretages, anvendes for datagruppe 10.2 kilometerstanden fra den sidste tilgængelige kortisætning før denne dag	
10.3	*Aktivitet*	
	Aktivitetspiktogram, starttid, varighed, førerholdstatus (førerholdspiktogram hvis FØRERHOLD, blanke hvis ÉN FØRER)	A hh:mm hh**h**mm ⊙⊙
10.3a	*Særlig omstændighed*. Indlæsningstidspunkt, piktogram (eller piktogramkombination) for særlige omstændigheder.	hh:mm ---pppp---
10.4	*Udtagning af kort eller slutning på "intet kort" periode*	
	Køretøjets kilometerstand ved udtagning af kortet eller ved slutningen af "intet kort"-perioden, og tilbagelagt distance siden isætning eller siden "intet kort"-periodens begyndelse.	x xxx xxx **km**; x xxx **km**

(*) Kortgeneration kan kun udskrives af intelligente takografer.

11	***Døgnoversigt***	
	Datagruppeidentifikator	----------Σ----------
11.1	***Køretøjsenhedens oversigt over perioder uden kort i førerens kortplads***	
	Datagruppeidentifikator	1⊙▬---
11.2	***Køretøjsenhedens oversigt over perioder uden kort i medchaufførens kortplads***	
	Datagruppeidentifikator	2⊙▬---
11.3	***Køretøjsenhedens døgnoversigt for hver fører***	
	Postidentifikator	----------
	Førerens efternavn	⊙ Last_Name_____
	Førerens fornavn(e)	First_Name_____
	Identifikation af førerkort	Card_Identification_____
11.4	*Indlæsning af sted, hvor daglig arbejdstid begynder og/eller slutter*	
	pi = piktogram for sted begynder/slutter, tidspunkt, land, region	pihh:mm Cou Reg
	Kilometerstand	x xxx xxx **km**
11.5	*Indlæsning af sted, hvor daglig arbejdstid begynder og/eller slutter*	
	og efter tre timers sammenhængende køretid	⁘ hh:mm
	Kilometerstand	x xxx xxx **km**

11.6	*Aktivitet i alt (fra et kort)*	
	Total varighed af kørsel, tilbagelagt distance	⊙ hh**h**mm x xxx **km**
	Total varighed af arbejde og rådighed	⚒ hh**h**mm ⧈ hh**h**mm
	Total varighed af hvile og ukendt	⊢ hh**h**mm ? hh**h**mm
	Total varighed af førerholdsaktiviteter	⊙⊙ hh**h**mm
11.7	*Totalværdier for aktivitet (perioder uden kort i førerens kortplads)*	
	Total varighed af kørsel, tilbagelagt distance	⊙ hh**h**mm x xxx **km**
	Total varighed af arbejde og rådighed	⚒ hh**h**mm ⧈ hh**h**mm
	Total varighed af hvile	⊢ hh**h**mm

▼B

11.8	*Totalværdier for aktivitet (perioder uden kort i medchaufførens kortplads)*	
	Total varighed af arbejde og rådighed	* hhhmm ⧈ hhhmm
	Total varighed af hvile	⊢ hhhmm
11.9	*Aktivitet i alt (pr. chauffør, begge kortpladser medregnet)*	
	Total varighed af kørsel, tilbagelagt distance	⊙ hhhmm x xxx km
	Total varighed af arbejde og rådighed	* hhhmm ⧈ hhhmm
	Total varighed af hvile	⊢ hhhmm
	Total varighed af førerholdsaktiviteter	⊙⊙ hhhmm

Når der kræves daglig udskrift for det aktuelle døgn, beregnes daglig sammenfatning med de data, der foreligger på udskrivningstidspunktet.

12	***Hændelser og/eller fejl, som er gemt på et kort***	
12.1	Datagruppeidentifikator for seneste fem "hændelser og fejl" fra et kort	----------!×▪----------
12.2	Datagruppeidentifikator for alle registrerede "hændelser" på et kort	----------!▪----------
12.3	Datagruppeidentifikator for alle registrerede "fejl" på et kort	----------×▪----------
12.4	*Post vedrørende hændelser og/eller fejl*	
	Postidentifikator	----------
	Piktogram for hændelser/fejl, postens formål, startdato og -klokkeslæt	Pic (p) dd/mm/yyyy hh:mm
	Eventuel supplerende fejl-/hændelseskode, varighed	!xx hhhmm
	Registrerende medlemsstat og registreringsnummer for det køretøj, hvor hændelsen eller fejlen optrådte	Nat/VRN_____

13	***Hændelser og/eller fejl, som er gemt eller er igangværende på en køretøjsenhed***	
13.1	Datagruppeidentifikator for seneste fem "hændelser og fejl" fra køretøjsenheden	----------!×▲----------
13.2	Datagruppeidentifikator for alle registrerede eller igangværende "hændelser" på en køretøjsenhed	----------!▲----------
13.3	Datagruppeidentifikator for alle registrerede eller igangværende "fejl" på en køretøjsenhed	----------×▲----------
13.4	*Post vedrørende hændelser og/eller fejl*	
	Postidentifikator	----------
	Piktogram for hændelser/fejl, postens formål, startdato og -klokkeslæt	Pic (p) dd/mm/yyyy hh:mm
	Eventuel supplerende fejl-/hændelseskode, antal tilsvarende hændelser det pågældende døgn, varighed	!xx (xxx) hhhmm
	Identifikation af de kort, der er indsat ved begyndelsen eller enden på hændelsen eller fejlen (indtil fire linjer uden to gentagelser af de samme kortnumre)	Card_Identification_____ Card_Identification_____ Card_Identification_____ Card_Identification_____
	Tilfælde, hvor intet kort var isat	▪---
	Fabrikantspecifikke data	< Literal><ErrorCode>

Postens formål (p) er en numerisk kode, som forklarer, hvorfor hændelsen eller fejlen blev registreret, og som er kodet i henhold til dataelementet `EventFaultRecordPurpose`.

`Literal` er en streng bestående af højst 12 tegn, som er anført af fabrikanten af takografen.

`ErrorCode` er en fejlkode bestående af højst 12 tegn, som er anført af fabrikanten af takografen.

▼B

14	***Identifikation af køretøjsenhed***	
	Datagruppeidentifikator	`----------B----------`
	Navn på fabrikanten af køretøjsenheden	`B Name_____`
	Adresse på fabrikanten af køretøjsenheden	`Address_____`
	Reservedelsnummer for køretøjsenhed	`PartNumber_____`
	Godkendelsesnummer for køretøjsenhed	`Apprv_____`
	Serienummer på køretøjsenhed	`S/N_____`
	Fabrikationsår på køretøjsenheden	`yyyy`
	Version og installationsdato for køretøjsenhedens programmel	`V xxxx dd/mm/yyyy`
15	***Identifikation af sensor***	
	Datagruppeidentifikator	`----------Л----------`
15.1	*Parringspost*	
	Serienummer på sensor	`Л S/N_____`
	Godkendelsesnummer på sensor	`Apprv_____`
	Dato for første parring af sensoren	`dd/mm/yyyy hh:mm`
16	***GNSS-identifikation***	
	Datagruppeidentifikator	`----------▚----------`
16.1	*Forbindelsespost*	
	Serienummer på eksternt GNSS-udstyr	`▚ S/N_____`
	Godkendelsesnummer på eksternt GNSS-udstyr	`Apprv_____`
	Forbindelsesdato for eksternt GNSS-udstyr	`dd/mm/yyyy hh:mm`
17	***Kalibreringsdata***	
	Datagruppeidentifikator	`----------T----------`
17.1	*Kalibreringspost*	
	Postidentifikator	`--------------------`
	Det værksted, der har foretaget kalibreringen	`T Workshop_name_____`
	Værkstedets adresse	`Workshop_address_____`
	Identifikation af værkstedskort	`Card_Identification_____`
	Værkstedskortets udløbsdato	`dd/mm/yyyy`
	Tom linje	
	Kalibreringsdato + kalibreringens formål	`T dd/mm/yyyy (p)`
	VIN	`Д VIN_____`
	Registrerende medlemsstat og VRN	`Nat/VRN_____`
	Køretøjets vejdrejetal	`w xx xxx Imp/km`
	Kontrolapparatets konstant	`k xx xxx Imp/km`
	Effective circumference of wheel tyres	`l xx xxx mm`
	Størrelse på monterede dæk	`● TyreSize_____`
	Hastighedsbegrænserens indstilling	`> xxx km/h`
	Gamle og nye værdier af kilometerstanden	`x xxx xxx - x xxx xxx km`

Kalibreringens formål (p) er en numerisk kode, som forklarer, hvorfor de pågældende kalibreringsparametre blev registreret, og som er kodet i henhold til dataelementet `CalibrationPurpose`.

▼B

18	***Tidsjustering***	
	Datagruppeidentifikator	`----------◷----------`
18.1	*Tidsjusteringspost*	
	Postidentifikator	`--------------------`
	Gammel dato og gammelt klokkeslæt	`!◷ dd/mm/yyyy hh:mm`
	Ny dato og nyt klokkeslæt	`◷ dd/mm/yyyy hh:mm`
	Det værksted, der har foretaget tidsjusteringen	`T Workshop_name_____`
	Værkstedets adresse	`Workshop_address_____`
	Identifikation af værkstedskort	`Card_Identification_____`
	Værkstedskortets udløbsdato	`dd/mm/yyyy`
19	***Den seneste hændelse og fejl, som er registreret i køretøjsenheden***	
	Datagruppeidentifikator	`----------!×A----------`
	Dato og klokkeslæt for seneste hændelse	`! dd/mm/yyyy hh:mm`
	Dato og klokkeslæt for seneste fejl	`× dd/mm/yyyy hh:mm`
20	***Information vedrørende overskridelse af tilladt hastighed***	
	Datagruppeidentifikator	`----------»»----------`
	Dato og klokkeslæt for seneste KONTROL FOR OVERSKRIDELSE AF TILLADT HASTIGHED	`»dd/mm/yyyy hh:mm`
	Dato/klokkeslæt for første overskridelse af tilladt hastighed og antal hændelser med overskridelse af tilladt hastighed siden da	`»»dd/mm/yyyy hh:mm (nnn)`
21	***Post vedrørende overskridelse af tilladt hastighed***	
21.1	Datagruppeidentifikatoren "Første overskridelse af tilladt hastighed efter seneste kalibrering"	`--------»»T---------`
21.2	Datagruppeidentifikatoren "De fem alvorligste hændelser inden for de sidste 365 dage"	`-------»»(365)------`
21.3	Datagruppeidentifikatoren "Den alvorligste hændelse for hver af de 10 seneste dage, den er forekommet"	`-------»»(10)-------`
21.4	Postidentifikator	`--------------------`
	Dato, klokkeslæt og varighed	`»»dd/mm/yyyy hh:mm hhhmm`
	Maks. og gennemsnitlige hastigheder, antal lignende hændelser denne dag	`xxx km/h xxx km/h(xxx)`
	Førerens efternavn	`Last_Name_____`
	Førerens fornavn(e)	`First_Name_____`
	Identifikation af førerkort	`Card_Identification_____`
21.5	Hvis der ikke findes nogen post for overskridelse af tilladt hastighed i en gruppe	`»»---`
22	***Håndskrevne oplysninger***	
	Datagruppeidentifikator	`------------------------`
22.1	Kontrolsted	`•  .....`
22.2	Den tilsynsførendes underskrift	`  .....`
22.3	Fra tidspunkt	`◷+ .....`
22.4	Til tidspunkt	`+◷ .....`
22.5	Førerens underskrift	`  .....`

Vedr. "håndskrevne oplysninger": Indsæt tilstrækkelig mange tomme linjer oven over en håndskreven post til at kunne skrive de nødvendige oplysninger eller en underskrift.

▼B

23 ***Seneste kort, som er isat køretøjsenheden***

Datagruppeidentifikator

23.1 Isat kort

Postidentifikator

Korttype, generation, version, fabrikant (*)

Kortidentifikation

Kortets serienummer

Dato og klokkeslæt for sidste isætning af kort

```
-------- ⊟◨◷ --------


----
↑ <gen> <version> <MC>
Card Identification
Card Serial Number
dd/mm/yyyy hh:mm
```

(*) (det hele på én linje)

med

korttype: Piktogram, ét tegn + mellemrum

generation: GEN1 eller GEN2, 4 tegn + mellemrum

version: op til 10 tegn

MC: fabrikantkode, 3 tegn

3. SPECIFIKATION AF UDSKRIFTER

I dette kapitel er anvendt følgende notationsregler for format:

N	Udskriv datagruppe- eller postantal N
N	Udskriv datagruppe- eller postantal N, gentaget så mange gange som nødvendigt
X/Y	Udskriv datagruppe eller post X og/eller Y efter behov, gentaget som mange gange som nødvendigt.

3.1. **Daglig udskrift af føreraktivitet fra kort**

PRT_008 Daglig udskrift af føreraktivitet fra kort skal overholde følgende format:

1	Dato og tidspunkt for udskrivning af dokumentet
2	Udskriftens art
3	Identifikation af den tilsynsførende (hvis der er isat et kontrolkort i køretøjsenheden)
3	Identifikation af føreren (fra det kort, som udskriften omhandler + GEN)
4	Identifikation af køretøj (det køretøj, hvorfra udskriften tages)
5	Identifikation af køretøjsenhed (den køretøjsenhed, hvorfra udskriften tages + GEN)
6	Seneste kalibrering af denne køretøjsenhed
7	Seneste kontrol, som den kontrollerede fører har været genstand for
8	Skilletegn for føreraktiviteter
8a	Betingelsen »uden for gyldighedsområde« ved den aktuelle dags begyndelse
8.1a / 8.1b / 8.1c / 8.2 / 8.3 / 8.3a / 8.4	Føreraktiviteter i kronologisk rækkefølge
11	Skilletegn for døgnoversigt

▼B

11.4	Indlæste steder i kronologisk rækkefølge
11.5	GNSS-data
11.6	Aktiviteter, i alt
12.1	Hændelser eller fejl fra skilletegn for kort
12.4	Poster med hændelser/fejl (seneste fem hændelser eller fejl, som er gemt på kortet)
13.1	Hændelser eller fejl fra skilletegn for køretøjsenhed
13.4	Poster med hændelser/fejl (seneste fem hændelser eller fejl, som er gemt eller igangværende på køretøjsenheden)
22.1	Kontrolsted
22.2	Den tilsynsførendes underskrift
22.5	Førerens underskrift

3.2. **Daglig udskrift af føreraktivitet fra køretøjsenhed**

PRT_009 Daglig udskrift af føreraktivitet fra køretøjsenhed skal overholde følgende format:

1	Dato og tidspunkt for udskrivning af dokumentet
2	Udskriftens art
3	Identifikation af kortindehaver (for alle kort isat i køretøjsenhed + GEN)
4	Identifikation af køretøj (det køretøj, hvorfra udskriften tages)
5	Identifikation af køretøjsenhed (den køretøjsenhed, hvorfra udskriften tages + GEN)
6	Seneste kalibrering af denne køretøjsenhed
7	Seneste kontrol på denne takograf
9	Skilletegn for føreraktiviteter
10	Skilletegn for førerkortplads (kortplads 1)
10a	Betingelsen ”uden for gyldighedsområde” ved den aktuelle dags begyndelse
10.1 / 10.2 / 10.3 /10.3a / 10.4	Aktiviteter i kronologisk rækkefølge (førerkortplads)
10	Skilletegn for medchaufførens kortplads (kortplads 2)
10a	Betingelsen ”uden for gyldighedsområde” ved den aktuelle dags begyndelse
10.1 / 10.2 / 10.3 /10.3a / 10.4	Aktiviteter i kronologisk rækkefølge (medchaufførens kortplads)
11	Skilletegn for døgnoversigt
11.1	Oversigt over perioder uden kort i førerens kortplads
11.4	Indlæste steder i kronologisk rækkefølge
11.5	GNSS-data

▼B

11.6	Aktiviteter, i alt
11.2	Oversigt over perioder uden kort i medchaufførens kortplads
11.4	Indlæste steder i kronologisk rækkefølge
11.5	GNSS-data
11.7	Aktiviteter, i alt
11.3	Oversigt over føreraktiviteter, begge kortpladser medregnet
11.4	Steder indlæst af denne fører i kronologisk rækkefølge
11.5	GNSS-data
11.8	Aktiviteter i alt for denne fører
13.1	Skilletegn for hændelser/fejl
12.4	Poster med hændelser/fejl (seneste fem hændelser eller fejl, som er gemt eller igangværende på køretøjsenheden)
13.1	Kontrolsted
22.2	Den tilsynsførendes underskrift
22.3	Fra tidspunkt (plads til rådighed for en fører uden kort til angivelse af de relevante perioder)
22.4	Til tidspunkt
22.5	Førerens underskrift

3.3. **Udskrift af hændelser og fejl fra kort**

PRT_010 Udskrift af hændelser og fejl fra kort skal overholde følgende format:

1	Dato og tidspunkt for udskrivning af dokumentet
2	Udskriftens art
3	Identifikation af den tilsynsførende (hvis der er isat et kontrolkort i køretøjsenheden + GEN)
3	Identifikation af føreren (fra det kort, som udskriften omhandler)
4	Identifikation af køretøj (det køretøj, hvorfra udskriften tages)
12.2	Skilletegn for hændelser
12.4	Hændelsesposter (alle hændelser gemt på kortet)
12.3	Skilletegn for fejl
12.4	Poster vedrørende fejl (alle fejl gemt på kortet)
22.1	Kontrolsted
22.2	Den tilsynsførendes underskrift
22.5	Førerens underskrift

▼B

3.4. **Udskrift af hændelser og fejl fra køretøjsenhed**

PRT_011 Udskrift af hændelser og fejl fra køretøjsenhed skal overholde følgende format:

1	Dato og tidspunkt for udskrivning af dokumentet
2	Udskriftens art
3	Identifikation af kortindehaver (for alle kort isat i køretøjsenhed + GEN)
4	Identifikation af køretøj (det køretøj, hvorfra udskriften tages)
13.2	Skilletegn for hændelser
13.4	Hændelsesposter (alle hændelser, som er gemt eller igangværende på køretøjsenheden)
13.3	Skilletegn for fejl
13.4	Poster vedrørende fejl (alle fejl, som er gemt eller igangværende på køretøjsenheden)
22.1	Kontrolsted
22.2	Den tilsynsførendes underskrift
22.5	Førerens underskrift

3.5. **Udskrift af tekniske data**

PRT_012 Udskrift af tekniske data skal overholde følgende format:

1	Dato og tidspunkt for udskrivning af dokumentet
2	Udskriftens art
3	Identifikation af kortindehaver (for alle kort isat i køretøjsenhed + GEN)
4	Identifikation af køretøj (det køretøj, hvorfra udskriften tages)
14	Identifikation af køretøjsenhed
15	Identifikation af sensor
15.1	Data fra sensorparring (alle tilgængelige data i kronologisk rækkefølge)
16	GNSS-identifikation
16.1	Koblingsdata for eksternt GNSS-udstyr (alle tilgængelige data i kronologisk rækkefølge)
17	Skilletegn for kalibreringsdata
17.1	Kalibreringsposter (alle foreliggende poster i kronologisk rækkefølge)
18	Skilletegn for tidsjustering
18.1	Poster vedrørende tidsjustering (alle poster, som er til rådighed fra tidsjustering og fra kalibreringsdataposter)
19	Den seneste hændelse og fejl, som er registreret i køretøjsenheden

▼B

3.6. **Udskrift af overskridelse af tilladt hastighed**

PRT_013 Udskrift af overskridelser af tilladt hastighed skal overholde følgende format:

1	Dato og tidspunkt for udskrivning af dokumentet
2	Udskriftens art
3	Identifikation af kortindehaver (for alle kort isat i køretøjsenhed + GEN)
4	Identifikation af køretøj (det køretøj, hvorfra udskriften tages)
20	Information vedrørende overskridelse af tilladt hastighed
21.1	Identifikator for data vedrørende overskridelser af tilladt hastighed
21.4/21.5	Første overskridelse af tilladt hastighed efter seneste kalibrering
21.2	Identifikator for data vedrørende overskridelser af tilladt hastighed
21.4/21.5	De 5 alvorligste hændelser med overskridelse af tilladt hastighed inden for de sidste 365 dage
21.3	Identifikator for data vedrørende overskridelser af tilladt hastighed
21.4/21.5	Den alvorligste hændelse vedrørende overskridelse af tilladt hastighed for hver af de 10 seneste dage, den er forekommet
22.1	Kontrolsted
22.2	Den tilsynsførendes underskrift
22.5	Førerens underskrift

3.7. **Historik over isatte kort**

PRT_014 Udskriften af historikken over isatte kort skal overholde følgende format:

1	Dato og tidspunkt for udskrivning af dokumentet
2	Udskriftens art
3	Identifikation af kortindehaver (for alle kort isat i køretøjsenheden)
23	Seneste kort, som er isat køretøjsenheden
23.1	Isatte kort (op til 88 poster)
12.3	Skilletegn for fejl

▼B

Tillæg 5

SKÆRM

I dette tillæg er anvendt følgende notationsregler for format:

— tegn med **fede** typer angiver almindelig tekst, som vises (vises på skærmen med normale typer)

— normale typer angiver variabler (piktogrammer eller data) som på skærmen skal erstattes med deres værdi:

  — dd mm yyyy: dag, måned, år

  — hh: timer

  — mm: minutter

  — D: varighedspiktogram

  — EF: kombination af piktogrammer for begivenheder eller fejl

  — O: piktogram for funktionsmåde.

DIS_001 Takografen skal på skærmen vise data i følgende formater:

Data	Format
Standardskærmbillede	
Lokal tid	hh:mm
Funktionsmåde	O
Oplysninger vedrørende fører	1 Dhh**h**mm ▮▮hh**h**mm
Oplysninger vedrørende medchauffør	2 Dhh**h**mm
Omstændigheden »uden for område« åbnet	OUT
Visning af advarsel	
Overskridelse af sammenhængende køretid	1 ⊙ hh**h**mm ▮▮hh**h**mm
Hændelse eller fejl	EF
Andre skærmbilleder	
UTC-dato tid	UTC ◔ dd/mm/yyyy eller UTC ◔ dd.mm.yyyy hh:mm
Førers sammenhængende køretid og akkumulerede pausetid	1 ⊙ hh**h**mm ▮▮hh**h**mm
Medchaufførs sammenhængende køretid og akkumulerede pausetid	2 ⊙ hh**h**mm ▮▮hh**h**mm
Førers akkumulerede køretid for den foregående og den aktuelle uge	1 ⊙ ‖ hhh**h**mm
Medchaufførs akkumulerede køretid for den foregående og den aktuelle uge	2 ⊙ ‖ hhh**h**mm

▼B

Tillæg 6

STIK TIL KALIBRERING OG DATAOVERFØRSEL PÅ FRONTPANELET

INDHOLDSFORTEGNELSE

1. HARDWARE

1.1. Stik

1.2. Kontakternes tildeling

1.3. Blokdiagram

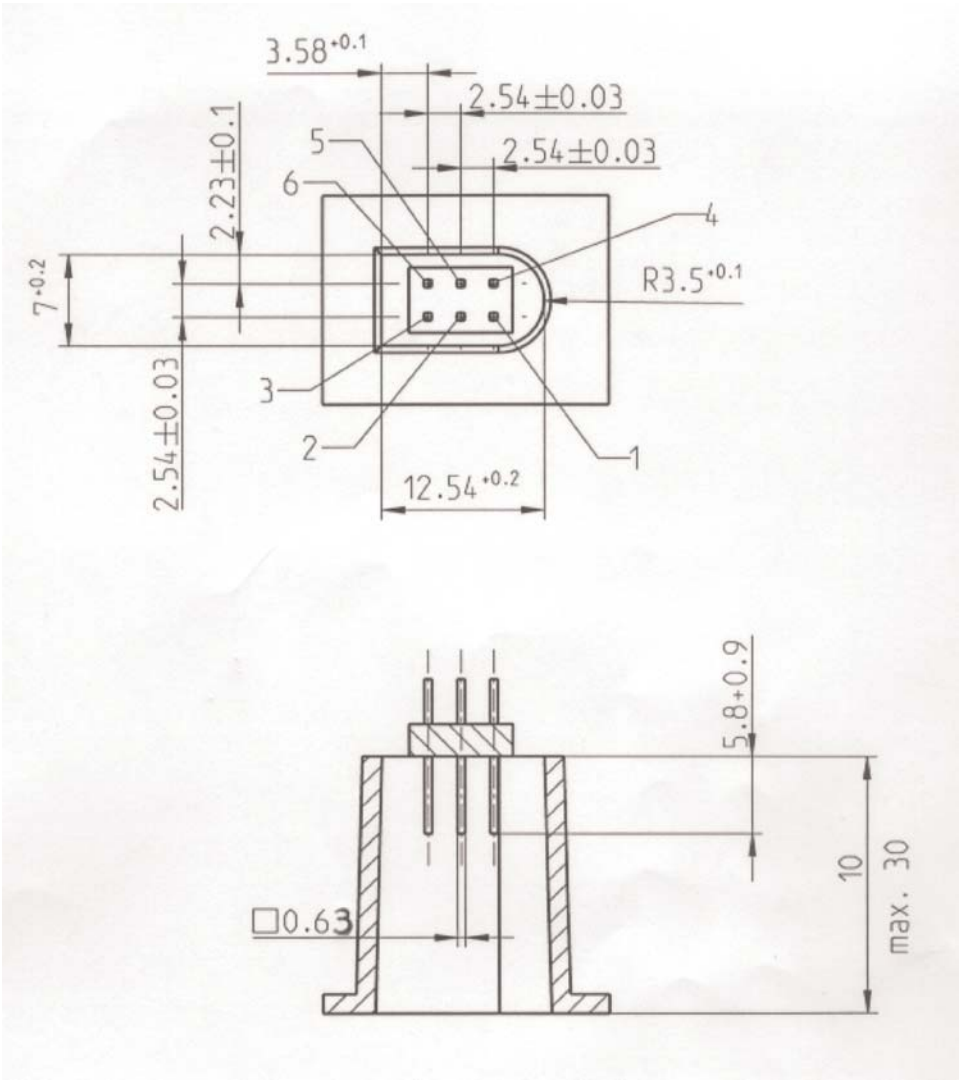
2. GRÆNSEFLADE FOR DATAOVERFØRSEL

3. GRÆNSEFLADE FOR KALIBRERING

1. HARDWARE

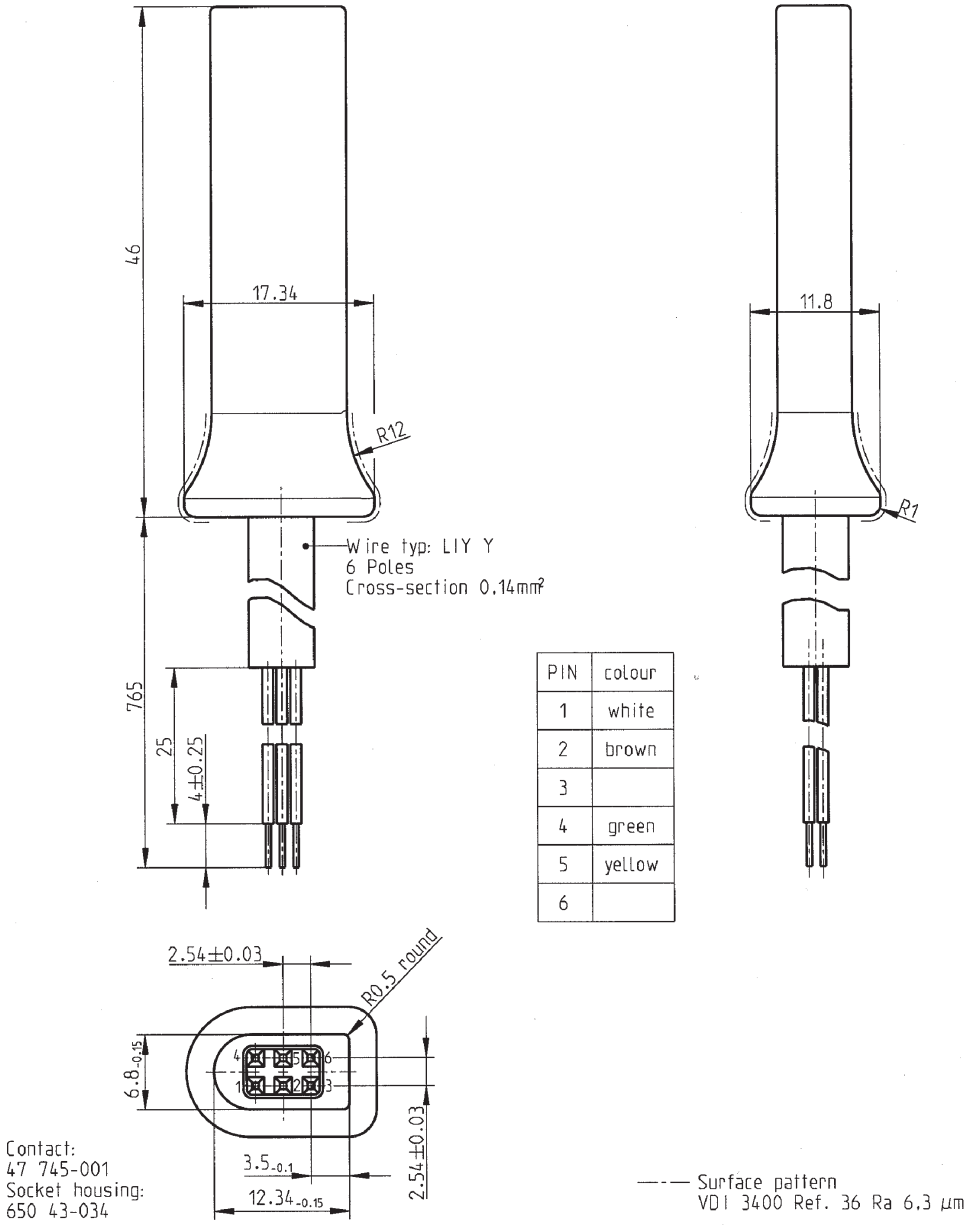
1.1. **Stik**

INT_001 Stikket til dataoverførsel/kalibrering skal være 6-benet, skal være tilgængeligt fra frontpanelet, uden at nogen del af takografen behøver adskilles, og skal være i overensstemmelse med følgende tegning (alle mål i mm):



▼B

Følgende diagram viser et typisk 6-benet stik:



PIN	colour
1	white
2	brown
3	
4	green
5	yellow
6	

1.2. **Kontakternes tildeling**

INT_002 Kontakterne skal være tildelt i overensstemmelse med følgende tabel:

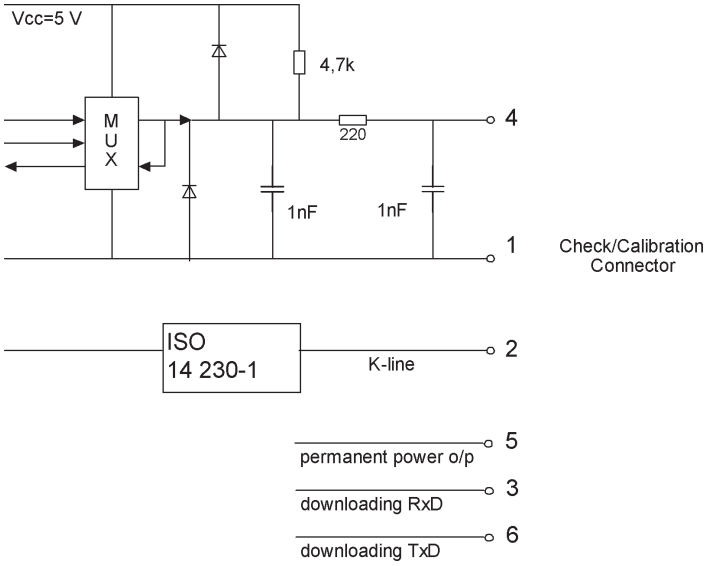
Klemme	Beskrivelse	Bemærkning
1	Batteri minus	Tilsluttet køretøjets negative batteripol
2	Datakommunikation	K-linje (ISO 14230-1)
3	RxD — dataoverførsel	Dataindgang til takograf
4	Indgangs-/udgangssignal	Kalibrering

▼B

Klemme	Beskrivelse	Bemærkning
5	Permanent effektudgang	Det foreskrevne spændingsområde er som køretøjets strømforsyning minus 3 V for at tage hensyn til spændingstabet over beskyttelseskredsen Udgangseffekt 40 mA
6	TxD — dataoverførsel	Dataoverførsel fra takograf

1.3. **Blokdiagram**

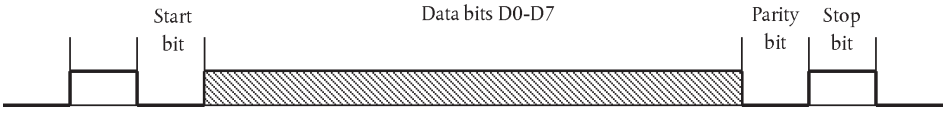
INT_003 Blokdiagrammet skal være i overensstemmelse med følgende:



2. GRÆNSEFLADE FOR DATAOVERFØRSEL

INT_004 Grænsefladen for dataoverførsel skal opfylde specifikationerne RS232.

INT_005 Grænsefladen for dataoverførsel skal have én startbit, 8 mindst betydende databit først, én lige paritetsbit og 1 stopbit.



Organisation af databytes

Startbit: én bit med logisk niveau 0

Databit: overføres med mindst betydende bit først

Paritetsbit: lige paritet

Stopbit: én bit med logisk niveau 1

Ved overførsel af numeriske data bestående af flere end én byte overføres den mest betydende byte først, og den mindst betydende byte sidst.

INT_006 Transmissionshastigheden skal kunne indstilles mellem 9 600 bps og 115 200 bps. Transmission skal kunne ske med den højst mulige transmissionshastighed, idet den indledende hastighed efter start af kommunikationen er stillet på 9 600 bps.

▼B

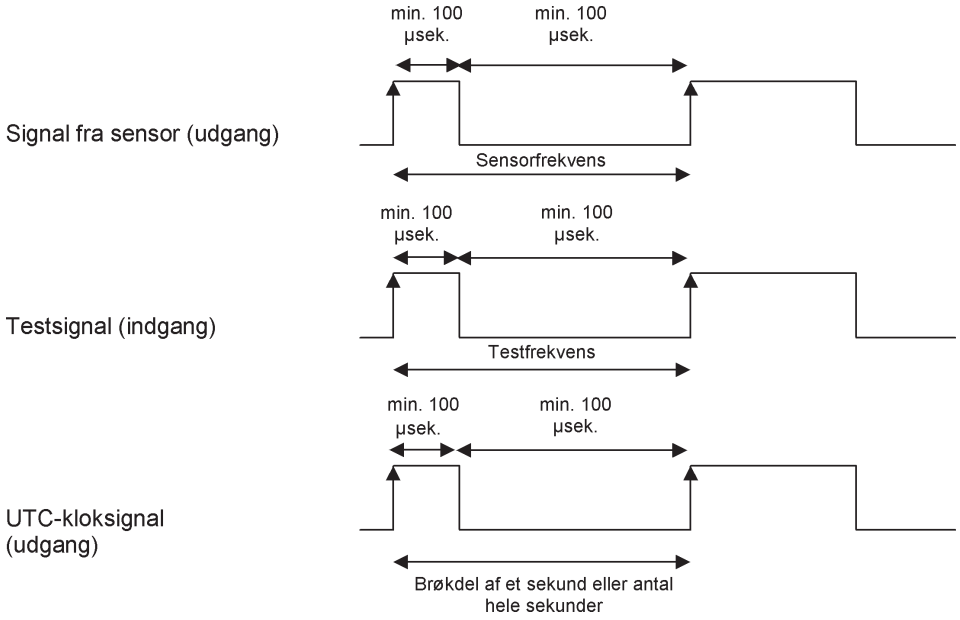
3. GRÆNSEFLADE FOR KALIBRERING

INT_007 Datakommunikationen skal opfylde ISO 14230-1 Road vehicles — Diagnostic systems — Keyword protocol 2000 — Part 1: Physical layer, First edition: 1999.

INT_008 Indgangs- og udgangssignalet skal opfylde følgende elektriske forskrift:

Parameter	Minimum	Typisk	Maksimum	Bemærkning
U_{lav} (ind)			1,0 V	I = 750 µA
$U_{høj}$ (ind)	4 V			I = 200 µA
Frekvens			4 kHz	
U_{lav} (ud)			1,0 V	I = 1 mA
$U_{høj}$ (ud)	4 V			I = 1 mA

INT_009 Indgangs- og udgangssignalet skal opfylde følgende tidsdiagrammer:



▼B

Tillæg 7

PROTOKOLLER FOR DATAOVERFØRSEL

INDHOLDSFORTEGNELSE

1. INDLEDNING

1.1. Anvendelsesområde

1.2. Akronymer og notation

2. OVERFØRSEL AF DATA FRA KØRETØJSENHEDEN

2.1. Fremgangsmåde ved dataoverførsel

2.2. Protokol for dataoverførsel

2.2.1 Meddelelsesstruktur

2.2.2 Meddelelsestyper

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 Meddelelsesstrøm

2.2.4 Synkronisering

▼B

2.2.5 Fejlhåndtering

2.2.5.1 Fasen Begynd kommunikation

2.2.5.2 Kommunikationsfasen

2.2.6 Svarmeddelelsens indhold

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. Lagring af fil på eksternt lagermedium

3. PROTOKOL FOR OVERFØRSEL AF TAKOGRAFKORT

3.1. Anvendelsesområde

3.2. Definitioner

3.3. Dataoverførsel af kort

3.3.1 Initialiseringssekvens

3.3.2 Sekvens for ikke-underskrevne datafiler

3.3.3 Sekvens for underskrevne datafiler

3.3.4 Sekvens for nulstilling af kalibreringstæller

3.4. Format for lagring af data

3.4.1 Indledning

3.4.2 Filformat

4. OVERFØRSEL AF TAKOGRAFKORT VIA KØRETØJS-ENHEDEN

1. INDLEDNING

Dette tillæg beskriver de procedurer, der skal følges ved forskellige typer dataoverførsel til et eksternt lagermedium (ESM), foruden de protokoller, der skal gennemføres for at sikre korrekt overførsel af data og fuld kompatibilitet af det overførte dataformat, således at enhver tilsynsførende har adgang til disse data og mulighed for at kontrollere deres ægthed og integritet, før de analyseres.

1.1. **Anvendelsesområde**

Der kan overføres data til et eksternt lagermedium:

— fra en køretøjsenhed med en intelligent dedikeret enhed (IDE) tilsluttet køretøjsenheden

— fra et takografkort med en IDE-enhed med kortlæser (IFD)

▼B

— fra et takografkort via en køretøjsenhed ved hjælp af en IDE-enhed tilsluttet køretøjsenheden.

For at man skal kunne fastslå ægthed og integritet af overførte data, som er gemt på et eksternt lagermedium, bliver der ved dataoverførsel vedhæftet en underskrift i overensstemmelse med tillæg 11 (fælles sikkerhedsmekanismer). Kildeenhedens (køretøjsenhed eller kort) identifikation og sikkerhedsattester (fra medlemsstaten og for udstyret) bliver ligeledes overført. Den, der kontrollerer data, skal uafhængigt være indehaver af en betroet europæisk offentlig nøgle.

DDP_001 Data overført i én overførselssession skal på det eksterne lagermedium gemmes i én fil.

1.2. **Akronymer og notation**

I dette tillæg anvendes følgende akronymer:

AID Applikationsidentifikator (Application Identifier)

ATR Svar på reset (Answer to Reset)

CS Kontrolsumbyte

DF Dedikeret fil

DS_ Diagnosesession

EF Elementærfil (Elementary File)

ESM Eksternt lagermedium

FID Filidentifikator (filnavn)

FMT Formatbyte (første byte i meddelelsens hoved)

ICC Chipkort (Integrated Circuit Card)

IDE Intelligent dedikeret udstyr: Det udstyr, som anvendes til at overføre data til det eksterne lagermedium (f.eks. pc)

IFD Kortlæser (interface device)

KWP Nøgleordsprotokol 2000

LEN Længdebyte (sidste byte i meddelelsens hoved)

PPS Protokolparametervalg (Protocol Parameter Selection)

PSO Udfør sikkerhedsoperation

SID Tjenesteidentifikator

SRC Kildebyte

TGT Adressebyte

TLV Etiketlængde (Tag length value)

TREP Parameter for svar på overførsel

TRTP Parameter for anmodning om overførsel

VU Køretøjsenhed

▼B

2. OVERFØRSEL AF DATA FRA KØRETØJSENHEDEN

2.1. **Fremgangsmåde ved dataoverførsel**

For at overføre data fra køretøjsenheden skal operatøren foretage følgende:

— indsætte sit takografkort i en kortplads i køretøjsenheden (*)

— tilslutte IDE-enheden til køretøjsenhedens datastik

— etablere forbindelse mellem IDE-enhed og køretøjsenhed

— på IDE-enheden vælge data, som skal overføres, og sende anmodningen til køretøjsenheden

— afslutte dataoverførselssessionen.

2.2. **Protokol for dataoverførsel**

Protokollen har master/slave-struktur, således at IDE-enheden fungerer som master og køretøjsenheden som slave.

Meddelelsesstruktur, -typer og -strøm er hovedsagelig baseret på Keyword protocol 2000 (KWP) (ISO 14230-2 Road vehicles — Diagnostic systems — Keyword protocol 2000 — Part 2: Data link layer).

Applikationslaget bygger hovedsagelig på det aktuelle udkast til ISO 14229-1 (Road vehicles — Diagnostic systems — Part 1: Diagnostic services, version 6 af 22. februar 2001).

2.2.1 *Meddelelsesstruktur*

DDP_002 Alle meddelelser, som udveksles mellem IDE-enhed og køretøjsenhed, er formateret med tredelt struktur:

— et hoved bestående af en formatbyte (FMT), en destinationsbyte (TGT), en kildebyte (SRC) og eventuelt en længdebyte (LEN)

— et datafelt bestående af en tjenesteidentifikatorbyte (SID) og et varierende antal databytes, som kan omfatte en ikke-obligatorisk diagnosesessionsbyte (DS) eller en frivillig overførselsparameterbyte (TRTP eller TREP)

— en kontrolsum bestående af en kontrolsumbyte (CS).

Hoved				Datafelt					Kontrolsum
FMT	TGT	SRC	LEN	SID	DATA	…	…	…	CS
4 bytes				Maks. 255 bytes					1 byte

TGT- og SRC-byten repræsenterer den fysiske adresse på modtageren og afsenderen af meddelelsen. De har værdierne F0 Hex for IDE-enheden og EE Hex for køretøjsenheden.

LEN-byten er længden af datafeltdelen.

Kontrolsumbyten er 8 bit-sumserie modulo 256 for alle meddelelsens bytes bortset fra selve kontrolsummen.

FMT-, SID-, DS-, TRTP- og TREP-bytes er defineret senere i dette dokument.

(*) Det indsatte kort vil udløse de nødvendige adgangsrettigheder til overførselsfunktionen og til data. Det skal imidlertid være muligt at overføre data fra et førerkort, der er indsat i en af køretøjsenhedens kortpladser, hvis der ikke er isat en anden korttype i den anden kortplads.

▼B

DDP_003 Hvis de data, som meddelelsen skal medføre, er længere end pladsen i datafeltdelen, bliver meddelelsen reelt sendt som flere delmeddelelser. Hver sådan delmeddelelse har et hoved, samme SID og TREP og en 2-byte-delmeddelelsestæller, som angiver delmeddelelsens nummer i den samlede meddelelse. For at der skal kunne foretages fejlkontrol og afbrydelse, kvitterer IDE-enheden for hver delmeddelelse. IDE-enheden kan acceptere delmeddelelsen, anmode om, at den genoverføres, anmode køretøjsenheden om at begynde igen eller afbryde dataoverførslen.

DDP_004 Hvis den sidste delmeddelelse indeholder nøjagtig 255 bytes i datafeltet, skal der vedhæftes en afsluttende delmeddelelse, hvor datafeltet er tomt (bortset fra SID, TREP og delmeddelelsestælleren), som angivelse af meddelelsens slutning.

Eksempel:

Hoved	SID	TREP	Meddelelse	CS
4 bytes	Længere end 255 bytes			

Vil blive overført som:

Hoved	SID	TREP	00	01	Delmeddelelse 1	CS
4 bytes	255 bytes					

Hoved	SID	TREP	00	02	Delmeddelelse 2	CS
4 bytes	255 bytes					

…

Hoved	SID	TREP	xx	yy	Delmeddelelse n	CS
4 bytes	Mindre end 255 bytes					

eller som:

Hoved	SID	TREP	00	01	Delmeddelelse 1	CS
4 bytes	255 bytes					

Hoved	SID	TREP	00	02	Delmeddelelse 2	CS
4 bytes	255 bytes					

…

Hoved	SID	TREP	xx	yy	Delmeddelelse n	CS
4 bytes	255 bytes					

Hoved	SID	TREP	xx	yy+1	CS
4 bytes	4 bytes				

▼B

2.2.2 *Meddelelsestyper*

Kommunikationsprotokollen for overførsel af data mellem køretøjsenheden og IDE-enheden kræver udveksling af 8 forskellige typer meddelelser.

Disse meddelelser er sammenfattet i følgende tabel.

Meddelelsesstruktur	Maks. 4 bytes Hoved				Maks. 255 bytes Data			1 byte Kontrolsum
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								
Oversigt	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		9A
Technical Data	80	EE	F0	02	36	05		9B
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

Meddelelsesstruktur	Maks. 4 bytes Hoved				Maks. 255 bytes Data			1 byte Kontro-lsum
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

Bemærkninger:

— Sid Req = Sid for den tilsvarende anmodning, Lid Req = Lid for den tilsvarende anmodning.

— TREP = TRTP for den tilsvarende anmodning.

— Mørke celler angiver, at intet overføres.

— Betegnelsen upload (set fra IDE-enheden) anvendes for kompatibilitet med nøgleordsprotokollen (ISO 14229). Betydningen er den samme som af dataoverførsel (set fra køretøjsenheden).

— Eventuelle 2-byte-delmeddelelsestællere er ikke vist i denne tabel.

— »Slot« er kortpladsnummeret — enten »1« (kort i førerens kortplads) eller »2« (kort i medchaufførens kortplads).

— Er kortpladsnummeret ikke angivet, skal køretøjsenheden vælge kortplads 1, hvis et kort er sat i denne plads, mens den kun skal vælge kortplads 2, hvis brugeren vælger dette.

2.2.2.1 Start Communication Request (SID 81)

DDP_005 Denne meddelelse afgives af IDE-enheden for at etablere en kommunikationsforbindelse med køretøjsenheden. Den indledende kommunikation udføres altid ved 9 600 baud (indtil transmissionshastigheden til sidst ændres ved hjælp af de pågældende link-kontroltjenester).

▼B

2.2.2.2 Positive Response Start Communication (SID C1)

DDP_006 Denne meddelelse afgives af IDE-enheden som positivt svar på anmodning om at begynde kommunikation. Den indeholder de to nøglebytes 'EA' '8F', som angiver, at enheden understøtter protokollen, og hovedet indeholder oplysninger om destination, kilde og længde.

2.2.2.3 Start Diagnostic Session Request (SID 10)

DDP_007 IDE-enheden sender denne meddelelse for at anmode om en ny diagnosesession med køretøjsenheden. Delfunktionen 'default session' (81 Hex) angiver, at der skal åbnes en standarddiagnosesession.

2.2.2.4 Positive Response Start Diagnostic (SID 50)

DDP_008 Denne meddelelse afgives af køretøjsenheden som positivt svar på anmodning om diagnosesession.

2.2.2.5 Link Control Service (SID 87)

DDP_052 Link Control Service anvendes af IDE-enheden til at indlede en ændring i transmissionshastigheden. Dette sker i to trin. I første trin foreslår IDE-enheden en ændring i transmissionshastigheden. Ved modtagelse af et positivt svar fra køretøjsenheden afgiver IDE-enheden en bekræftelse på den ændrede transmissionshastighed til køretøjsenheden (andet trin). IDE-enheden skifter derefter til den nye transmissionshastighed. Efter modtagelse af bekræftelsen skifter køretøjsenheden til den nye transmissionshastighed.

2.2.2.6 Link Control Positive Response (SID C7)

DDP_053 Link Control Positive response angives af køretøjsenheden som svar på en anmodning til linkkontroltjenesten (første trin). Bemærk, at der ikke svares på bekræftelsen af anmodningen (trin to).

2.2.2.7 Request Upload (SID 35)

DDP_009 Request Upload afgives af IDE-enheden for over for køretøjsenheden at anmode om en dataoverførsel. For at opfylde kravene i ISO 14229 indgår der data om adresse, størrelse og format af de ønskede data. Da disse ikke kendes af IDE-enheden før overførslen, sættes lageradressen til 0, formatet til ukrypteret og lagerstørrelsen til maksimum.

2.2.2.8 Positive Response Request Upload (SID 75)

DDP_010 Positive Response Request Upload sendes af køretøjsenheden for at fortælle IDE-enheden, at køretøjsenheden er klar til at overføre data. For at opfylde kravene i ISO14229 indeholder den positive svarmeddelelse data, som fortæller IDE-enheden, at yderligere meddelelser med positivt svar på dataoverførsel vil indeholde maksimalt 00FF hex byte.

▼B

2.2.2.9 Transfer Data Request (SID 36)

DDP_011 Transfer Data Request sendes af IDE-enheden for over for køretøjsenheden at specificere den type data, som skal overføres. Overførslens type angives af en parameter for anmodning om dataoverførsel (TRTP) på én byte.

Der er seks typer dataoverførsel:

— Oversigt (TRTP 01)

— Aktiviteter på en nærmere angivet dato (TRTP 02)

— Hændelser og fejl (TRTP 03)

— Detaljeret hastighed (TRTP 04)

— Tekniske data (TRTP 05)

— Overførsel af data fra kort (TRTP 06).

DDP_054 IDE-enheden skal obligatorisk anmode om oversigt over dataoverførsel (TRTP 01) under en dataoverførselssession, da det kun på denne måde kan sikres, at køretøjsenhedens certifikater registreres i den overførte fil (så der er mulighed for verificering af en digital underskrift).

I andet tilfælde (TRTP 02) er det i meddelelsen overfør data angivet, hvilken kalenderdag (`TimeReal`-format) der skal overføres.

2.2.2.10 Positive Response Transfer Data (SID 76)

DDP_012 Positive Response Transfer Data afgives af køretøjsenheden som svar på Transfer Data Request. Meddelelsen indeholder de anmodede data med en parameter for svar på overførsel (Transfer Response Parameter — TREP) svarende til anmodningens TRTP.

DDP055 I første tilfælde (TREP F01) vil køretøjsenheden sende data, som hjælper IDE-operatøren til at vælge de data, som han yderligere vil overføre. Denne meddelelse indeholder følgende oplysninger:

— sikkerhedscertifikater

— identifikation af køretøjer

— køretøjsenhedens aktuelle dato og klokkeslæt

— mindste og største dato, som kan overføres (data fra køretøjsenhed)

— angivelse af kort, som er isat i køretøjsenheden

— tidligere dataoverførsler til en virksomhed

— virksomhedslåse

— tidligere kontroller.

▼B

2.2.2.11 Request Transfer Exit (SID 37)

DDP_013 Request Transfer Exit afgives af IDE-enheden for at fortælle køretøjsenheden, at dataoverførselssessionen er slut.

2.2.2.12 Positive Response Request Transfer Exit (SID 77)

DDP_014 Positive Response Request Transfer Exit afgives af køretøjsenheden for at kvittere for Request Transfer Exit.

2.2.2.13 Stop Communication Request (SID 82)

DDP_015 Stop Communication Request afgives af IDE-enheden for at afbryde kommunikationsforbindelsen til køretøjsenheden.

2.2.2.14 Positive Response Stop Communication (SID C2)

DDP_016 Positive Response Stop Communication afgives af køretøjsenheden for at kvittere for Stop Communication Request.

2.2.2.15 Acknowledge Sub Message (SID 83)

DDP_017 Acknowledge Sub Message afgives af IDE-enheden for at bekræfte de enkelte dele af en meddelelse, der overføres som flere delmeddelelser. Datafeltet indeholder den SID, som er modtaget fra køretøjsenheden, og en 2-byte-kode som følger:

— MsgC + 1 kvitterer for korrekt modtagelse af delmeddelelse nummer MsgC.

Anmodning fra IDE-enheden til køretøjsenheden om at sende næste delmeddelelse.

— MsgC angiver, at der er en fejl ved modtagelse af delmeddelelse nummer MsgC.

Anmodning fra IDE-enheden til køretøjsenheden om at sende delmeddelelsen igen.

— FFFF anmoder om afslutning af meddelelsen.

Dette kan af IDE-enheden anvendes til at afslutte overførslen af meddelelsen fra køretøjsenheden uanset grund.

For den afsluttende delmeddelelse i en meddelelse (LEN byte < 255) kan der kvitteres med enhver af disse koder, eller kvittering kan undlades.

Svar fra køretøjsenheden består af flere delmeddelelser og kan være:

— Positive Response Transfer Data (SID 76)

▼B

2.2.2.16 Negative Response (SID 7F)

DDP_018 Som svar på ovennævnte anmodninger sender køretøjsenheden Negative Response, når køretøjsenheden ikke kan imødekomme anmodningen. Meddelelsens datafelter indeholder svarets SID (7F), anmodningens SID og en kode, som angiver begrundelsen for det negative svar. Følgende koder er til rådighed:

— 10 generel afvisning

Operationen kan ikke gennemføres af grunde, som ikke er omfattet af nedenstående.

— 11 tjeneste ikke understøttet

Anmodningens SID er ikke blevet forstået.

— 12 delfunktion understøttes ikke

Anmodningens DS_ eller TRTP forstås ikke, eller der er ikke flere delmeddelelser at overføre.

— 13 ukorrekt meddelelseslængde

Længden af den modtagne meddelelse er forkert.

— 22 ukorrekte betingelser eller fejl i anmodningssekvens

Den anmodede tjeneste er ikke aktiv eller sekvensen af anmodningsmeddelelsen ukorrekt.

— 31 Anmodning uden for gyldighedsområde

Posten med anmodningens parametre (datafelt) er ugyldig.

— 50 upload ikke accepteret

Anmodningen kan ikke efterkommes (køretøjsenhed ikke i korrekt driftstilstand, eller intern fejl i køretøjsenhed).

— 78 svar uafgjort

Den anmodede operation kan ikke gennemføres i tide, og køretøjsenheden er ikke klar til at modtage endnu en anmodning.

— FA-data foreligger ikke

Dataobjektet for en anmodning om dataoverførsel findes ikke i køretøjsenheden (f.eks. hvis der ikke er isat noget kort).

2.2.3 *Meddelelsesstrøm*

En typisk meddelelsesstrøm ved en normal dataoverførselsprocedure er følgende:

IDE		VU
Start Communication Request	⇨	
	⇦	Positive Response
Start Diagnostic Service Request	⇨	
	⇦	Positive Response
Request Upload	⇨	
	⇦	Positive Response

▼B

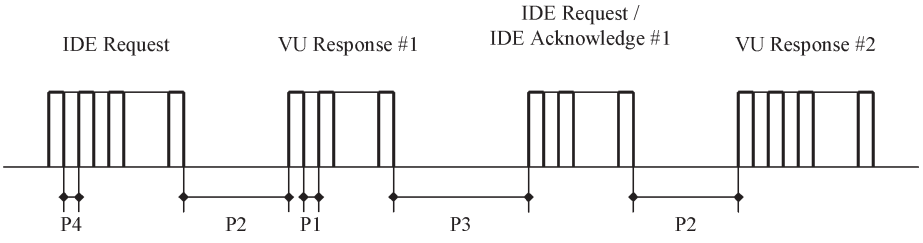
IDE		VU
Transfer Data Request Overview	⇨	
	⇦	Positive Response
Transfer Data Request #2	⇨	
	⇦	Positive Response #1
Acknowledge Sub Message #1	⇨	
	⇦	Positive Response #2
Acknowledge Sub Message #2	⇨	
	⇦	Positive Response #m
Acknowledge Sub Message #m	⇨	
	⇦	Positive Response (Data Field<255 Bytes)
Acknowledge Sub Message (optional)	⇨	
…		
Transfer Data Request #n	⇨	
	⇦	Positive Response
Request Transfer Exit	⇨	
	⇦	Positive Response
Stop Communication Request	⇨	
	⇦	Positive Response

2.2.4 *Synkronisering*

DDP_019 Under normal drift er tidsparametrene i følgende figur relevante:

Figur 1

Meddelelsesstrøm, synkronisering



Hvor:

P1 = Tidsrum, som adskiller bytes for svar fra køretøjsenhed.

P2 = Tid fra slutning af IDE-enhedens anmodning til start på køretøjsenhedens svar, eller fra slutning af IDE-enhedens kvittering til start på køretøjsenhedens næste svar.

P3 = Tid fra slutning af køretøjsenhedens svar til start på ny anmodning fra IDE-enheden, eller fra slutningen af køretøjsenhedens svar til start på IDE-enhedens kvittering, eller fra slutningen af IDE-enhedens anmodning til start på ny anmodning fra IDE-enheden, hvis køretøjsenheden ikke svarer.

P4 = Tidsrum, der adskiller bytes i anmodning fra IDE-enheden.

P5 = Forlænget P3 ved overførsel fra kort.

▼B

Tilladte værdier af tidsparametrene er angivet i følgende tabel (det udvidede KWP-tidsparametersæt, som anvendes ved fysisk adressering for at gøre kommunikationen hurtigere).

Synkroniseringsparameter	Nedre grænseværdi (ms)	Øvre grænseværdi (ms)
P1	0	20
P2	20	1 000 (*)
P3	10	5 000
P4	5	20
P5	10	20 minutter

(*) Hvis køretøjsenheden reagerer med et Negative Response, der indeholder en kode med betydningen »anmodning modtaget som foreskrevet, svar afventes«, gælder den samme øvre grænseværdi for denne værdi som for P3.

2.2.5 *Fejlhåndtering*

Indtræffer der en fejl under meddelelsesudvekslingen, ændres meddelelsesstrømmene alt efter, hvilket udstyr der har fundet fejlen, og den meddelelse, som har udløst fejlen.

I figur 2 og 3 vises fejlhåndteringsprocedurer for hhv. køretøjsenhed og IDE-enhed.

2.2.5.1 Fasen Begynd kommunikation

DDP_020 Hvis IDE-enheden finder en fejl i start kommunikationfasen, enten i synkroniseringen eller i bitstrømmen, venter den i et tidsrum af P3min, før den igen afgiver anmodningen.

DDP_021 Hvis køretøjsenheden finder en fejl i den afgivne sekvens fra IDE-enheden, skal den intet svar sende og vente på endnu en anmodning om start på kommunikation inden for et tidsrum af P3max.

2.2.5.2 Kommunikationsfasen

Der kan defineres to forskellige fejlhåndteringsområder:

1. **Køretøjsenheden konstaterer en fejl i dataoverførslen for IDE-enheden**

DDP_022 For hver modtaget meddelelse skal køretøjsenheden finde eventuelle synkroniseringsfejl, fejl ved byteformat (f.eks. fejl ved start- og stopbit) og rammefejl (forkert antal bytes modtaget, forkert kontrolsumbyte).

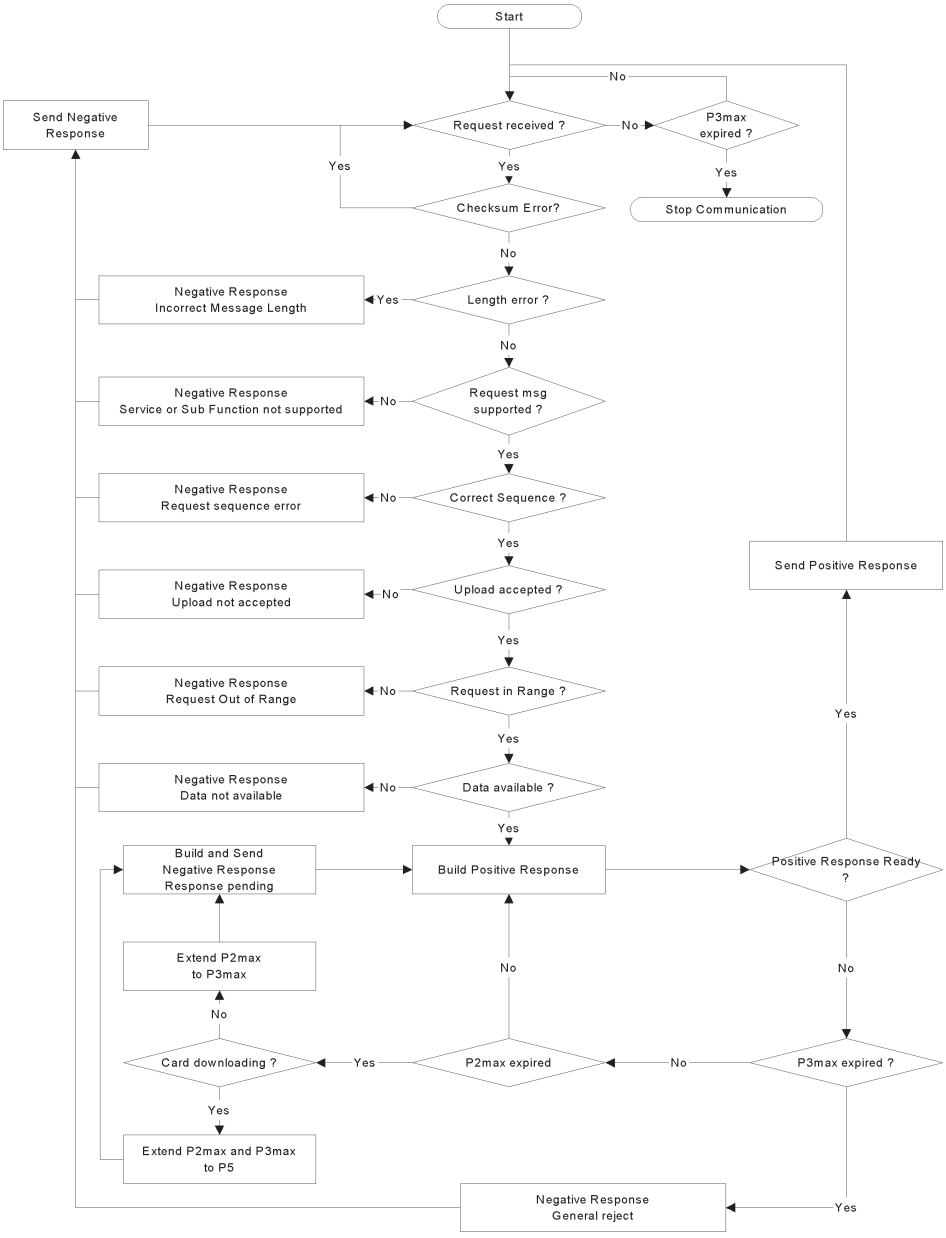
DDP_023 Hvis køretøjsenheden finder en af ovennævnte fejl, afgiver den intet svar og ignorerer den modtagne meddelelse.

DDP_024 Køretøjsenheden kan finde andre fejl i den modtagne meddelelses format eller indhold (f.eks. at meddelelsen ikke understøttes), uanset om meddelelsen opfylder forskrifterne for længde og kontrolsum. I så fald skal køretøjsenheden svare IDE-enheden med et Negative Response med angivelse af fejlens art.

▼B

Figur 2

Håndtering af fejl ved køretøjsenhed



2. **IDE-enheden registrerer en dataoverførselsfejl ved køretøjsenheden**

DDP_025 For hver modtaget meddelelse skal IDE-enheden finde eventuelle synkroniseringsfejl, fejl ved byteformat, (f.eks. fejl ved start- og stopbit) og rammefejl (forkert antal bytes modtaget, forkert kontrolsumbyte).

DDP_026 IDE-enheden skal finde sekvensfejl, f.eks. ukorrekt forøgelse af tællerne for delmeddelelser i successivt modtagne meddelelser.

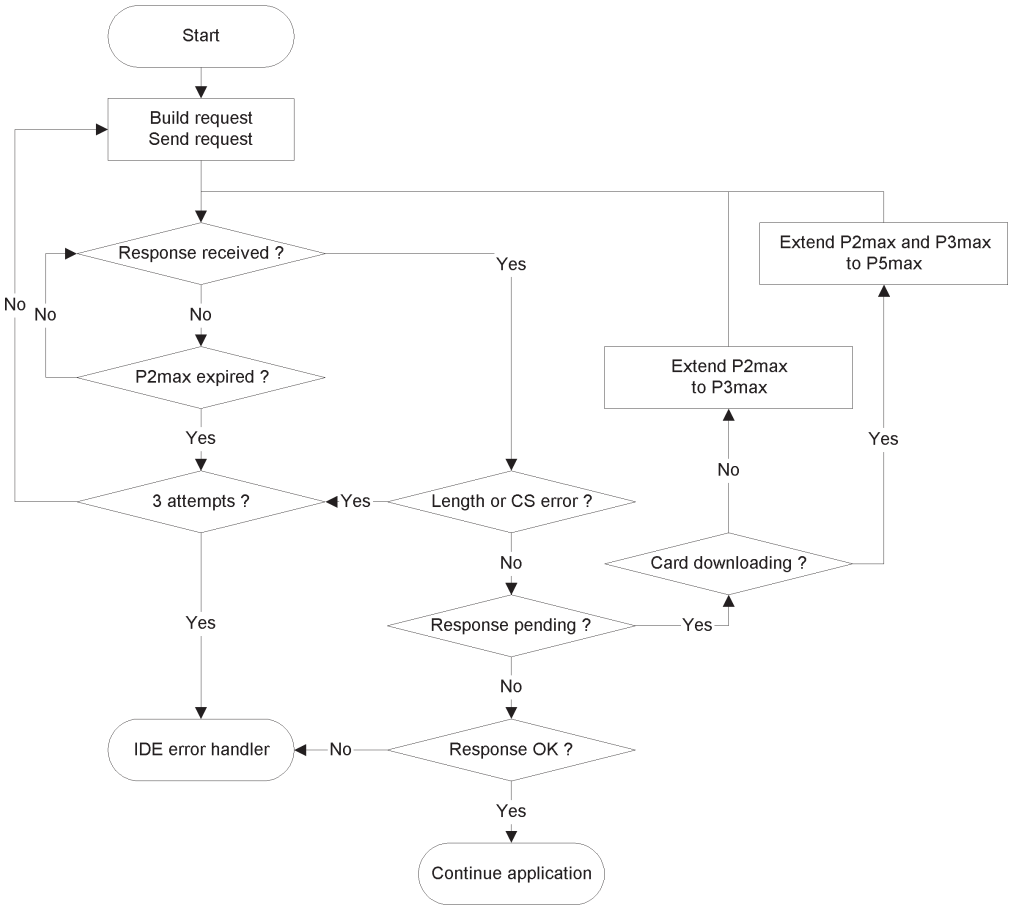
DDP_027 Hvis IDE-enheden konstaterer en fejl, eller der ikke kom svar fra køretøjsenheden inden for et tidsrum af P2max, vil anmodningen blive sendt igen, til den er sendt i alt højst tre gange. Hvad angår denne fejlfinding, vil en kvittering for delmeddelelse blive betragtet som en anmodning til køretøjsenheden.

▼B

DDP_028 IDE-enheden skal vente mindst P3min, før den begynder hver dataoverførsel. Venteperioden måles fra seneste beregnede forekomst af en stopbit, efter at fejlen blev konstateret.

Figur 3

Håndtering af fejl ved IDE-enhed



2.2.6 *Svarmeddelelsens indhold*

Dette afsnit angiver indholdet af datafelterne i de forskellige positive svarmeddelelser.

Dataelementerne er defineret i tillæg 1 (Dataordliste).

Bemærk: For dataoverførsel ved brug af udstyr af anden generation gælder det, at hvert dataelement på øverste niveau repræsenteres af et array med poster (record array), også selv om det kun indeholder én post. Et record array indledes med et hoved. Dette hoved angiver posttypen, poststørrelsen og antallet af poster. Record arrays navngives »…RecordArray« (med hoved) som i følgende tabeller.

2.2.6.1 Positive Response Transfer Data Overview

DDP_029 Datafeltet i meddelelsen »Positive Response Transfer Data Overview« skal bære følgende data i følgende rækkefølge under SID 76 Hex, TREP 01 Hex og med passende opdeling i delmeddelelser og behørig tælling:

▼B

Datastruktur, første generation

Dataelement	Bemærkning
MemberStateCertificate VUCertificate	Køretøjsenheders sikkerhedsattester
VehicleIdentificationNumber VehicleRegistrationIdentification	Identifikation af køretøj
CurrentDateTime	Køretøjsenhedens aktuelle dato og klokkeslæt
VuDownloadablePeriod	Periode, som kan overføres
CardSlotsStatus	Type af kort, som er isat køretøjsenheden
VuDownloadActivityData	Foregående overførsel fra køretøjsenheden
VuCompanyLocksData	Alle gemte virksomhedslåse. Hvis feltet står tomt, sendes kun noOfLocks = 0.
VuControlActivityData	Alle kontrolposter, der er gemt i køretøjsenheden. Hvis feltet står tomt, sendes kun noOfControls = 0.
Signature	RSA-underskrift for alle data (undtagen attester) fra VehicleIdentificationNumber ned til sidste byte i sidste VuControlActivityData.

Datastruktur, anden generation:

Dataelement	Bemærkning
MemberStateCertificateRecordArray	Attest fra medlemsstaten
VUCertificateRecordArray	Attest for køretøjsenheden
VehicleIdentificationNumberRecordArray	Identifikation af køretøj
VehicleRegistrationNumberRecordArray	Køretøjets registreringsnummer
CurrentDateTimeRecordArray	Køretøjsenhedens aktuelle dato og klokkeslæt
VuDownloadablePeriodRecordArray	Periode, som kan overføres
CardSlotsStatusRecordArray	Type af kort, som er isat køretøjsenheden
VuDownloadActivityDataRecordArray	Foregående overførsel fra køretøjsenheden
VuCompanyLocksRecordArray	Alle gemte virksomhedslåse. Hvis feltet står tomt, sendes et array-hoved med noOfRecords = 0.
VuControlActivityRecordArray	Alle kontrolposter, der er gemt i køretøjsenheden. Hvis feltet står tomt, sendes et array-hoved med noOfRecords = 0.
SignatureRecordArray	ECC-underskrift for alle foregående data undtagen attesterne.

2.2.6.2 Positive Response Transfer Data Activities

DDP_030 Datafeltet i meddelelsen »Positive Response Transfer Data Activities« skal indeholde følgende data i følgende rækkefølge under SID 76 Hex og TREP 02 Hex med passende opdeling i delmeddelelser og behørig tælling:

▼B

Datastruktur, første generation

Dataelement	Bemærkning
TimeReal	Dato for overført dag
OdometerValueMidnight	Kilometertæller ved afslutning af overført dag
VuCardIWData	Data om cyklusser med isætning/udtagning af kort. — Hvis dette felt ikke indeholder nogen tilgængelige data, sendes kun noOfVuCardIWRecords = 0. — Hvis en VuCardIWRecord-post overskrider 00:00 (kort isat den foregående dag) eller 24:00 (kort udtaget den følgende dag), skal den vises fuldt ud inden for de to pågældende dage.
VuActivityDailyData	Kortpladsers status kl. 00:00 og aktivitetsskift, der er registreret for den overførte dag.
VuPlaceDailyWorkPeriodData	Data vedrørende steder, der er registreret for den overførte dag. Hvis feltet står tomt, sendes kun noOfPlaceRecords = 0.
VuSpecificConditionData	Data vedrørende særlige omstændigheder, der er registreret for den overførte dag. Hvis feltet står tomt, sendes kun noOfSpecificConditionRecords = 0.
Signature	RSA-underskrift for alle data fra TimeReal ned til sidste byte i sidste post vedrørende særlige omstændigheder.

Datastruktur, anden generation:

Dataelement	Bemærkning
DateOfDayDownloadedRecordArray	Dato for overført dag
OdometerValueMidnightRecordArray	Kilometertæller ved afslutning af overført dag
VuCardIWRecordArray	Data om cyklusser med isætning/udtagning af kort. — Hvis dette felt ikke indeholder nogen tilgængelige data, sendes et array-hoved med noOfRecords = 0. — Hvis en VuCardIWRecord-post overskrider 00:00 (kort isat den foregående dag) eller 24:00 (kort udtaget den følgende dag), skal den vises fuldt ud inden for de to pågældende dage.
VuActivityDailyRecordArray	Kortpladsers status kl. 00:00 og aktivitetsskift, der er registreret for den overførte dag.
VuPlaceDailyWorkPeriodRecordArray	Data vedrørende steder, der er registreret for den overførte dag. Hvis feltet står tomt, sendes et array-hoved med noOfRecords = 0.
VuGNSSCDRecordArray	Køretøjets GNSS-positioner, hvis førerens kontinuerlige køretid når op på et multiplum af tre timer. Hvis feltet står tomt, sendes et array-hoved med noOfRecords = 0.
VuSpecificConditionRecordArray	Data vedrørende særlige omstændigheder, der er registreret for den overførte dag. Hvis feltet står tomt, sendes et array-hoved med noOfRecords = 0.
SignatureRecordArray	ECC-underskrift for alle foregående data.

▼B

2.2.6.3 Positive Response Transfer Data Events and Faults

DDP_031 Datafeltet i meddelelsen »Positive Response Transfer Data Events and Faults« skal indeholde følgende data i følgende rækkefølge under SID 76 Hex og TREP 03 Hex, med passende opdeling i delmeddelelser og behørig tælling:

Datastruktur, første generation

Dataelement	Bemærkning
VuFaultData	Alle fejl, som er gemt eller igangværende på køretøjsenheden. Hvis feltet står tomt, sendes kun noOfVuFaults = 0.
VuEventData	All hændelser (undtagen overskridelse af tilladt hastighed), som er gemt eller igangværende på køretøjsenheden. Hvis feltet står tomt, sendes kun noOfVuEvents = 0.
VuOverSpeedingControlData	Data vedrørende sidste kontrol med overskridelse af tilladt hastighed (standardværdi i mangel af data).
VuOverSpeedingEventData	Alle hændelser med overskridelse af tilladt hastighed, der er gemt i køretøjsenheden. Hvis feltet står tomt, sendes kun noOfVuOverSpeedingEvents = 0.
VuTimeAdjustmentData	Alle tidsjusteringshændelser, der er gemt i køretøjsenheden (uden for rammerne af en komplet kalibrering). Hvis feltet står tomt, sendes kun noOfVuTimeAdjRecords = 0.
Signature	RSA-underskrift for alle data fra noOfVuFaults ned til sidste byte i sidste tidsjusteringspost.

Datastruktur, anden generation:

Dataelement	Bemærkning
VuFaultRecordArray	Alle fejl, som er gemt eller igangværende på køretøjsenheden. Hvis feltet står tomt, sendes et array-hoved med noOfRecords = 0.
VuEventRecordArray	All hændelser (undtagen overskridelse af tilladt hastighed), som er gemt eller igangværende på køretøjsenheden. Hvis feltet står tomt, sendes et array-hoved med noOfRecords = 0.
VuOverSpeedingControlDataRecordArray	Data vedrørende sidste kontrol med overskridelse af tilladt hastighed (standardværdi i mangel af data).
VuOverSpeedingEventRecordArray	Alle hændelser med overskridelse af tilladt hastighed, der er gemt i køretøjsenheden. Hvis feltet står tomt, sendes et array-hoved med noOfRecords = 0.
VuTimeAdjustmentRecordArray	Alle tidsjusteringshændelser, der er gemt i køretøjsenheden (uden for rammerne af en komplet kalibrering). Hvis feltet står tomt, sendes et array-hoved med noOfRecords = 0.
VuTimeAdjustmentGNSSRecordArray	
SignatureRecordArray	ECC-underskrift for alle foregående data.

▼B

2.2.6.4 Positive Response Transfer Data Detailed Speed

DDP_032 Datafeltet i meddelelsen »Positive Response Transfer Data Detailed Speed« skal indeholde følgende data i følgende rækkefølge under SID 76 Hex og TREP 04 Hex, med passende opdeling i delmeddelelser og behørig tælling:

Datastruktur, første generation

Dataelement	Bemærkning
VuDetailedSpeedData	Alle detaljerede hastighedsdata, der er gemt i køretøjsenheden (én hastighedsblok pr. minut, i hvilket køretøjet har bevæget sig). 60 hastighedsværdier pr. minut (én pr. sekund).
Signature	RSA-underskrift for alle data fra noOfSpeedBlocks ned til sidste byte i sidste hastighedsblok.

Datastruktur, anden generation:

Dataelement	Bemærkning
VuDetailedSpeedBlockRecordArray	Alle detaljerede hastighedsdata, der er gemt i køretøjsenheden (én hastighedsblok pr. minut, i hvilket køretøjet har bevæget sig). 60 hastighedsværdier pr. minut (én pr. sekund).
SignatureRecordArray	ECC-underskrift for alle foregående data.

2.2.6.5 Positive Response Transfer Data Technical Data

DDP_033 Datafeltet i meddelelsen »Positive Response Transfer Data Technical Data« skal indeholde følgende data i følgende rækkefølge under SID 76 Hex og TREP 05 Hex med passende opdeling i delmeddelelser og behørig tælling:

Datastruktur, første generation

Dataelement	Bemærkning
VuIdentification	
SensorPaired	
VuCalibrationData	Alle kalibreringsposter, der er gemt i køretøjsenheden.
Signature	RSA-underskrift for alle data fra vuManufacturerName ned til sidste byte i sidste VuCalibrationRecord.

▼B

Datastruktur, anden generation:

Dataelement	Bemærkning
VuIdentificationRecordArray	
VuSensorPairedRecordArray	Alle bevægelsessensorparringer, der er gemt i køretøjsenheden
VuSensorExternalGNSSCoupledRecordArray	Alle koblinger med det eksterne GNSS-udstyr, der er gemt i køretøjsenheden
VuCalibrationRecordArray	Alle kalibreringsposter, der er gemt i køretøjsenheden.
VuCardRecordArray	Alle data om isætning af kort, der er gemt i køretøjsenheden.
VuITSConsentRecordArray	
VuPowerSupplyInterruptionRecordArray	
SignatureRecordArray	ECC-underskrift for alle foregående data.

2.3. **Lagring af fil på eksternt lagermedium**

DDP_034 Når en dataoverførselssession har omfattet overførsel af data fra en køretøjsenhed, skal IDE-enheden i én fysisk fil gemme alle data, som er modtaget fra køretøjsenheden under overførselssessionen i meddelelser om Positive Response Transfer Data. Data, som gemmes, omfatter ikke meddelelsers hoved, delmeddelelsestællere, tomme delmeddelelser og kontrolsummer, men indbefatter SID og TREP (af første delmeddelelse kun, hvis der er flere delmeddelelser).

3. PROTOKOL FOR OVERFØRSEL AF TAKOGRAFKORT

3.1. **Anvendelsesområde**

Dette afsnit beskriver direkte overførsel af data fra et takografkort til en IDE-enhed. IDE-elementet indgår ikke i det sikre miljø. Derfor udføres der ikke ægthedskontrol mellem kortet og IDE-enheden.

3.2. **Definitioner**

Overførselssession: Hver gang der finder en overførsel af chipkortdata sted. Sessionen omfatter hele forløbet fra en kortlæser nulstiller chipkortet til deaktivering af chipkortet (udtagning af kort eller næste isætning).

Underskrevet datafil: En fil fra chipkortet. Filen overføres til kortlæseren som almindelig tekst. På chipkortet bliver filen hashet og underskrevet, og underskriften overføres til kortlæseren.

3.3. **Dataoverførsel af kort**

DDP_035 Overførsel af et takografkort omfatter følgende trin:

— Overførsel af kortets fælles oplysninger i elementærfilerne ICCog IC. Disse oplysninger er ikke obligatoriske og sikres ikke med digital underskrift.

▼B

— Overførsel af elementærfilens Card_Certificate (eller CardSignCertificate) og CA_Certificate. Disse oplysninger sikres ikke med digital underskrift.

Det er obligatorisk at overføre disse filer ved hver overførselssession.

— Overførsel af applikationens øvrige elementærfiler (i de dedikerede filer Tachograph DF og Tachograph_G2 DF, hvis relevant) undtagen elementærfilen Card_Download. Disse oplysninger sikres med digital underskrift.

— Ved hver overførselssession er det obligatorisk som minimum at overføre elementærfilerne Application_Identification og ID.

— Ved overførsel af et førerkort er det desuden obligatorisk at overføre følgende elementærfiler:

- Events_Data
- Faults_Data
- Driver_Activity_Data
- Vehicles_Used
- Places
- GNSS_Places (hvis relevant)
- Control_Activity_Data
- Specific_Conditions.

— Ved dataoverførsel fra førerkort opdateres LastCardDownload-datoen i elementærfilen Card_Download.

— Ved dataoverførsel fra værkstedskort skal kalibreringstælleren i elementærfilen EF Card_Download nulstilles.

— Ved dataoverførsel fra et værkstedskort skal elementærfilen EF Sensor_Installation_Data ikke overføres.

3.3.1 *Initialiseringssekvens*

DDP_036 IDE-enheden skal indlede sekvensen som følger:

Kort	Retning	IDE-enhed/kortlæser	Betydning/bemærkninger
	⇦	Nulstilling af hardware	
ATR	⇨		

Om ønsket kan man ved hjælp af PPS skifte til en højere transmissionshastighed, når blot denne understøttes af chipkortet.

3.3.2 *Sekvens for ikke-underskrevne datafiler*

DDP_037 Følgende sekvens anvendes til overførsel af elementærfilerne ICC, IC, Card_Certificate (eller CardSignCertificate) og CA_Certificate:

Kort	Retning	IDE-enhed/kortlæser	Betydning/bemærkninger
	⇦	**Select File**	Vælg ved filnavn
OK	⇨		

▼B

Kort	Retning	IDE-enhed/kortlæser	Betydning/bemærkninger
	⇦	**Read Binary**	Indeholder filen flere data end svarende til bufferstørrelsen af kortlæser eller kort, må kommandoen gentages, indtil hele filen er læst.
Fildata OK	⇨	Gem data på eksternt lagermedium	i overensstemmelse med **3.4** Format for lagring af data

Note 1: Før valg af elementærfilen Card_Certificate (eller CardSignCertificate) skal takografapplikationen være valgt (vælges ved applikationsnavn).

Note 2: Valg og læsning af en fil kan også foretages i ét trin ved brug af en Read Binary-kommando med et kort id for elementærfilen.

3.3.3 *Sekvens for underskrevne datafiler*

DDP_038 Følgende sekvens anvendes til hver af de efterfølgende filer, som skal overføres med tilhørende underskrift:

Kort	Retn.	IDE-enhed/kortlæser	Betydning/bemærkninger
	⇦	**Select File**	
OK	⇨		
	⇦	**Perform Hash of File**	Beregner hash-værdien af den valgte fils dataindhold ved hjælp af den foreskrevne hash-algoritme i overensstemmelse med tillæg 11. Denne kommando er ikke en ISO-kommando
Beregn hashværdi af fil, og gem hashværdi midlertidigt			
OK	⇨		
	⇦	**Read Binary**	Indeholder filen flere data end svarende til bufferstørrelsen af kortlæser eller kort, må kommandoen gentages, indtil hele filen er læst.
Fildata OK	⇨	Gem de modtagne data på eksternt lagermedium	i overensstemmelse med **3.4** Format for lagring af data

▼B

Kort	Retn.	IDE-enhed/kortlæser	Betydning/bemærkninger
	⇦	**PSO: Compute Digital Signature**	
Udfør sikkerhedsoperationen »Compute Digital Signature« med anvendelse af den midlertidigt gemte hashværdi			
Signature OK	⇨	Tilføj data til de data, som i forvejen er gemt på det eksterne lagermedium	i overensstemmelse med **3.4** Format for lagring af data

Bemærk: Valg og læsning af en fil kan også foretages i ét trin ved brug af en Read Binary-kommando med et kort id for elementærfilen. I dette tilfælde kan elementærfilen vælges og læses, før kommandoen Perform Hash of File udføres.

3.3.4 *Sekvens for nulstilling af kalibreringstæller*

DDP_039 Til nulstilling af `NoOfCalibrationsSinceDownload` -tælleren i elementærfilen `Card_Download` på et værkstedskort anvendes følgende sekvens:

Kort	Retn.	IDE-enhed/kortlæser	Betydning/bemærkninger
	⇦	**Select File**, elementærfilen Card_Download	Vælg ved filnavn
OK	⇨		
	⇦	**Update Binary** NoOfCalibrationsSince-Download = '00 00'	
nulstiller antal overførsler fra kort			
OK	⇨		

Bemærk: Valg og opdatering af en fil kan også foretages i ét trin ved brug af en Update Binary-kommando med et kort id for elementærfilen.

3.4. **Format for lagring af data**

3.4.1 *Indledning*

DDP_040 De overførte data skal gemmes i overensstemmelse med følgende betingelser:

— Data skal opbevares transparent. Dette indebærer, at byte-rækkefølgen såvel som bitrækkefølgen i den overførte byte skal forblive uændret ved overførslen.

— Alle filer, der overføres fra kortet i løbet af en overførselssession, gemmes i én fil på det eksterne lagermedium.

▼B

3.4.2 *Filformat*

DDP_041 Filformatet er en sammenkædning af flere TLV-objekter.

DDP_042 Etiketten for en elementærfil skal være filidentifikatoren med tilføjelsen »00«.

DDP_043 Etiketten for en elementærfils underskrift skal være filidentifikatoren plus tilføjelsen »01«.

DDP_044 Længden er en to byte-værdi. Værdien fastlægger antal bytes i feltet Værdi. Værdien 'FF FF' i længdefeltet er forbeholdt fremtidig brug.

DDP_045 Når en fil ikke overføres, må intet vedrørende filen gemmes (ingen etiket og ingen nullængde).

DDP_046 En underskrift skal gemmes som næste TLV-objekt direkte efter det TLV-objekt, som indeholder filens data.

Definition	Betydning	Længde
FID (2 bytes) || »00«	Etiket for elementærfil (FID)	3 bytes
FID (2 bytes) || »01«	Etiket for underskrift af elementærfil (FID)	3 bytes
xx xx	Længde af feltet Værdi	2 bytes

Eksempel på data i en fil overført til eksternt lagermedium:

Mærkat	Længde	Værdi
00 02 00	00 11	Data i elementærfilen ICC
C1 00 00	00 C2	Data i elementærfilens Card_Certificate
		…
05 05 00	0A 2E	Data i elementærfilen Vehicles_Used
05 05 01	00 80	Underskrift af elementærfilen Vehicles_Used

4. OVERFØRSEL AF TAKOGRAFKORT VIA KØRETØJSENHEDEN

DDP_047 Køretøjsenheden skal gøre det muligt at overføre indholdet af et førerkort, som indsættes i en tilsluttet IDE-enhed.

DDP_048 IDE-enheden sender meddelelsen Transfer Data Request Card Download til køretøjsenheden for at indlede denne arbejdstilstand (se 2.2.2.9).

DDP_049 Køretøjsenheden skal derefter overføre hele kortet fil for fil i overensstemmelse med protokollen for overførsel af kort som fastlagt i punkt 3 og skal fremsende alle data, som er modtaget fra kortet, til det eksterne lagermedium i det korrekte TLV-filformat (se 3.4.2) og indkapslet i en »Positive Response Transfer Data«-meddelelse.

▼B

DDP_050 IDE-enheden skal hente data fra meddelelsen »Positive Response Transfer Data« (efter fjernelse af alle hoveder, SID, TREP, delmeddelelsestællere og kontrolsummer) og gemme dem i én fysisk fil som beskrevet i punkt 2.3.

DDP_051 Køretøjsenheden skal derefter i givet fald ajourføre førerkortets `Control_Activity_Data`-fil eller `Card_Download`-fil.

▼B

Tillæg 8

KALIBRERINGSPROTOKOL

INDHOLDSFORTEGNELSE

1. INDLEDNING

2. TERMER, DEFINITIONER OG HENVISNINGER

3. OVERSIGT OVER SERVICER

3.1. Tilgængelige servicer

3.2. Svarkoder

4. KOMMUNIKATIONSSERVICER

4.1. Servicen StartCommunication

4.2. StopCommunication-service

4.2.1 Beskrivelse af meddelelser

4.2.2 Meddelelsesformat

4.2.3 Parameterdefinition

4.3. TesterPresent-service

4.3.1 Beskrivelse af meddelelser

4.3.2 Meddelelsesformat

5. ADMINISTRATIONSSERVICER

5.1. StartDiagnosticSession-service

5.1.1 Beskrivelse af meddelelser

5.1.2 Meddelelsesformat

5.1.3 Parameterdefinition

5.2. SecurityAccess-service

5.2.1 Beskrivelse af meddelelser

5.2.2 Meddelelsesformat — SecurityAccess — requestSeed

5.2.3 Meddelelsesformat — SecurityAccess — sendKey

6. DATAOVERFØRSELSSERVICER

6.1. ReadDataByIdentifier-service

6.1.1 Beskrivelse af meddelelser

6.1.2 Meddelelsesformat

6.1.3 Parameterdefinition

6.2. WriteDataByIdentifier-service

6.2.1 Beskrivelse af meddelelser

6.2.2 Meddelelsesformat

6.2.3 Parameterdefinition

▼B

7. KONTROL AF TESTIMPULSER — FUNKTIONSENHED FOR IND-/UDDATASTYRING

7.1. InputOutputControlByIdentifier-service

7.1.1 Beskrivelse af meddelelser

7.1.2 Meddelelsesformat

7.1.3 Parameterdefinition

8. FORMATER TIL DATARECORDS

8.1. Værdiområder for overførte parametre

8.2. Formater til dataRecords

1. INDLEDNING

I dette tillæg beskrives, hvordan der udveksles data mellem en køretøjsenhed og en tester via K-linjen, som er en del af den i tillæg 6 beskrevne kalibreringsgrænseflade. Det beskriver desuden styringen af ind-/uddatalinjen på kalibreringsstikket.

Etablering af K-linje-kommunikationer er beskrevet i punkt 4 »Kommunikationsservicer«.

I dette tillæg anvendes begrebet »diagnosesessioner« til fastlæggelse af omfanget af styring over K-linjen under forskellige betingelser. Den forudindstillede tilstand er »standardsessionen«, hvor alle data kan aflæses fra køretøjsenheden, men ingen data kan skrives til den.

Valg af diagnosesession er beskrevet i punkt 5 »Administrationsservicer«.

Dette tillæg skal betragtes som relevant for begge generationer af køretøjsenheder og værkstedskort, som overholder de interoperabilitetskrav, der er fastlagt i denne forordning.

CPR_001 I »ECUProgrammingSession« kan der indlæses data til køretøjsenheden. Ved indlæsning af kalibreringsdata skal køretøjsenheden desuden være i funktionstilstand CALIBRATION.

Dataoverførsel via K-linje er beskrevet i afsnit 6 »Dataoverførselsservicer«. Formatet af de overførte data er beskrevet i afsnit 8 »Formater til dataRecords«.

CPR_002 I »ECUAdjustmentSession« kan kalibrerings-I/O-signallinjens I/O-funktionstilstand vælges via K-linjegrænsefladen. Kontrol af kalibrerings-I/O-signallinjen er beskrevet i afsnit 7 »Kontrol af testimpulser — funktionsenhed for ind-/uddatastyring«.

CPR_003 I hele dette dokument betegnes testerens adresse som 'tt'. Skønt visse adresser for testere kan være foretrukne, skal køretøjsenheden svare korrekt på enhver testeradresse. Køretøjsenhedens fysiske adresse er 0xEE.

▼B

2. TERMER, DEFINITIONER OG HENVISNINGER

Protokoller, meddelelser og fejlkoder bygger hovedsagelig på udkastet til ISO 14229-1 (Road vehicles — Diagnostic systems — Part 1: Diagnostic services, version 6 af 22. februar 2001).

Der anvendes bytekodning og hexadecimale værdier til serviceidentifikatorer, serviceanmodninger og -svar samt standardparametre.

Begrebet »tester« anvendes for det udstyr, som benyttes til at indlæse programmerings- og kalibreringsdata i køretøjsenheden.

Begreberne »klient« og »server« henviser henholdsvis til testeren og køretøjsenheden.

Begrebet ECU står for »Electronic control unit« og henviser til køretøjsenheden.

Henvisninger:

ISO 14230-2: Road Vehicles — Diagnostic Systems — Keyword Protocol 2000 — Part 2: Data Link Layer.

First edition: 1999.

Vehicles — Diagnostic.

3. OVERSIGT OVER SERVICER

3.1. **Tilgængelige servicer**

I nedenstående tabel gives en oversigt over de servicer, som vil være til rådighed i takografen og er fastlagt i dette dokument.

CPR_004 Tabellerne angiver servicer, som er til rådighed i en påbegyndt diagnosesession.

— **Søjle 1** angiver de servicer, som er til rådighed.

— **Søjle 2** henviser til nummeret på det punkt i dette tillæg, hvor denne service er nærmere defineret.

— **Søjle 3** tildeler værdier til serviceidentifikatorer for anmodningsmeddelelser.

— **Søjle 4** angiver de servicer i en »StandardDiagnosticSession« (SS), som skal være implementeret i hver køretøjsenhed.

— **Søjle 5** angiver de servicer i en »ECUAdjustmentSession« (ECUAS), som skal være implementeret, så der er mulighed for styring af I/O-signallinjen i kalibreringsstikket på køretøjsenhedens frontpanel.

— **Søjle 6** angiver de servicer i en »ECUProgrammingSession« (ECUPS), som skal være implementeret, så der kan programmeres parametre i køretøjsenheden.

▼B

Tabel 1

Oversigtstabel over serviceidentifikatorer

			Diagnosesession		
Navn på diagnoseservice	Afsnit nr.	Værdi af Sid-anmodning	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		■	

■ Dette symbol angiver, at servicen er obligatorisk i denne diagnosesession.
Hvis der ikke er noget symbol, er servicen ikke er tilladt i denne diagnosesession.

3.2. **Svarkoder**

Svarkoder er defineret for hver service.

4. KOMMUNIKATIONSSERVICER

Visse servicer er nødvendige til at etablere og opretholde kommunikation. De figurerer ikke i applikationslaget. I følgende tabel beskrives de servicer, som er til rådighed:

Tabel 2

Kommunikationsservicer

Servicens navn	Beskrivelse
StartCommunication	Klienten anmoder om påbegyndelse af en kommunikationssession med en server
StopCommunication	Klienten anmoder om at standse den aktuelle kommunikationssession
TesterPresent	Klienten angiver over for serveren, at den stadig er til stede

CPR_005 Servicen StartCommunication anvendes til at begynde en kommunikation. For enhver service gælder, at kommunikationen skal være initialiseret, og kommunikationsparametrene skal være passende til den pågældende funktionstilstand.

4.1. **Servicen StartCommunication**

CPR_006 Ved modtagelse af en StartCommunication-indikation skal køretøjsenheden kontrollere, om den ønskede dataforbindelse kan initialiseres under de aktuelle betingelser. De gældende betingelser for initialisering af en dataforbindelse er beskrevet i dokument ISO 14230-2.

▼B

CPR_007 Derefter skal køretøjsenheden udføre alle de operationer, som er nødvendige for at initialisere dataforbindelsen og sende et StartCommunication-svar, hvor parametre for positivt svar er valgt.

CPR_008 Hvis en køretøjsenhed, som i forvejen er initialiseret (og har påbegyndt en diagnosesession, uanset hvilken), modtager en ny StartCommunication-anmodning (f.eks. pga. fejlafhjælpning i testeren), skal anmodningen accepteres, og køretøjsenheden skal reinitialiseres.

CPR_009 Hvis dataforbindelsen af en eller grund ikke kan initialiseres, skal køretøjsenheden fortsætte med at fungere, som den gjorde umiddelbart før forsøget på at initialisere dataforbindelsen.

CPR_010 Meddelelsen med anmodningen StartCommunication skal være fysisk adresseret.

CPR_011 Initialisering af køretøjsenheden til servicer sker ved hurtig initialisering

— forud for enhver aktivitet er en periode, hvor bussen er ledig

— testeren sender derefter et initialiseringsmønster

— alle oplysninger, som er nødvendige til oprettelse af dataforbindelsen, er indeholdt i svaret fra køretøjsenheden.

CPR_012 Når initialisering har fundet sted,

— er alle kommunikationsparametre sat til de i Tabel 4 fastlagte standardværdier i henhold til nøglebytes.

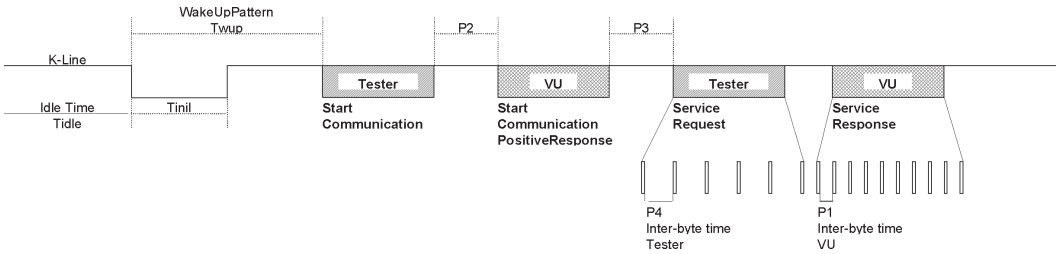
— afventer køretøjsenheden første anmodning fra testeren.

— er køretøjsenheden i sin standardfunktionstilstand for diagnose, dvs. StandardDiagnosticSession.

— er I/O-signallinjen for kalibrering i standardtilstand, dvs. deaktiveret.

CPR_014 Datahastigheden på K-linjen skal være 10 400 baud.

CPR_016 Hurtig initialisering igangsættes ved, at testeren overfører et opvågningsmønster (Wup) på K-linjen. Efter den ledige periode på K-linjen begynder mønsteret med et kortvarigt Tinil. Testeren overfører første bit af StartCommunication-servicen efter en periode med Twup, som efterfølger den første slutkant.



▼B

CPR_017 Synkroniseringsværdierne for hurtig initialisering og for meddelelser i almindelighed er givet i nedenstående tabel. Der er forskellige muligheder for den ledige tid:

— Første overførsel, efter at der er tændt, Tidle = 300 ms.

— Efter afslutning af en StopCommunication Service, Tidle = P3 min.

— Efter afbrydelse af kommunikation ved tidsudkobling P3 maks., Tidle = 0.

Tabel 3

Synkroniseringsværdier for hurtig initialisering

Parameter		Min. værdi	Maks. værdi
Tinil	25 ± 1 ms	24 ms	26 ms
Twup	50 ± 1 ms	49 ms	51 ms

Tabel 4

Synkroniseringsværdier for kommunikation

Tidspunkt Parameter	Parameterbeskrivelse	Nedre grænse (ms)	Øvre grænse (ms)
		Min.	maks.
P1	Tid mellem bytes for svar fra køretøjsenhed	0	20
P2	Tid mellem anmodning fra tester og svar fra køretøjsenhed, eller mellem to svar fra køretøjsenhed	25	250
P3	Tid mellem slutning af svar fra køretøjsenhed og begyndelse på ny anmodning fra tester	55	5 000
P4	Tid mellem bytes for anmodning fra tester	5	20

CPR_018 Meddelelsesformatet for hurtig initialisering er givet i nedenstående tabeller.

Tabel 5

StartCommunication-anmodning

Byte #	Parameternavn	Hex-værdi	Huskeværdi
#1	Formatbyte — fysisk adressering	81	FMT
#2	Adressebyte på destination	EE	TGT
#3	Adressebyte på kilde	tt	SRC

▼B

Byte #	Parameternavn	Hex-værdi	Huskeværdi
#4	**Service-ID på StartCommunication-anmodning**	**81**	**SCR**
#5	Kontrolsum	00-FF	CS

Tabel 6

Positivt svar på StartCommunication

Byte #	Parameternavn	Hex-værdi	Huskeværdi
#1	Formatbyte — fysisk adressering	80	FMT
#2	Adressebyte på destination	tt	TGT
#3	Adressebyte på kilde	EE	SRC
#4	Ekstra længdebyte	03	LEN
#5	**Service-ID for positivt svar på StartCommunication**	**C1**	**SCRPR**
#6	Nøglebyte 1	EA	KB1
#7	Nøglebyte 2	8F	KB2
#8	Kontrolsum	00-FF	CS

CPR_019 Der findes intet negativt svar på en StartCommunication-anmodning; er der ingen positiv svarmeddelelse at overføre, bliver køretøjsenheden ikke initialiseret, der overføres intet, og enheden fortsætter i normal funktionstilstand.

4.2. **StopCommunication-service**

4.2.1 *Beskrivelse af meddelelser*

Denne service er placeret i kommunikationslaget og anvendes til at afslutte en kommunikationssession.

CPR_020 Ved modtagelse af en StopCommunication-indikation skal køretøjsenheden kontrollere, om kommunikationen kan afsluttes under de aktuelle betingelser. I bekræftende fald skal køretøjsenheden udføre alle de nødvendige operationer til at afslutte kommunikationen.

CPR_021 Hvis det kan lade sig gøre at afslutte kommunikationen, skal køretøjsenheden afgive et StopCommunication-svar med parametre svarende til positivt svar, før kommunikationen afsluttes.

CPR_022 Hvis kommunikationen af en eller anden grund ikke kan afsluttes, skal køretøjsenheden afgive et StopCommunication-svar med parameteren negativt svar.

CPR_023 Hvis køretøjsenheden registrerer tidsudkobling af P3max, skal kommunikationen afsluttes, uden at der afgives et svar.

▼B

4.2.2 *Meddelelsesformat*

CPR_024 Meddelelsesformater for StopCommunication er givet i følgende tabeller:

Tabel 7

StopCommunication-anmodning

Byte #	Parameternavn	Hex-værdi	Huskeværdi
#1	Formatbyte — fysisk adressering	80	FMT
#2	Adressebyte på destination	EE	TGT
#3	Adressebyte på kilde	tt	SRC
#4	Ekstra længdebyte	01	LEN
#5	**Service-ID på StopCommunication-anmodning**	**82**	**SPR**
#6	Kontrolsum	00-FF	CS

Tabel 8

Positivt svar på StopCommunication

Byte #	Parameternavn	Hex-værdi	Huskeværdi
#1	Formatbyte — fysisk adressering	80	FMT
#2	Adressebyte på destination	tt	TGT
#3	Adressebyte på kilde	EE	SRC
#4	Ekstra længdebyte	01	LEN
#5	**Service-ID for positivt svar på StopCommunication**	**C2**	**SPRPR**
#6	Kontrolsum	00-FF	CS

Tabel 9

Negativt svar på StopCommunication

Byte #	Parameternavn	Hex-værdi	Huskeværdi
#1	Formatbyte — fysisk adressering	80	FMT
#2	Adressebyte på destination	tt	TGT
#3	Adressebyte på kilde	EE	SRC
#4	Ekstra længdebyte	03	LEN

▼B

Byte #	Parameternavn	Hex-værdi	Huskeværdi
#5	**Service-ID på negativt svar**	**7F**	**NR**
#6	Service-ID på StopCommunication	82	SPR
#7	responseCode = generalReject	10	RC_GR
#8	Kontrolsum	00-FF	CS

4.2.3 *Parameterdefinition*

Denne service kræver ingen parameterdefinition.

4.3. **TesterPresent-service**

4.3.1 *Beskrivelse af meddelelser*

Servicen TesterPresent anvendes af testeren til at angive, at serveren stadig er til stede for at undgå, at serveren automatisk returnerer til normal drift og eventuelt standser kommunikationen. Denne service, der udføres med regelmæssige mellemrum, holder diagnosesession/kommunikation aktive ved at tilbagestille P3-timeren, hver gang der modtages en anmodning om denne service.

4.3.2 *Meddelelsesformat*

CPR_079 Meddelelsesformater for TesterPresent-instruktioner er angivet i følgende tabeller.

Tabel 10

TesterPresent-anmodning

Byte #	Parameternavn	Hex-værdi	Huskeværdi
#1	Formatbyte — fysisk adressering	80	FMT
#2	Adressebyte på destination	EE	TGT
#3	Adressebyte på kilde	tt	SRC
#4	Ekstra længdebyte	02	LEN
#5	**Identifikation af servicen TesterPresent-forespørgsel**	**3E**	**TP**
#6	Delfunktion = [ja responseRequired = nej]	01 02	RESPREQ_Y RESPREQ_NO
#7	Kontrolsum	00-FF	CS

CPR_080 Hvis parameteren responseRequired sættes til »ja«, skal serveren svare med følgende positive svarmeddelelse. Hvis den sættes til »nej«, kommer der intet svar fra serveren.

▼B

Tabel 11

Positivt svar på TesterPresent

Byte #	Parameternavn	Hex-værdi	Huskeværdi
#1	Formatbyte — fysisk adressering	80	FMT
#2	Adressebyte på destination	tt	TGT
#3	Adressebyte på kilde	EE	SRC
#4	Ekstra længdebyte	01	LEN
#5	**Identifikation af servicen TesterPresent-forespørgsel**	**7E**	**TPPR**
#6	Kontrolsum	00-FF	CS

CPR_081 Servicen skal understøtte følgende negative svarkoder:

Tabel 12

Negativt svar på TesterPresent

Byte #	Parameternavn	Hex-værdi	Huskeværdi
#1	Formatbyte — fysisk adressering	80	FMT
#2	Adressebyte på destination	tt	TGT
#3	Adressebyte på kilde	EE	SRC
#4	Ekstra længdebyte	03	LEN
#5	**Service-ID på negativt svar**	**7F**	**NR**
#6	Identifikation af servicen TesterPresent-forespørgsel	3E	TP
#7	responseCode = [SubFunctionNotSupported-InvalidFormat	12	RC_SFNS_IF
	incorrectMessageLength]	13	RC_IML
#8	Kontrolsum	00-FF	CS

▼B

5. ADMINISTRATIONSSERVICER

I følgende tabel beskrives de servicer, som er til rådighed:

Tabel 13

Administrationsservicer

Servicens navn	Beskrivelse
StartDiagnosticSession	Klienten anmoder om at påbegynde en diagnosesession med en VU.
SecurityAccess	Klienten anmoder om adgang til funktioner, som er forbeholdt autoriserede brugere.

5.1. **StartDiagnosticSession-service**

5.1.1 *Beskrivelse af meddelelser*

CPR_025 Servicen StartDiagnosticSession anvendes til at tillade forskellige diagnosesessioner i serveren. En diagnosesession tillader et nærmere bestemt sæt servicer i henhold til Tabel 17. En session kan for køretøjsfabrikanten åbne særlige servicer, som ikke indgår i dette dokument. Implementeringsreglerne skal være i overensstemmelse med følgende krav:

— Der skal altid være netop én aktiv diagnosesession i køretøjsenheden.

— Køretøjsenheden skal altid åbne StandardDiagnosticSession, når den startes op. Hvis der ikke påbegyndes nogen anden diagnosesession, skal StandardDiagnosticSession køre, så længe køretøjsenheden er tændt.

— Har testeren anmodet om en diagnosesession, som i forvejen kører, skal køretøjsenheden afgive en positiv svarmeddelelse.

— Når testeren anmoder om en ny diagnosesession, skal køretøjsenheden først sende en positiv svarmeddelelse på StartDiagnosticSession, før den nye session bliver aktiv i køretøjsenheden. Er køretøjsenheden ikke i stand til at starte den anmodede nye diagnosesession, skal den svare med en negativ svarmeddelelse på StartDiagnosticSession, og den aktuelle session skal fortsætte.

CPR_026 En diagnosesession må kun påbegyndes, hvis der er etableret kommunikation mellem klienten og køretøjsenheden.

CPR_027 Efter en vellykket StartDiagnosticSession med diagnosticSession-parameteren sat til »StandardDiagnsticSession« i anmodningsmeddelelsen skal de i Tabel 4 angivne synkroniseringsparametre være aktive, hvis en anden diagnosesession i forvejen var aktiv.

5.1.2 *Meddelelsesformat*

CPR_028 Meddelelsesformaterne for StartDiagnosticSession er givet i følgende tabeller.

▼B

Tabel 14

StartDiagnosticSession-anmodning

Byte #	Parameternavn	Hex-værdi	Huskeværdi
#1	Formatbyte — fysisk adressering	80	FMT
#2	Adressebyte på destination	EE	TGT
#3	Adressebyte på kilde	tt	SRC
#4	Ekstra længdebyte	02	LEN
#5	**Service-ID på StartDiagnosticSession-anmodning**	**10**	**STDS**
#6	diagnosticSession = [en værdi fra Tabel 17]	xx	DS_…
#7	Kontrolsum	00-FF	CS

Tabel 15

Positivt svar på StartDiagnosticSession

Byte #	Parameternavn	Hex-værdi	Huskeværdi
#1	Formatbyte — fysisk adressering	80	FMT
#2	Adressebyte på destination	tt	TGT
#3	Adressebyte på kilde	EE	SRC
#4	Ekstra længdebyte	02	LEN
#5	**Service-ID for positivt svar på StartDiagnosticSession**	**50**	**STDSPR**
#6	diagnosticSession = [samme værdi som byte #6 i Tabel 14]	xx	DS_…
#7	Kontrolsum	00-FF	CS

Tabel 16

Negativt svar på StartDiagnosticSession

Byte #	Parameternavn	Hex-værdi	Huskeværdi
#1	Formatbyte — fysisk adressering	80	FMT
#2	Adressebyte på destination	tt	TGT
#3	Adressebyte på kilde	EE	SRC

▼B

Byte #	Parameternavn		Hex-værdi	Huskeværdi
#4	Ekstra længdebyte		03	LEN
#5	**Service-ID på negativt svar**		**7F**	**NR**
#6	Service-ID på StartDiagnosticSession-anmodning		10	STDS
#7	Response-Code =	[subFunctionNotSupported ([a])	12	RC_SFNS
		incorrectMessageLength ([b])	13	RC_IML
		conditionsNotCorrect ([c])	22	RC_CNC
#8	Kontrolsum		00-FF	CS

([a]) — værdien i byte #6 i anmodningen understøttes ikke, dvs. ikke i tabel 17
([b]) — anmodningens længde er forkert
([c]) — kriterierne for anmodningen StartDiagnosticSession er ikke opfyldt.

5.1.3 *Parameterdefinition*

CPR_029 Parameteren ***diagnosticSession (DS_)*** anvendes af StartDiagnosticSession-servicen til at vælge en nærmere bestemt adfærd for serveren (serverne). Følgende diagnosesessioner er beskrevet i dette dokument:

Tabel 17

Fastlæggelse af værdier for diagnosticSession

Hex	Beskrivelse	Huskeværdi
81	**StandardDiagnosticSession** Denne diagnosesession tillader alle servicer i **tabel 1, søjle 4 "SD"**. Disse servicer giver mulighed for læsning af data fra en server (køretøjsenhed). Denne diagnosesession er aktiv efter vellykket initialisering mellem klient (tester) og server (køretøjsenhed). Denne diagnosesession kan overskrives af andre diagnosesessioner, som foreskrives i dette afsnit.	**SD**
85	**ECUProgrammingSession** Denne diagnosesession tillader alle servicer i **tabel 1, søjle 6 "ECUPS"**. Disse servicer understøtter programmering af hukommelsen på en server (køretøjsenhed). Denne diagnosesession kan overskrives af andre diagnosesessioner, som er beskrevet i dette afsnit.	**ECUPS**

▼B

Hex	Beskrivelse	Huskeværdi
87	**ECUAdjustmentSession** Denne diagnosesession tillader alle servicer i **tabel 1, søjle 5 "ECUAS".** Disse servicer understøtter ind-/uddatastyring for en server (køretøjsenhed). Denne diagnosesession kan overskrives af andre diagnosesessioner, som foreskrives i dette afsnit.	**ECUAS**

5.2. **SecurityAccess-service**

Skrivning af kalibreringsdata er kun mulig, når køretøjsenheden er i CALIBRATION-funktionstilstand. For at få adgang til CALIBRATION-funktionstilstand skal man isætte et gyldigt værkstedskort i køretøjsenheden og indlæse korrekt PIN-kode i køretøjsenheden.

Når køretøjsenheden er i funktionstilstandene CALIBRATION eller CONTROL er der også adgang til kalibreringens ind-/uddatalinje.

SecurityAccess-servicen kan anvendes til at indlæse PIN-koden og angive over for testeren, om køretøjsenheden er i funktionstilstand CALIBRATION eller ej.

Det kan godtages, at indlæsning af PIN-koden kan ske på anden måde.

5.2.1 *Beskrivelse af meddelelser*

Sikkerhedsservicen består af en SecurityAccess »requestSeed«-meddelelse, senere efterfulgt af en SecurityAccess »sendKey«-meddelelse. SecurityAccess skal udføres efter StartDiagnosticSession.

CPR_033 Testeren skal anvende SecurityAccess »sendKey«-meddelelsen til kontrol af, om køretøjsenheden er klar til at modtage en PIN-kode.

CPR_034 Er køretøjsenheden i forvejen i CALIBRATION-funktionstilstand, skal den besvare forespørgslen ved at sende et »basistal« på 0x0000 ved hjælp af servicen positivt svar på SecurityAccess.

CPR_035 Er køretøjsenheden klar til at modtage en PIN-kode med henblik på kontrol ved hjælp af et værkstedskort, skal den besvare forespørgslen ved at sende et »basistal« større end 0x0000 ved hjælp af servicen positivt svar på SecurityAccess.

CPR_036 Er køretøjsenheden ikke klar til at acceptere en PIN-kode fra testeren, enten fordi det isatte værkstedskort ikke er gyldigt, fordi der ikke er indsat et værkstedskort, eller fordi køretøjsenheden forventer PIN-koden indlæst på anden måde, skal den besvare forespørgslen med et negativt svar, hvor svarkoden er sat til conditionsNotCorrectOrRequestSequenceError.

CPR_037 Testeren skal derefter til sidst anvende servicen SecurityAccess »SendKey«-meddelelse til at fremsende en PIN-kode til køretøjsenheden. For at give tid til ægthedskontrol skal køretøjsenheden anvende den negative svarkode requestCorrectlyReceived-ResponsePending for at forlænge tiden til at

▼B

svare. Dog må den maksimale svartid ikke være over 5 minutter. Så snart den ønskede service er udført, skal køretøjsenheden sende en positiv svarmeddelelse eller negativ svarmeddelelse med en svarkode forskellig fra denne. Den negative svarkode requestCorrectlyReceived-ResponsePending kan af køretøjsenheden gentages, indtil den ønskede service er udført og den endelige svarmeddelelse sendt.

CPR_038 Køretøjsenheden skal kun besvare denne anmodning med servicen positivt svar på SecurityAccess, når den er i CALIBRATION-funktionstilstand.

CPR_039 I følgende tilfælde skal køretøjsenheden besvare denne forespørgsel med et negativt svar med en svarkode sat til:

— subFunctionNot supported: Ugyldigt format af delfunktionens parameter (accessType)

— conditionsNotCorrectOrRequestSequenceError: Køretøjsenheden ikke klar til at acceptere en indtastet PIN-kode

— invalidKey: PIN-kode ikke gyldig, og antal PIN-kodeforsøg ikke overskredet,

— exceededNumberOfAttempts: PIN-kode ikke gyldig, og antal PIN-kodeforsøg overskredet,

— generalReject: korrekt PIN-kode, men gensidig ægthedskontrol med værkstedskort mislykkedes.

5.2.2 *Meddelelsesformat — SecurityAccess — requestSeed*

CPR_040 Meddelelsesformaterne for SecurityAccess »requestSeed«-instruktionerne er angivet i nedenstående tabeller:

Tabel 18

SecurityAccess-anmodning — requestSeed-meddelelse

Byte #	Parameternavn	Hex-værdi	Huskeværdi
#1	Formatbyte — fysisk adressering	80	FMT
#2	Adressebyte på destination	EE	TGT
#3	Adressebyte på kilde	tt	SRC
#4	Ekstra længdebyte	02	LEN
#5	**Service-ID på SecurityAccess-anmodning**	**27**	**SA**
#6	accessType — requestSeed	7D	AT_RSD
#7	Kontrolsum	00-FF	CS

▼B

Tabel 19

Positiv svarmeddelelse på SecurityAccess — requestSeed

Byte #	Parameternavn	Hex-værdi	Huskeværdi
#1	Formatbyte — fysisk adressering	80	FMT
#2	Adressebyte på destination	tt	TGT
#3	Adressebyte på kilde	EE	SRC
#4	Ekstra længdebyte	04	LEN
#5	**Service-ID for positivt svar på SecurityAccess**	**67**	**SAPR**
#6	accessType — requestSeed	7D	AT_RSD
#7	Basistal højt	00-FF	SEEDH
#8	Basistal lavt	00-FF	SEEDL
#9	Kontrolsum	00-FF	CS

Tabel 20

Negativt svar på SecurityAccess

Byte #	Parameternavn	Hex-værdi	Huskeværdi
#1	Formatbyte — fysisk adressering	80	FMT
#2	Adressebyte på destination	tt	TGT
#3	Adressebyte på kilde	EE	SRC
#4	Ekstra længdebyte	03	LEN
#5	**Service-ID for negativeResponse**	**7F**	**NR**
#6	Service-ID på SecurityAccess-anmodning	27	SA
#7	responseCode = [conditionsNotCorrectOrRequestSequenceError	22	RC_CNC
	incorrectMessageLength]	13	RC_IML
#8	Kontrolsum	00-FF	CS

▼B

5.2.3 *Meddelelsesformat — SecurityAccess — sendKey*

CPR_041 Meddelelsesformaterne for SecurityAccess »sendKey«-instruktioner er givet i nedenstående tabeller:

Tabel 21

SecurityAccess-anmodning — sendKey-meddelelse

Byte #	Parameternavn	Hex-værdi	Huskeværdi
#1	Formatbyte — fysisk adressering	80	FMT
#2	Adressebyte på destination	EE	TGT
#3	Adressebyte på kilde	tt	SRC
#4	Ekstra længdebyte	m+2	LEN
#5	**Service-ID på SecurityAccess-anmodning**	**27**	**SA**
#6	accessType — sendKey	7E	AT_SK
#7 til #m+6	Nøgle #1 (høj) … Nøgle #m (lav, m skal være mindst 4 og højst 8)	xx … xx	KEY
#m+7	Kontrolsum	00-FF	CS

Tabel 22

Positiv svarmeddelelse på SecurityAccess — sendKey

Byte #	Parameternavn	Hex-værdi	Huskeværdi
#1	Formatbyte — fysisk adressering	80	FMT
#2	Adressebyte på destination	tt	TGT
#3	Adressebyte på kilde	EE	SRC
#4	Ekstra længdebyte	02	LEN
#5	**Service-ID for positivt svar på SecurityAccess**	**67**	**SAPR**
#6	accessType — sendKey	7E	AT_SK
#7	Kontrolsum	00-FF	CS

▼B

Tabel 23

Negativt svar på SecurityAccess

Byte #	Parameternavn		Hex-værdi	Huskeværdi
#1	Formatbyte — fysisk adressering		80	FMT
#2	Adressebyte på destination		tt	TGT
#3	Adressebyte på kilde		EE	SRC
#4	Ekstra længdebyte		03	LEN
#5	**Service-ID på NegativeResponse**		**7F**	**NR**
#6	Service-ID på SecurityAccess-anmodning		27	SA
#7	Response-Code =	[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	Kontrolsum		00-FF	CS

6. DATAOVERFØRSELSSERVICER

I følgende tabel beskrives de servicer, som er til rådighed:

Tabel 24

Dataoverførselsservicer

Servicens navn	Beskrivelse
ReadDataByIdentifier	Klienten anmoder om overførsel af den aktuelle værdi af en post med adgang gennem recordDataIdentifier.
WriteDataByIdentifier	Klienten anmoder om at skrive en post, hvortil der er adgang gennem recordDataIdentifier

▼B

6.1. **ReadDataByIdentifier-service**

6.1.1 *Beskrivelse af meddelelser*

CPR_050 Servicen ReadDataByIdentifier anvendes af klienten til at skrive recordValues (dataværdier) fra en server. Data identificeres af en recordDataIdentifier. Fabrikanten af køretøjsenheden har ansvaret for, at de for serveren gældende betingelser er opfyldt ved udførelse af denne service.

6.1.2 *Meddelelsesformat*

CPR_051 Meddelelsesformaterne for ReadDataByIdentifier instruktioner er givet i følgende tabeller.

Tabel 25

ReadDataByIdentifier-anmodning

Byte #	Parameternavn	Hex-værdi	Huskeværdi
#1	Formatbyte — fysisk adressering	80	FMT
#2	Adressebyte på destination	EE	TGT
#3	Adressebyte på kilde	tt	SRC
#4	Ekstra længdebyte	03	LEN
#5	**Service-ID på ReadDataByIdentifier-anmodning**	**22**	**RDBI**
#6 til #7	recordDataIdentifier = [en værdi fra Tabel 28]	xxxx	RDI_…
#8	Kontrolsum	00-FF	CS

Tabel 26

Positivt svar på ReadDataByIdentifier

Byte #	Parameternavn	Hex-værdi	Huskeværdi
#1	Formatbyte — fysisk adressering	80	FMT
#2	Adressebyte på destination	tt	TGT
#3	Adressebyte på kilde	EE	SRC
#4	Ekstra længdebyte	m+3	LEN
#5	**Service-ID for positivt svar på ReadDataByIdentifier**	**62**	**RDBIPR**
#6 og #7	recordDataIdentifier = [samme værdi som byte #6 og #7 Tabel 25]	xxxx	RDI_…

▼B

Byte #	Parameternavn		Hex-værdi	Huskeværdi
#8 til #m+7	dataRecord[] =	[data#1	xx	DREC_DATA1
		:	:	:
		data#m]	xx	DREC_DATAm
#m+8	Kontrolsum		00-FF	CS

Tabel 27

Negativt svar på ReadDataByIdentifier

Byte #	Parameternavn		Hex-værdi	Huskeværdi
#1	Formatbyte — fysisk adressering		80	FMT
#2	Adressebyte på destination		tt	TGT
#3	Adressebyte på kilde		EE	SRC
#4	Ekstra længdebyte		03	LEN
#5	**Service-ID på NegativeResponse**		**7F**	**NR**
#6	Service-ID på ReadDataByIdentifier-anmodning		22	RDBI
#7	ResponseCode=	[requestOutOfRange	31	RC_ROOR
		incorrectMessageLength	13	RC_IML
		conditionsNotCorrect]	22	RC_CNC
#8	Kontrolsum		00-FF	CS

6.1.3 *Parameterdefinition*

CPR_052 Parameteren ***recordDataIdentifier (RDI_)*** i anmodningen ReadDataByIdentifier identificerer en datapost.

CPR_053 De værdier af recordDataIdentifier, som defineres af dette dokument, er vist i tabellen nedenfor.

Tabellen recordDataIdentifier består af tre søjler og mange linjer.

— **Søjle 1** indeholder den »Hex-værdi«, der er tilordnet den i søjle 3 angivne recordDataIdentifier.

— **Søjle 2** fastlægger det dataelement i tillæg 1, som er knyttet til recordDataIdentifier (omkodning er undertiden nødvendig).

▼B

— **Søjle 3** angiver navnet på den tilsvarende recordDataIdentifier.

— **Søjle 4** angiver huskeværdien af denne recordDataIdentifier.

Tabel 28

Definition af recordDataIdentifier-værdier

Hex	Dataelement	recordDataIdentifier-navn (se format i afsnit 8.2)	Huskeværdi
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 Parameteren ***dataRecord (DREC_)*** anvendes af den positive svarmeddelelse på ReadDataByIdentifier til at hente den datapost, der er identificeret ved recordDataIdentifier, til klienten (testeren). Dataformater er fastlagt i punkt 8. Der kan fastlægges andre dataposter, som brugeren frivilligt kan benytte, herunder køretøjsenhedsspecifikke inddata, interne data og uddata, men disse er ikke defineret i dette dokument.

6.2. WriteDataByIdentifier-service

6.2.1 *Beskrivelse af meddelelser*

CPR_056 Servicen WriteDataByIdentifier anvendes af klienten til at skrive dataværdier til en server. Data identificeres af en recordDataIdentifier. Fabrikanten af køretøjsenheden har ansvaret for, at de for serveren gældende betingelser er opfyldt ved udførelse af denne service. For at opdatere parametrene i Tabel 28 skal køretøjsenheden være i CALIBRATION-funktionstilstand.

6.2.2 *Meddelelsesformat*

CPR_057 Meddelelsesformaterne for WriteDataByIdentifier-instruktioner er givet i nedenstående tabeller.

▼B

Tabel 29

WriteDataByIdentifier-anmodning

Byte #	Parameternavn	Hex-værdi	Huskeværdi
#1	Formatbyte — fysisk adressering	80	FMT
#2	Adressebyte på destination	EE	TGT
#3	Adressebyte på kilde	tt	SRC
#4	Ekstra længdebyte	m+3	LEN
#5	**Service-ID på WriteDataByIdentifier-anmodning**	**2E**	**WDBI**
#6 til #7	recordDataIdentifier = [en værdi fra Tabel 28]	xxxx	RDI_…
#8 til m+7	dataRecord[] = [data#1 : data#m]	xx : xx	DREC_DATA1 : DREC_DATAm
#m+8	Kontrolsum	00-FF	CS

Tabel 30

Positivt svar på WriteDataByIdentifier

Byte #	Parameternavn	Hex-værdi	Huskeværdi
#1	Formatbyte — fysisk adressering	80	FMT
#2	Adressebyte på destination	tt	TGT
#3	Adressebyte på kilde	EE	SRC
#4	Ekstra længdebyte	03	LEN
#5	**Service-ID for positivt svar på WriteDataByIdentifier**	**6E**	**WDBIPR**
#6 til #7	recordDataIdentifier = [samme værdi som byte #6 og #7 Tabel 29]	xxxx	RDI_…
#8	Kontrolsum	00-FF	CS

▼B

Tabel 31

Negativt svar på WriteDataByIdentifier

Byte #	Parameternavn		Hex-værdi	Huskeværdi
#1	Formatbyte — fysisk adressering		80	FMT
#2	Adressebyte på destination		tt	TGT
#3	Adressebyte på kilde		EE	SRC
#4	Ekstra længdebyte		03	LEN
#5	**Service-ID på NegativeResponse**		**7F**	**NR**
#6	Service-ID på WriteDataByIdentifier-anmodning		2E	WDBI
#7	ResponseCode=	[requestOutOfRange	31	RC_ROOR
		incorrectMessageLength	13	RC_IML
		conditionsNotCorrect]	22	RC_CNC
#8	Kontrolsum		00-FF	CS

6.2.3 *Parameterdefinition*

Parameteren ***recordDataIdentifier (RDI_)*** er defineret i Tabel 28.

Parameteren ***dataRecord (DREC_)*** anvendes i anmodningen ReadDataByIdentifier til at hente de dataværdier, der er identificeret ved recordDataIdentifier, til serveren (køretøjsenheden). Dataformater er fastlagt i punkt 8.

7. KONTROL AF TESTIMPULSER — FUNKTIONSENHED FOR IND-/UDDATASTYRING

I følgende tabel beskrives de servicer, som er til rådighed:

Tabel 32

Funktionsenhed for ind-/uddatastyring

Servicens navn	Beskrivelse
InputOutputControlByIdentifier	Klienten anmoder om at måtte styre et sæt serverspecifikke ind-/uddata.

7.1. **InputOutputControlByIdentifier-service**

7.1.1 *Beskrivelse af meddelelser*

Testimpulser kan styres eller overvåges ved hjælp af en passende tester, som tilsluttes via det forreste stik.

▼B

CPR_058 Denne I/O-signallinje for kalibrering kan konfigureres med ordrer over K-linjen ved hjælp af servicen InputOutputControlByIdentifier, med hvilken man vælger den ønskede ind- eller udlæsningsfunktion for linjen. Linjen kan have følgende status:

— frakoblet

— speedSignalInput, hvor der gennem I/O-signallinjen for kalibrering tilføres et hastighedssignal (testsignal), som erstatter hastighedssignalet fra bevægelsesføleren; denne funktion er ikke tilgængelig i funktionstilstanden CONTROL

— realTimeSpeedSignalOutputSensor, hvor der gennem I/O-signallinjen for kalibrering afgives et hastighedssignal fra bevægelsesføleren; denne funktion er ikke tilgængelig i funktionstilstanden CONTROL

— RTCOutput, hvor der gennem I/O-signallinjen for kalibrering afgives et UTC-kloksignal.

CPR_059 Køretøjsenheden skal have indledt en justeringssession og skal være i CALIBRATION- eller CONTROL-funktionstilstand, for at linjens tilstand kan konfigureres. Når køretøjsenheden er i funktionstilstanden CALIBRATION, kan der vælges fire status for linjen (disabled, speedSignalInput, realTimeSpeedSignalOutputSensor, RTCOutput). Når køretøjsenheden er i funktionstilstanden CONTROL, kan der kun vælges to status for linjen (disabled, realTimeSpeedOutputSensor). Når køretøjsenheden forlader justeringssession eller CALIBRATION- eller CONTROL-funktionstilstanden, skal den stille I/O-signallinjen for kalibrering tilbage i »deaktiveret« tilstand (standardtilstanden).

CPR_060 Hvis der modtages hastighedsimpulser på køretøjsenhedens indgangslinje for tidstro hastighedssignal, mens I/O-signallinjen for kalibrering er stillet på indgang, vil I/O-signallinjen blive stillet på udgang eller ført tilbage i deaktiveret tilstand.

CPR_061 Sekvensen skal være:

— Der oprettes kommunikation med StartCommunication-servicen

— Der åbnes en justeringssession med StartDiagnosticSession-servicen og benyttes CALIBRATION-tilstand (rækkefølgen af disse to operationer har ikke betydning)

— Tilstanden af uddata ændres med InputOutputControlByIdentifier-servicen.

7.1.2 *Meddelelsesformat*

CPR_062 Meddelelsesformaterne af InputOutputControlByIdentifier-instruktionerne er givet i følgende tabeller.

▼B

Tabel 33

InputOutputControlByIdentifier-anmodning

Byte #	Parameternavn	Hex-værdi	Huskeværdi
#1	Formatbyte — fysisk adressering	80	FMT
#2	Adressebyte på destination	EE	TGT
#3	Adressebyte på kilde	tt	SRC
#4	Ekstra længdebyte	xx	LEN
#5	**Sid for InputOutputControlByIdentifier-anmodning**	**2F**	**IOCBI**
#6 og #7	InputOutputIdentifier = [CalibrationInputOutput]	F960	IOI_CIO
#8 eller #8 til #9	ControlOptionRecord = [		COR_…
	inputOutputControlParameter — en værdi fra Tabel 36	xx	IOCP_…
	controlState — en værdi fra Tabel 37 (se bemærkning nedenfor)]	xx	CS_…
#9 eller #10	Kontrolsum	00-FF	CS

Bemærk: Parameteren controlState findes kun i visse tilfælde (se 7.1.3).

Tabel 34

Positivt svar på InputOutputControlByIdentifier

Byte #	Parameternavn	Hex-værdi	Huskeværdi
#1	Formatbyte — fysisk adressering	80	FMT
#2	Adressebyte på destination	tt	TGT
#3	Adressebyte på kilde	EE	SRC
#4	Ekstra længdebyte	xx	LEN
#5	**S-id for positivt svar på inputOutputControlByIdentifier**	**6F**	**IOCBIPR**
#6 og #7	inputOutputIdentifier = [CalibrationInputOutput]	F960	IOI_CIO
#8 eller #8 til #9	controlStatusRecord = [		CSR_
	inputOutputControlParameter (samme værdi som byte #8 i Tabel 33)	xx	IOCP_…
	controlState (samme værdi som byte #9 Tabel 33)] (i givet fald)	xx	CS_…
#9 eller #10	Kontrolsum	00-FF	CS

▼B

Tabel 35

Negativt svar på InputOutputControlByIdentifier

Byte #	Parameternavn	Hex-værdi	Huskeværdi
#1	Formatbyte — fysisk adressering	80	FMT
#2	Adressebyte på destination	tt	TGT
#3	Adressebyte på kilde	EE	SRC
#4	Ekstra længdebyte	03	LEN
#5	**Service-ID for negativeResponse**	**7F**	**NR**
#6	Sid for anmodning om inputOutputControlByIdentifier	2F	IOCBI
#7	responseCode=[		
	incorrectMessageLength	13	RC_IML
	conditionsNotCorrect	22	RC_CNC
	requestOutOfRange	31	RC_ROOR
	deviceControlLimitsExceeded]	7A	RC_DCLE
#8	Kontrolsum	00-FF	CS

7.1.3 *Parameterdefinition*

CPR_064 Parameteren ***inputOutputControlParameter (IOCP_)*** er defineret i følgende tabel:

Tabel 36

Definition af inputOutputControlParameter-værdier

Hex	Beskrivelse	Huskeværdi
00	**ReturnControlToECU** Denne værdi angiver over for serveren (køretøjsenheden), at testeren ikke længere kontrollerer ind/ud-signallinjen for kalibrering.	RCTECU
01	**ResetToDefault** Denne værdi skal anmode serveren (køretøjsenheden) om at tilbagestille ind/ud-signallinjen for kalibrering til dens standardtilstand.	RTD

▼B

Hex	Beskrivelse	Huskeværdi
03	**ShortTermAdjustment** Denne værdi skal fortælle serveren (køretøjsenheden), at den anmodes om at justere ind/ud-signallinjen for kalibrering til den værdi, som er indeholdt i controlState-parameteren.	STA

CPR_065 Parameteren ***controlState***, som kun er til stede, når inputOutputControlParameter er sat til ShortTermAdjustment, er fastlagt i følgende tabel:

Tabel 37

Definition af controlState-værdier

Funktionstilstand	Hex-værdi	Beskrivelse
Deaktiver	00	I/O-linjen er deaktiveret (standardtilstand)
Aktivér	01	Aktivér ind/ud-linje for kalibrering som speedSignalInput
Aktivér	02	Aktivér ind/ud-linje for kalibrering som realTimeSpeedSignalOutputSensor
Aktivér	03	Aktivér ind/ud-linje for kalibrering som RTCOutput

8. FORMATER TIL DATARECORDS

Dette punkt angiver:

— generelle regler, som gælder for områderne for de parametre, som overføres af køretøjsenheden til testeren

— formater, som skal anvendes til data, som overføres med de datatransmissionsservicer, der er beskrevet i punkt 6.

CPR_067 Alle angivne parametre skal være understøttet af køretøjsenheden.

CPR_068 De data, som overføres af køretøjsenheden til testeren som svar på en forespørgselsmeddelelse, skal være af den målte type (dvs. den aktuelle værdi af den anmodede parameter, således som den måles eller observeres af køretøjsenheden).

8.1. **Værdiområder for overførte parametre**

CPR_069 Tabel 38 fastlægger de områder, som anvendes til at bestemme gyldigheden af en overført parameter.

CPR_070 Værdierne i området »fejlindikator« giver køretøjsenheden mulighed for øjeblikkelig at angive, at der som følge af en fejl i takografen ikke aktuelt forefindes gyldige parameterværdier.

CPR_071 Værdierne i området »forefindes ikke« giver køretøjsenheden mulighed for at overføre en meddelelse, som indeholder en parameter, som ikke er til rådighed eller ikke understøttes i den pågældende programenhed. Værdierne i området »ikke anmodet« giver en enhed mulighed for at overføre en kommandomeddelelse og fastlægge de parametre, for hvilke der ikke forventes noget svar fra den modtagende enhed.

▼B

CPR_072 Hvis der som følge af komponentsvigt ikke kan overføres gyldige data for en parameter, skal fejlindikatoren som beskrevet i Tabel 38 anvendes i stedet for den pågældende parameters data. Men hvis de målte og beregnede data har resulteret i en værdi, som er gyldig, men falder uden for det fastlagte parameterområde, bør fejlindikatoren ikke benyttes. Data bør overføres med den pågældende minimum- eller maksimumværdi af parameteren.

Tabel 38

Områder for dataRecords

Områdenavn	1 byte (Hex-værdi)	2 bytes (Hex-værdi)	4 bytes (Hex-værdi)	ASCII
Gyldigt signal	00 til FA	0000 til FAFF	00000000 til FAFFFFFF	1 til 254
Parameterspecifik indikator	FB	FB00 til FBFF	FB000000 til FBFFFFFF	ingen
Område reserveret fremtidige indikatorbit	FC til FD	FC00 til FDFF	FC000000 til FDFFFFFF	ingen
Fejlindikator	FE	FE00 til FEFF	FE000000 a FEFFFFFF	0
Foreligger ikke eller er ikke anmodet	FF	FF00 til FFFF	FF000000 til FFFFFFFF	FF

CPR_073 For parametre kodet i ASCII skal ASCII-tegnet »*« reserveres som skilletegn.

8.2. **Formater til dataRecords**

Tabel 39 til Tabel 42 nedenfor angiver de formater, som skal anvendes via servicerne ReadDataByIdentifier og WriteDataByIdentifier.

CPR_074 Tabel 39 angiver længde, opløsning og arbejdsområde for hver parameter, som er identificeret ved sin recordDataIdentifier:

Tabel 39

Format af dataRecords

Parameternavn	Datalængde (byte)	Resolution	Arbejdsområde
TimeDate	8	Se nærmere i Tabel 40	
HighResolutionTotalVehicle-Distance	4	forstærkning 5 m/bit, forskydning 0 m	0 til +21 055 406 km
Kfactor	2	forstærkning 0,001 impulser/m/bit, forskydning 0	0 til 64,255 impulser/m
LfactorTyreCircumference	2	forstærkning 0,125 10^{-3} m/bit, forskydning 0	0 til 8,031 m
WvehicleCharacteristicFactor	2	forstærkning 0,001 impulser/m/bit, forskydning 0	0 til 64,255 impulser/m
TyreSize	15	ASCII	ASCII
NextCalibrationDate	3	Se nærmere i Tabel 41	
SpeedAuthorised	2	forstærkning 1/256 km/t/bit, forskydning 0	0 til 250 996 km/t

▼B

Parameternavn	Datalængde (byte)	Resolution	Arbejdsområde
RegisteringMemberState	3	ASCII	ASCII
VehicleRegistrationNumber	14	Se nærmere i Tabel 42	
VIN	17	ASCII	ASCII

CPR_075 Tabel 40 angiver formater for de forskellige byte i Time-Date-parameteren:

Tabel 40

Detaljeret format af TimeDate (recordDataIdentifier-værdi # F90B)

Byte	Parameterdefinition	Resolution	Arbejdsområde
1	Sekunder	Forstærkning 0,25 s/bit, forskydning 0 s	0 til 59,75 s
2	Minutter	Forstærkning 1 min/bit, forskydning 0 min	0 til 59 min
3	Timer	Forstærkning 1 t/bit, forskydning 0 t	0 til 23 t
4	Måned	Forstærkning 1 måned/bit, forskydning 0 måned	1 til 12 måneder
5	Dag	Forstærkning 0,25 dag/bit, forskydning 0 dage (se bemærkning under Tabel 41)	0,25 til 31,75 dage
6	År	Forstærkning 1 år/bit, forskydning + 1985 år (se bemærkning under Tabel 41)	år 1985 til 2235
7	Lokal forskydning, minutter	Forstærkning 1 min/bit, forskydning – 125 min	– 59 til + 59 min
8	Forskydning af lokalt timetal	Forstærkning 1 t/bit, forskydning – 125 t	– 23 til + 23 t

CPR_076 Tabel 41 angiver formater for de forskellige byte i NextCalibrationDate-parameteren:

Tabel 41

Detaljeret format af NextCalibrationDate (recordDataIdentifier-værdi # F922)

Byte	Parameterdefinition	Resolution	Arbejdsområde
1	Måned	Forstærkning 1 måned/bit, forskydning 0 måned	1 til 12 måneder
2	Dag	Forstærkning 0,25 dag/bit, forskydning 0 dage (se bemærkning nedenfor)	0,25 til 31,75 dage
3	År	Forstærkning 1 år/bit, forskydning + 1985 år (se bemærkning nedenfor)	år 1985 til 2235

▼B

Bemærkning vedrørende brug af parameteren »Dag«:

1) En værdi på 0 for datoen er ugyldig. Værdierne 1, 2, 3 og 4 anvendes til at angive første dag i måneden. Værdierne 5, 6, 7 og 8 angiver anden dag i måneden osv.

2) Denne parameter kan ikke påvirke eller ændre ovenstående timeparameter.

Bemærkning vedrørende brug af parameterbyten »År«:

En værdi på 0 for året angiver år 1985, mens en værdi på 1 angiver år 1986 osv.

CPR_078 Tabel 42 angiver formater for de forskellige bytes i VehicleRegistrationNumber-parameteren:

Tabel 42

Detaljeret format af VehicleRegistrationNumber (recordDataIdentifier-værdi # F97E)

Byte	Parameterdefinition	Resolution	Arbejdsområde
1	Tegntabel (som fastlagt i tillæg 1)	ASCII	01 til 0A
2 — 14	Køretøjets indregistreringsnummer (som defineret i tillæg 1)	ASCII	ASCII

▼B

Tillæg 9.

TYPEGODKENDELSE — LISTE OVER MINDSTEKRAV TIL PRØVER

INDHOLDSFORTEGNELSE

1. INDLEDNING

2. FUNKTIONSPRØVER FOR KØRETØJSENHED

3. FUNKTIONSPRØVER FOR BEVÆGELSESFØLER

4. FUNKTIONSPRØVER FOR TAKOGRAFKORT

5. PRØVNING AF EKSTERNT GNSS-UDSTYR

6. PRØVNING AF FACILITETEN TIL FJERNKOMMUNIKATION

7. FUNKTIONSPRØVNING AF PAPIR

8. INTEROPERABILITETSPRØVER

1. INDLEDNING

1.1. **Typegodkendelse**

EF-typegodkendelse for kontrolapparater (eller komponenter dertil) eller takografkort bygger på

— en **sikkerhedsattestering** baseret på fælles kriterier efter et sikkerhedsmål, som er i fuld overensstemmelse med tillæg 10 til dette bilag (færdiggøres/ændres)

— en **funktionel attestering**, som udføres af en medlemsstats myndigheder, og ved hvilken det attesteres, at den afprøvede genstand opfylder forskrifterne i dette bilag hvad angår udførte funktioner, målenøjagtighed og miljøegenskaber

— en **interoperabilitetsattestering**, som udføres af den kompetente myndighed, og som certificerer, at kontrolapparatet (eller takografkortet) er gensidigt fuldt kompatibelt med den nødvendige type takografkort (eller kontrolapparat) (se afsnit 8 i dette bilag).

I tillægget foreskrives det, hvilke prøver der som minimum skal udføres af medlemsstatens myndigheder ved funktionsprøverne, og hvilke prøver der som minimum skal udføres af de kompetente myndigheder under interoperabilitetsprøverne. Der er ingen yderligere forskrifter for de procedurer, som skal følges ved udførelse af prøverne eller den pågældende type prøver.

Spørgsmål vedrørende sikkerhedsattestering er ikke omfattet af dette tillæg. Såfremt nogle af de prøver, som kræves til typegodkendelse, udføres som led i sikkerhedsvurdering og -attestering, behøver disse prøver ikke udføres igen. I så fald er det tilstrækkeligt kun at kontrollere resultaterne af disse sikkerhedsprøver. De krav, som der forventes prøvet for (eller nærtbeslægtede prøver foretaget) som led i sikkerhedsattesteringen, er mærket med »*« i tillægget.

De nummererede krav refererer til bilagets korpus, mens de øvrige krav refererer til de andre tillæg (f.eks. refererer PIC_001 til kravet PIC_001 i tillæg 3 Piktogrammer).

I dette tillæg er særskilt omhandlet typegodkendelse af bevægelsesføler, køretøjsenhed og eksternt GNSS-udstyr som komponenter i kontrolapparatet. Hver komponent får sin egen typegodkendelsesattest, hvori de

▼B

øvrige kompatible komponenter angives. Funktionsprøvningen af bevægelsesføleren (eller det eksterne GNSS-udstyr) foretages sammen med køretøjsenheden og omvendt.

Der kræves ikke interoperabilitet mellem hver enkelt model af bevægelsesføleren/det eksterne GNSS-udstyr og hver enkelt model af køretøjsenheden. I relevante tilfælde kan typegodkendelsen for en bevægelsesføler (eller eksternt GNSS-udstyr) kun udstedes sammen med typegodkendelsen for den pågældende køretøjsenhed og omvendt.

1.2. **Referencer**

I dette tillæg henvises til følgende referencer:

IEC 60068-2-1: Environmental testing — Part 2-1: Tests — Test A: Cold

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: Environmental testing. Part 2: Tests. Test Ea and guidance: Shock

IEC 60068-2-30: Environmental testing — Part 2-30: Tests — Test Db: Damp heat, cyclic (12 h + 12 h cycle)

IEC 60068-2-64: Environmental testing — Part 2-64: Tests — Test Fh: Vibration, broadband random and guidance

IEC 60068-2-78 Environmental testing — Part 2-78: Tests — Test Cab: Damp heat, steady state

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..

▼B

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

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 Paper and board — Determination of thickness, density and specific volume

FN/ECE R10 Uniform provisions concerning the approval of vehicles with regard to electromagnetic compatibility (United Nation Economic Commission for Europe)

2. FUNKTIONSPRØVER FOR KØRETØJSENHED

Nr.	Prøve	Beskrivelse	Tilknyttede krav
1	**Administrativ undersøgelse**		
1.1	Dokumentation	Dokumentationens korrekthed	
1.2	Fabrikantens prøvningsresultater	Resultater af fabrikantens prøvning, udført med kombination. Eftervisning på papir	88, 89,91
2	**Besigtigelse**		
2.1	Overensstemmelse med dokumentationen		
2.2	Identifikation/mærkning		224 til 226
2.3	Materialer		219 til 223
2.4	Plombering		398, 401 til 405
2.5	Eksterne grænseflader		
3	**Funktionsprøver**		
3.1	Ydede funktioner		03, 04, 05, 07, 382,
3.2	Funktionsmåder		09 til 11*, 132, 133
3.3	Funktioner og ret til dataadgang		12* 13*, 382, 383, 386 til 389
3.4	Overvågning af isætning og udtagning af kort		15, 16, 17, 18, 19*, 20*, 132
3.5	Måling af hastighed og tilbagelagt afstand		21 til 31

▼B

Nr.	Prøve	Beskrivelse	Tilknyttede krav
3.6	Tidsmåling (prøvning udført ved 20 °C)		38 til 43
3.7	Overvågning af føreraktiviteter		44 til 53, 132
3.8	Overvågning af kørestatus		54, 55, 132
3.9	Manuel indlæsning		56 til 62
3.10	Forvaltning af virksomhedslåse		63 til 68
3.11	Overvågning af kontrolaktiviteter		69, 70
3.12	Detektion af hændelser og/eller fejl		71 til 88 132
3.13	Identifikationsdata for apparat		93*, 94*, 97, 100
3.14	Data vedrørende isætning og udtagning af førerkort		102* til 104*
3.15	Føreraktivitetsdata		105* til 107*
3.16	Data om steder og positioner		108* til 112*
3.17	Kilometertællerdata		113* til 115*
3.18	Detaljerede hastighedsdata		116*
3.19	Data vedrørende hændelser		117*
3.20	Data vedrørende fejl		118*
3.21	Kalibreringsdata		119* til 121*
3.22	Tidsjusteringsdata		124*, 125*
3.23	Kontrolaktivitetsdata		126*, 127*
3.24	Data vedrørende virksomhedslåse		128*
3.25	Data vedrørende dataoverførselsaktivitet		129*
3.26	Data vedrørende særlige omstændigheder		130*, 131*
3.27	Registrering og lagring på takografkort		134, 135, 136*, 137*, 139*, 140, 141 142, 143, 144*, 145*, 146*, 147, 148
3.28	Visning på skærm		90, 132, 149 til 166, PIC_001, DIS_001
3.29	Trykning		90, 132, 167 til 179, PIC_001, PRT_001 til PRT_014
3.30	Advarsel		132, 180 til 189, PIC_001
3.31	Dataoverførsel til eksterne medier		90, 132, 190 til 194
3.32	Fjernkommunikation i forbindelse med målrettede vejsidekontroller		195 til 197
3.33	Udlæsning af data til supplerende eksterne enheder		198, 199

▼B

Nr.	Prøve	Beskrivelse	Tilknyttede krav
3.34	Kalibrering		202 til 206*, 383, 384, 386 til 391
3.35	Kalibreringskontrol ved vejsiden		207 til 209
3.36	Tidsjustering		210* til 212*
3.37	Fravær af forstyrrelse af ekstra funktioner		06, 425
3.38	Grænseflade til bevægelsesføler		02, 122
3.39	Eksternt GNSS-udstyr		03, 123
3.40	Det kontrolleres, at køretøjsenheden detekterer, registrerer og lagrer den/de hændelse(er) og/eller den/de fejl, som køretøjsenhedsfabrikanten har defineret, hvis en samparret bevægelsesføler reagerer på magnetiske felter, som forstyrrer køretøjets bevægelsesregistrering.		217
3.41	Krypteringsprogram og standardiserede domæneparametre		CSM_48, CSM_50
4	**Miljøprøver**		
4.1	Temperatur	Funktionaliteten eftervises gennem: Prøvning i overensstemmelse med ISO 16750-4, Chapter 5.1.1.2: Funktionsprøve ved lav temperatur (72 timer ved – 20 °C) For denne prøve henvises til IEC 60068-2-1: Environmental testing — Part 2-1: Tests — Test A: Cold Test i overensstemmelse med ISO 16750-4: Chapter 5.1.2.2: High temperature operation test (72 timer ved 70 °C) For denne prøve henvises til IEC 60068-2-2: Basic environmental testing procedures; part 2: tests; tests B: dry heat Prøvning i overensstemmelse med ISO 16750-4: Chapter 5.3.2: Rapid change of temperature with specified transition duration (– 20 °C/70 °C, 20 cycles, dwell time 2h at each temperature) Et reduceret sæt prøvninger (af dem, som foreskrives i afsnit 3 af denne tabel) kan udføres ved den lave temperatur, den høje temperatur og med gennemgang af temperaturcyklusserne	213
4.2	Fugtighed	Det eftervises, at køretøjsenheden kan modstå en cyklisk fugtighedsprøve (varmeprøve) ved gennemgang af IEC 60068-2-30, prøve Db, seks 24 timers cyklusser, hvor hver temperatur varierer fra + 25 °C til + 55 °C, og hvor den relative fugtighed er 97 % ved + 25 °C og 93 % ved + 55 °C	214

▼B

Nr.	Prøve	Beskrivelse	Tilknyttede krav
4.3	Mekanisk masse	1. Sinusvibrationer. Det kontrolleres, at køretøjsenheden kan modstå sinusvibrationer med følgende egenskaber: Konstant skift mellem 5 og 11 Hz: Topværdi 10mm konstant acceleration mellem 11 og 300 Hz: 5g Prøvning for dette krav sker med IEC 60068-2-6, prøve Fc, med en mindste prøvningsvarighed på 3 × 12 timer (12 timer for hver akseretning) ISO 16750-3 kræver ikke en sinusvibrationsprøvning for enheder, der sidder i afkoblede førerhuse. 2. Tilfældige vibrationer: Prøvning i overensstemmelse med ISO 16750-3: Chapter 4.1.2.8: Test VIII: Commercial vehicle, decoupled vehicle cab Prøvning for tilfældige vibrationer, 10…2 000 Hz, kvadratisk middel, lodret: 21,3 m/s^2, kvadratisk middel, langsgående: 11,8 m/s^2, kvadratisk middel, tværgående: 13,1 m/s^2, 3 akser, 32 timer pr. akse, herunder temperaturcyklus: – 20…70 °C. For denne prøve henvises til IEC 60068-2-64: Environmental testing — Part 2-64: Tests — Test Fh: Vibration, broadband random and guidance 3. Stød: mekanisk stød med 3g halv-sinus i overensstemmelse med ISO 16750. De ovenfor beskrevne prøvninger udføres på forskellige prøveeksemplarer af den afprøvede apparattype.	219
4.4	Beskyttelse mod vand og fremmedlegemer	Prøvning i overensstemmelse med ISO 20653: Road vehicles — Degree of protection (IP code) — Protection of electrical equipment against foreign objects, water and access (No change in parameters); Minimum value IP 40	220, 221
4.5	Overspændingsbeskyttelse	Det kontrolleres, at køretøjsenheden kan modstå en strømforsyning på: 24 V-udførelse: 34 V ved + 40 °C 1 time 12 V-udførelse: 17 V ved + 40 °C 1 time (ISO 16750-2)	216

▼B

Nr.	Prøve	Beskrivelse	Tilknyttede krav
4.6	Beskyttelse mod omvendt polaritet	Det kontrolleres, at køretøjsenheden kan modstå polvending af strømforsyningen (ISO 16750-2)	216
4.7	Kortslutningsbeskyttelse	Det kontrolleres, at ind- og udgangssignaler er beskyttet mod kortslutning til strømforsyningen og til stel (ISO 16750-2)	216
5	**Prøver for elektromagnetisk kompatibilitet**		
5.1	Strålingsemission og følsomhed	Overensstemmelse med ECE-regulativ R10	218
5.2	Elektrostatisk udladning	Overensstemmelse med ISO 10605:2008 + Technical Corrigendum:2010 + AMD1:2014: +/– 4 kV for kontakt og +/– 8 kV for udladning i luften	218
5.3	Transient nedre ledningsoverførsel for strømforsyning	For 24 V-udførelse: overensstemmelse med ISO 7637-2 og ECE-regulativ nr. 10, rev. 3: impuls 1a: Vs = – 450 V, Ri = 50 ohm impuls 2a: Vs = + 37 V, Ri = 2 ohm impuls 2b: Vs = + 20V, Ri = 0,05 ohm impuls 3a: Vs = – 150V, Ri = 50 ohm impuls 3b: Vs = + 150V, Ri = 50 ohm impuls 4: Vs = – 16 V Va = – 12 V t6 = 100 ms impuls 5: Vs = + 120 V Ri = 2,2 ohm td = 250 ms For 12 V-udførelse: overensstemmelse med ISO 7637-1 og ECE-regulativ nr. 10, rev. 3: impuls 1: Vs = – 75V, Ri = 10 ohm impuls 2a: Vs = + 37 V, Ri = 2 ohm impuls 2b: Vs = + 10V, Ri = 0,05 ohm impuls 3a: Vs = – 112V, Ri = 50 ohm impuls 3b: Vs = + 75V, Ri = 50 ohm impuls 4: Vs = – 6 V Va = – 5 V t6 = 15 ms impuls 5: Vs = + 65 V Ri = 3 ohm td = 100 ms Impuls 5 skal kun afprøves for køretøjsenheder bestemt til montering i køretøjer uden ekstern fælles overbelastningsbeskyttelse For så vidt angår overbelastningsbeskyttelse henvises til ISO 16750-2, 4. udgave, afsnit 4.6.4.	218

▼B

3. FUNKTIONSPRØVER FOR BEVÆGELSESFØLER

Nr.	Prøve	Beskrivelse	Tilknyttede krav
1.	**Administrativ undersøgelse**		
1.1	Dokumentation	Dokumentationens korrekthed	
2.	**Besigtigelse**		
2.1.	Overensstemmelse med dokumentationen		
2.2.	Identifikation/mærkning		225, 226
2.3	Materialer		219 til 223
2.4.	Plombering		398, 401 til 405
3.	**Funktionsprøver**		
3.1	Identifikationsdata for føler		95 til 97*
3.2	Bevægelsesføler — samparring med køretøjsenhed		122*, 204
3.3	Bevægelsesregistrering Nøjagtighed af målingen af bevægelsen		30 til 35
3.4	Grænseflade for køretøjsenhed		02
3.5	Det kontrolleres, at bevægelsesføleren er upåvirkelig af konstante magnetiske felter. Ellers kontrolleres det, at bevægelsesføleren reagerer på konstante magnetiske felter, som forstyrrer køretøjets bevægelsesregistrering, således at en tilsluttet køretøjsenhed kan detektere, registrere og lagre følerfejl.		217
4.	**Miljøprøver**		
4.1	Arbejdstemperatur	Funktionaliteten (som defineret i prøve nr. 3.3) efterprøves i temperaturintervallet [– 40 °C; + 135 °C] gennem: IEC 60068-2-1 prøve Ad, med en prøvningsvarighed på 96 timer ved den laveste temperatur To_{min} IEC 60068-2-2 prøve Bd, med en prøvningsvarighed på 96 timer ved den højeste temperatur To_{max} Prøvning i overensstemmelse med ISO 16750-4: Chapter 5.1.1.2: Funktionsprøve ved lav temperatur (24 timer ved – 40 °C) For denne prøve henvises til IEC 60068-2-1: Environmental testing — Part 2-1: Tests — Test A: Cold, IEC 68-2-2 prøve Bd, med en prøvningsvarighed på 96 timer ved temperaturer på ned til – 40 °C. Prøvning i overensstemmelse med ISO 16750-4: Chapter 5.1.2.2: Funktionsprøve ved høj temperatur (96 timer ved 135 °C) For denne prøve henvises til IEC 60068-2-2: Basic environmental testing procedures; part 2: tests; tests B: dry heat	213

▼B

Nr.	Prøve	Beskrivelse	Tilknyttede krav
4.2	Temperaturcyklusser	Prøvning i overensstemmelse med ISO 16750-4: Chapter 5.3.2: Rapid change of temperature with specified transition duration (– 40 °C/135 °C, 20 cyklusser, holdetid 30 min. ved hver temperatur) IEC 60068-2-14: Environmental testing; Part 2-14: Tests; Test N: Change of temperature	213
4.3	Fugtighedscyklusser	Funktionaliteten (som defineret i prøvning nr. 3.3) eftervises ved gennemgang af IEC 60068-2-30, prøve Db, seks 24-timers cyklusser, hvor hver temperatur varierer fra + 25 °C til + 55 °C.	214
4.4	Vibration	ISO 16750-3: Chapter 4.1.2.6: Test VI: Commercial vehicle, engine, gearbox Blandet vibrationsprøvning, inkl. a) sinusvibrationsprøvning, 20...520 Hz, 11,4 … 120 m/s^2, <= 0,5 okt./min b) Prøvning for tilfældige vibrationer, 10…2 000 Hz, kvadratisk middel 177 m/s^2 94 timer pr. akse, inkl. temperaturcyklus – 20…70 °C For denne prøve henvises til IEC 60068-2-80: Environmental testing — Part 2-80: Tests — Test Fi: Vibration — Mixed mode	219
4.5	Mekanisk stød	ISO 16750-3: Chapter 4.2.3: Test VI: Test for devices in or on the gearbox stød med halv-sinus, acceleration efter aftale inden for området 3 000…15 000 m/s^2, impulsvarighed efter aftale, dog < 1 ms, antal stød: efter aftale For denne prøve henvises til IEC 60068-2-27: Environmental testing. Part 2: Tests. Test Ea and guidance: Shock	219
4.6	Beskyttelse mod vand og fremmedlegemer	Prøvning i overensstemmelse med ISO 20653: Road vehicles — Degree of protection (IP code) — Protection of electrical equipment against foreign objects, water and access (Målværdi: IP 64)	220, 221
4.7	Beskyttelse mod omvendt polaritet	Det kontrolleres, at bevægelsesføleren kan modstå polvending af strømforsyningen	216
4.8	Kortslutningsbeskyttelse	Det kontrolleres, at ind- og udgangssignaler er beskyttet mod kortslutning til strømforsyningen og til stel	216

▼B

Nr.	Prøve	Beskrivelse	Tilknyttede krav
5.	**Elektromagnetisk kompatibilitet**		
5.1	Strålingsemission og følsomhed	Overensstemmelse med ECE-regulativ R10 påvises	218
5.2	Elektrostatisk udladning	Overensstemmelse med ISO 10605:2008 + Technical Corrigendum:2010 + AMD1:2014: +/– 4 kV for kontakt og +/– 8 kV for udladning i luften	218
5.3	Transient nedre ledningsoverførsel for datalinjerne	For 24V-udførelse: overensstemmelse med ISO 7637-2 og ECE-regulativ nr. 10, rev. 3: impuls 1a: Vs = – 450V, Ri = 50 ohm impuls 2a: Vs = + 37 V, Ri = 2 ohm impuls 2b: Vs = + 20V, Ri = 0,05 ohm impuls 3a: Vs = – 150V, Ri = 50 ohm impuls 3b: Vs = + 150V, Ri = 50 ohm impuls 4: Vs = – 16 V Va = – 12 V t6 = 100 ms impuls 5: Vs = + 120 V Ri = 2,2 ohm td = 250 ms For 12 V-udførelse: overensstemmelse med ISO 7637-1 og ECE-regulativ nr. 10, rev. 3: impuls 1: Vs = – 75V, Ri = 10 ohm impuls 2a: Vs = + 37 V, Ri = 2 ohm impuls 2b: Vs = + 10V, Ri = 0,05 ohm impuls 3a: Vs = – 112V, Ri = 50 ohm impuls 3b: Vs = + 75V, Ri = 50 ohm impuls 4: Vs = – 6 V Va = – 5 V t6 = 15 ms impuls 5: Vs = + 65 V Ri = 3 ohm td = 100 ms Impuls 5 skal kun afprøves for køretøjsenheder bestemt til montering i køretøjer uden ekstern fælles overbelastningsbeskyttelse For så vidt angår overbelastningsbeskyttelse henvises til ISO 16750-2, 4. udgave, afsnit 4.6.4.	218

4. FUNKTIONSPRØVER FOR TAKOGRAFKORT

Prøvning i overensstemmelse med dette afsnit 4,

nr. 5 »Protokolprøver«

nr. 6 »Kortstruktur« og

nr. 7 »Funktionsprøver«,

kan foretages af bedømmeren eller certificeringsmyndigheden under sikkerhedsattesteringen af chipmodulet i henhold til de fælleseuropæiske kriterier.

Prøvning nr. 2.3 og 4.2 er de samme. Disse er de mekaniske prøvninger af kombinationen kort og chipmodul. Hvis en af disse komponenter (kort eller chipmodul) ændres, er disse prøvninger nødvendige.

▼B

Nr.	Prøve	Beskrivelse	Tilknyttede krav
1.	**Administrativ undersøgelse**		
1.1	Dokumentation	Dokumentationens korrekthed	
2	**Kort**		
2.1	Tryk	Det kontrolleres, at alle faciliteter til beskyttelse samt synlige data er korrekt udskrevet på kortet og overensstemmende. [Designation] Bilag 1C, afsnit 4.1 »Synlige data«, 227) Forsiden skal indeholde: svarende til kortets art, ordet »Førerkort« eller »Kontrolkort« eller »Værkstedskort« eller »Virksomhedskort«, trykt med store bogstaver på de(t) officielle sprog i den medlemsstat, som har udstedt kortet. [Medlemsstatens navn] Bilag 1C, afsnit 4.1 »Synlige data«, 228) Forsiden skal indeholde: angivelse af navnet på den udstedende medlemsstat (valgfrit). [Mærke] Bilag 1C, afsnit 4.1 »Synlige data«, 229) Forsiden skal indeholde: den udstedende medlemsstats nationalitetsmærke, trykt med negativ skrift i et blåt rektangel og omgivet af 12 gule stjerner. [Fortegnelse] Bilag 1C, afsnit 4.1 »Synlige data«, 232) Bagsiden skal indeholde: en forklaring til de nummererede punkter på kortets forside [Farve] Bilag 1C, afsnit 4.1 »Synlige data«, 234) Takografkort skal være trykt med følgende dominerende baggrundsfarve: — førerkort: hvid — værkstedskort: rød — kontrolkort: blå — virksomhedskort: gul.	227 til 229, 232, 234 til 236

▼B

Nr.	Prøve	Beskrivelse	Tilknyttede krav
		[Sikkerhed] Bilag 1C, afsnit 4.1 »Synlige data«, 235) Takografkort skal have mindst følgende egenskaber til beskyttelse mod forfalskning og indgreb fra uvedkommende: — sikkerhedsbaggrund med fint slangeornament og regnbuetryk — mindst én tofarvet mikroprintlinje.	
		[Mærker] Bilag 1C, afsnit 4.1 »Synlige data«, 236) Medlemsstaterne kan tilføje farver eller mærker, f.eks. nationale symboler og sikkerhedsfeatures.	
		[Godkendelsesmærke] Takografkort skal indeholde et godkendelsesmærke. Godkendelsesmærket består af — et rektangel, i hvilket er anbragt bogstavet »e« efterfulgt af kodetallet eller kendingsbogstavet for det land, som har meddelt typegodkendelsen — et typegodkendelsesnummer, som svarer til nummeret i typegodkendelsesdokumentet for et takografkort, og som anbringes et sted i nærheden af rektanglet.	
2.2	Mekanisk prøvning	[Kortstørrelse] Takografkort skal overholde ISO/IEC 7810, Identification cards — Physical characteristics, [5] Dimensionering af kort [5.1] Kortstørrelse [5.1.1] Kortdimensioner og tolerancer korttype ID-1 Ubrugt kort	240, 243 ISO/IEC 7810
		[Kortkanter] Takografkort skal overholde ISO/IEC 7810, Identification cards — Physical characteristics, [5] Dimensionering af kort [5.1] Kortstørrelse [5.1.2] Kortkanter	

▼B

Nr.	Prøve	Beskrivelse	Tilknyttede krav
		[Kortopbygning] Takografkort skal overholde ISO/IEC 7810, Identification cards — Physical characteristics, [6] Kortopbygning	
		[Kortmaterialer] Takografkort skal overholde ISO/IEC 7810, Identification cards — Physical characteristics, [7] Kortmaterialer	
		[Bøjestivhed] Takografkort skal overholde ISO/IEC 7810, Identification cards — Physical characteristics, [8] Kortegenskaber [8.1] Bøjestivhed	
		[Toksicitet] Takografkort skal overholde ISO/IEC 7810, Identification cards — Physical characteristics, [8] Kortegenskaber [8.3] Toksicitet	
		[Modstandsdygtighed over for kemiske stoffer] Takografkort skal overholde ISO/IEC 7810, Identification cards — Physical characteristics, [8] Kortegenskaber [8.4] Modstandsdygtighed over for kemiske stoffer	
		[Kortstabilitet] Takografkort skal overholde ISO/IEC 7810, Identification cards — Physical characteristics, [8] Kortegenskaber [8.5] Kortets formbestandighed/krumning afhængigt af temperatur og fugtighed	

▼B

Nr.	Prøve	Beskrivelse	Tilknyttede krav
		[Lys] Takografkort skal overholde ISO/IEC 7810, Identification cards — Physical characteristics, [8] Kortegenskaber [8.6] Lys	
		[Holdbarhed] Bilag 1C, afsnit 4.4 »Miljømæssige og elektriske specifikationer«, 241) Takografkort skal kunne fungere korrekt i fem år, hvis de anvendes i overensstemmelse med de miljømæssige og elektriske specifikationer.	
		[Afrivningsstyrke] Takografkort skal overholde ISO/IEC 7810, Identification cards — Physical characteristics, [8] Kortegenskaber [8.8] Afrivningsstyrke	
		[Adhæsion eller blokering] Takografkort skal overholde ISO/IEC 7810, Identification cards — Physical characteristics, [8] Kortegenskaber [8.9] Adhæsion eller blokering	
		[Krumning] Takografkort skal overholde ISO/IEC 7810, Identification cards — Physical characteristics, [8] Kortegenskaber [8.11] Samlet kortkrumning	
		[Varmebestandighed] Takografkort skal overholde ISO/IEC 7810, Identification cards — Physical characteristics, [8] Kortegenskaber [8.12] Varmebestandighed	

▼B

Nr.	Prøve	Beskrivelse	Tilknyttede krav
		[Overfladeforvrængninger] Takografkort skal overholde ISO/IEC 7810, Identification cards — Physical characteristics, [8] Kortegenskaber [8.13] Overfladeforvrængninger	
		[Kontaminering] Takografkort skal overholde ISO/IEC 7810, Identification cards — Physical characteristics, [8] Kortegenskaber [8.14] Kontaminering og samspil blandt kortkomponenter	
2.3	Mekanisk prøvning med chipmodul indlejret	[Bøjning] Takografkort skal overholde ISO/IEC 7810:2003/Amd. 1:2009, Identification cards — Physical characteristics, Amendment 1: Criteria for cards containing integrated circuits [9.2] Dynamisk bøjespænding Samlet antal bøjningscyklusser: 4 000.	ISO/IEC 7810
		[Vridning] Takografkort skal overholde ISO/IEC 7810:2003/Amd. 1:2009, Identification cards — Physical characteristics, Amendment 1: Criteria for cards containing integrated circuits [9.3] Dynamisk vridningsspænding Samlet antal vridningscyklusser: 4 000.	
3	**Modul**		
3.1	Modul	Modulet består af chipindkapslingen og kontaktpladen. [Overfladeprofil] Takografkort skal overholde ISO/IEC 7816-1:2011, Identification cards — Integrated circuit cards — Part 1: Cards with contacts — Physical characteristics [4.2] Kontakters overfladeprofil	ISO/IEC 7816

▼B

Nr.	Prøve	Beskrivelse	Tilknyttede krav
		[Mekanisk styrke] Takografkort skal overholde ISO/IEC 7816-1:2011, Identification cards — Integrated circuit cards — Part 1: Cards with contacts — Physical characteristics [4.3] Mekanisk styrke (ved kort og kontakter)	
		[Elektrisk modstand] Takografkort skal overholde ISO/IEC 7816-1:2011, Identification cards — Integrated circuit cards — Part 1: Cards with contacts — Physical characteristics [4.4] Elektrisk modstand (ved kontakter)	
		[Dimensionering] Takografkort skal overholde ISO/IEC 7816-2:2007, Identification cards — Integrated circuit cards — Part 2: Cards with contacts — Dimension and location of the contacts [3] Dimensionering af kontakterne	
		[Placering] Takografkort skal overholde ISO/IEC 7816-2:2007, Identification cards — Integrated circuit cards — Part 2: Cards with contacts — Dimension and location of the contacts [4] Antal kontakter og deres placering I tilfælde af moduler med seks kontakter, indgår kontakt »C4« og »C8« ikke i denne prøvning.	
4	**Chip**		
4.1	Chip	[Arbejdstemperatur] Chippen i et takografkort skal fungere ved en omgivende temperatur i området mellem – 25 °C og + 85 °C.	241 til 244 ECE R10 ISO/IEC 7810 ISO/IEC 10373

▼B

Nr.	Prøve	Beskrivelse	Tilknyttede krav
		[Temperatur og fugtighed] Bilag 1C, afsnit 4.4 »Miljømæssige og elektriske specifikationer«, 241) Takografkort skal kunne fungere korrekt under alle de klimabetingelser, som normalt optræder på fællesskabets område, og som det mindste i temperaturområdet – 25 °C til + 70 °C med lejlighedsvise maksima på indtil + 85 °C, idet der ved »lejlighedsvis« forstås højst 4 timer ad gangen og højst 100 gange i løbet af kortets levetid. Takografkortene udsættes trinvist for følgende temperatur- og fugtighedsforhold i det givne tidsrum. Efter hvert trin afprøves takografkortenes elektriske funktionalitet. 1. Temperatur på – 20 °C i 2 timer. 2. Temperatur på +/–0 °C i 2 timer. 3. Temperatur på + 20 °C, 50 % RF, i 2 timer. 4. Temperatur på 50 °C, 50 % RF, i 2 timer. 5. Temperatur på 70 °C, 50 % RF, i 2 timer. Temperaturen øges periodisk til + 85 °C, 50 % RF, i 60 min. 6. Temperatur på 70 °C, 85 % RF, i 2 timer. Temperaturen øges periodisk til +85 °C, 85 % RF, i 30 min.	
		[Fugtighed] Bilag 1C, afsnit 4.4 »Miljømæssige og elektriske specifikationer«, 242) Takografkort skal fungere korrekt inden for fugtighedsintervallet 10 % — 90 %.	
		[Elektromagnetisk kompatibilitet — EMC] Bilag 1C, afsnit 4.4 »Miljømæssige og elektriske specifikationer«, 244 Under drift skal takografkort opfylde kravene i ECE R10 om elektromagnetisk kompatibilitet.	

▼B

Nr.	Prøve	Beskrivelse	Tilknyttede krav
		[Statisk elektricitet] Bilag 1C, afsnit 4.4 »Miljømæssige og elektriske specifikationer«, 244 Under drift skal takografkort være beskyttet mod elektrostatiske udladninger. Takografkort skal overholde ISO/IEC 7810:2003/Amd. 1:2009, Identification cards — Physical characteristics, Amendment 1: Criteria for cards containing integrated circuits [9.4] Statisk elektricitet [9.4.1] Kort med kontakt og integreret kredsløb Prøvespænding: 4 000 V	
		[Røntgen] Takografkort skal overholde ISO/IEC 7810:2003/Amd. 1:2009, Identification cards — Physical characteristics, Amendment 1: Criteria for cards containing integrated circuits [9.1] Røntgen	
		[Ultraviolet lys] ISO/IEC 10373-1:2006, Identification cards — Test methods — Part 1: General characteristics [5.11] Ultraviolet lys	
		[3-hjulsprøvning] Takografkort skal overholde ISO/IEC 10373-1:2006/Amd. 1:2012, Identification cards — Test methods — Part 1: General characteristics, Amendment 1 [5.22] Kort med integreret kreds — mekanisk styrke: 3-hjulsprøvning af kort med integreret kreds og kontakter	
		[Coating] Takografkort skal overholde 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

Nr.	Prøve	Beskrivelse	Tilknyttede krav
4.2	Mekanisk prøvning af chipmodul indlejret i kort-> samme som 2.3	[Bøjning] Takografkort skal overholde ISO/IEC 7810:2003/Amd. 1:2009, Identification cards — Physical characteristics, Amendment 1: Criteria for cards containing integrated circuits [9.2] Dynamisk bøjespænding Samlet antal bøjningscyklusser: 4 000.	ISO/IEC 7810
		[Vridning] Takografkort skal overholde ISO/IEC 7810:2003/Amd. 1:2009, Identification cards — Physical characteristics, Amendment 1: Criteria for cards containing integrated circuits [9.3] Dynamisk vridningsspænding Samlet antal vridningscyklusser: 4 000.	
5	**Protokolprøver**		
5.1	ATR	Kontroller, at ATR er overensstemmende	ISO/IEC 7816-3 TCS_14, TCS_17, TCS_18
5.2	T=0	Kontroller, at T = 0-protokollen er overensstemmende	ISO/IEC 7816-3 TCS_11, TCS_12, TCS_13, TCS_15
5.3	PTS	Kontroller, at PTS-kommandoen er overensstemmende, ved at sætte T = 1 fra T = 0.	ISO/IEC 7816-3 TCS_12, TCS_19, TCS_20, TCS_21
5.4	T=1	Kontroller, at T = 1-protokollen er overensstemmende	ISO/IEC 7816-3 TCS_11, TCS_13, TCS_16
6	**Kortets struktur**		
6.1		Kontroller, at kortets filstruktur er overensstemmende, ved at kontrollere for tilstedeværelse af påbudte filer i kortet og adgangsbetingelserne til dem	TCS_22 til TCS_28 TCS_140 til TCS_179
7	**Funktionsprøver**		
7.1	Normal behandling af data	Hver tilladt brug af hver kommando afprøves mindst én gang (f.eks. afprøves kommandoen UPDATE BINARY med CLA = '00', CLA = '0C' og med andre P1-, P2- og Lc-parametre). Kontroller, at operationerne faktisk er udført på kortet (f.eks. ved at læse den fil, kommandoen er udført på)	TCS_29 til TCS_139

▼B

Nr.	Prøve	Beskrivelse	Tilknyttede krav
7.2	Fejlmeddelelser	Hver fejlmeddelelse afprøves mindst én gang (som foreskrevet i tillæg 2) for hver kommando. Hver fælles fejl afprøves mindst én gang (bortset fra **'6400'** integritetsfejl, der kontrolleres som led i sikkerhedsattesteringen)	
7.3	Krypteringsprogram og standardiserede domæneparametre		CSM_48, CSM_50
8	**Tilpasning**		
8.1	Optisk tilpasning	Bilag 1C, afsnit 4.1 »Synlige data«, 230) Forsiden skal indeholde: oplysninger, der er specifikke for det udstedte kort.	230, 231, 235
		Bilag 1C, afsnit 4.1 »Synlige data«, 231) Forsiden skal indeholde: datoer i formatet »dd/mm/yyyy« eller »dd.mm.yyyy« (dag, måned, år).	
		Bilag 1C, afsnit 4.1 »Synlige data«, 235) Takografkort skal have mindst følgende egenskaber til beskyttelse mod forfalskning og indgreb fra uvedkommende: — i fotografiets område skal sikkerhedsbaggrund og fotografi overlappe.	

5. PRØVNING AF EKSTERNT GNSS-UDSTYR

Nr.	Prøve	Beskrivelse	Tilknyttede krav
1.	**Administrativ undersøgelse**		
1.1	Dokumentation	Dokumentationens korrekthed	
2.	**Visuel inspektion af eksternt GNSS-udstyr**		
2.1.	Overensstemmelse med dokumentationen		
2.2.	Identifikation/mærkning		224 til 226
2.3	Materialer		219 til 223
3.	**Funktionsprøver**		
3.1	Identifikationsdata for føler		98,99
3.2	Sammenkobling af eksternt GNSS-modul med køretøjsenhed		123, 205

▼B

Nr.	Prøve	Beskrivelse	Tilknyttede krav
3.3	GNSS-position		36, 37
3.4	Grænseflade for køretøjsenhed, hvis GNSS-modtageren er ekstern i forhold til køretøjsenheden		03
3.5	Krypteringsprogram og standardiserede domæneparametre		CSM_48, CSM_50
4.	**Miljøprøver**		
4.1	Temperatur	Funktionaliteten eftervises gennem: Prøvning i overensstemmelse med ISO 16750-4, Chapter 5.1.1.2: Funktionsprøve ved lav temperatur (72 timer ved – 20 °C) For denne prøve henvises til IEC 60068-2-1: Environmental testing — Part 2-1: Tests — Test A: Cold Test i overensstemmelse med ISO 16750-4: Chapter 5.1.2.2: High temperature operation test (72 timer ved 70 °C) For denne prøve henvises til IEC 60068-2-2: Basic environmental testing procedures; part 2: tests; tests B: dry heat Prøvning i overensstemmelse med ISO 16750-4: Chapter 5.3.2: Rapid change of temperature with specified transition duration (– 20 °C/70 °C, 20 cyklusser, holdetid 1 time ved hver temperatur) Et reduceret sæt prøvninger (af dem, som foreskrives i afsnit 3 af denne tabel) kan udføres ved den lave temperatur, den høje temperatur og med gennemgang af temperaturcyklusserne	213
4.2	Fugtighed	Det eftervises, at køretøjsenheden kan modstå en cyklisk fugtighedsprøve (varmeprøve) ved gennemgang af IEC 60068-2-30, prøve Db, seks 24 timers cyklusser, hvor hver temperatur varierer fra + 25 °C til + 5 °C, og hvor den relative fugtighed er 97 % ved + 25 °C og 93 % ved + 55 °C	214
4.3	Mekanisk masse	1. Sinusvibrationer. Det kontrolleres, at køretøjsenheden kan modstå sinusvibrationer med følgende egenskaber: Konstant skift mellem 5 og 11 Hz: Topværdi 10mm konstant acceleration mellem 11 og 300 Hz: 5g Prøvning for dette krav sker med IEC 60068-2-6, prøve Fc, med en mindste prøvningsvarighed på 3 × 12 timer (12 timer for hver akseretning) ISO 16750-3 kræver ikke en sinusvibrationsprøvning for enheder, der sidder i afkoblede førerhuse.	219

▼B

Nr.	Prøve	Beskrivelse	Tilknyttede krav
		2. Tilfældige vibrationer: Prøvning i overensstemmelse med ISO 16750-3: Chapter 4.1.2.8: Test VIII: Commercial vehicle, decoupled vehicle cab Prøvning for tilfældige vibrationer, 10…2 000 Hz, kvadratisk middel, lodret: 21,3 m/s^2, kvadratisk middel, langsgående: 11,8 m/s^2, kvadratisk middel, tværgående: 13,1 m/s^2, 3 akser, 32 timer pr. akse, herunder temperaturcyklus: – 20…70 °C. For denne prøve henvises til IEC 60068-2-64: Environmental testing — Part 2-64: Tests — Test Fh: Vibration, broadband random and guidance 3. Stød: mekanisk stød med 3g halv-sinus i overensstemmelse med ISO 16750. De ovenfor beskrevne prøvninger udføres på forskellige prøveeksemplarer af den afprøvede apparattype.	
4.4	Beskyttelse mod vand og fremmedlegemer	Prøvning i overensstemmelse med ISO 20653: Road vehicles — Degree of protection (IP code) — Protection of electrical equipment against foreign objects, water and access (no change in parameters)	220, 221
4.5	Overspændingsbeskyttelse	Det kontrolleres, at køretøjsenheden kan modstå en strømforsyning på: 24 V-udførelse: 34V ved + 40 °C 1 time 12 V-udførelse: 17 V ved + 40 °C 1 time (ISO 16750-2, punkt 4.3)	216
4.6	Beskyttelse mod omvendt polaritet	Det kontrolleres, at køretøjsenheden kan modstå polvending af strømforsyningen (ISO 16750-2, punkt 4.7)	216
4.7	Kortslutningsbeskyttelse	Det kontrolleres, at ind- og udgangssignaler er beskyttet mod kortslutning til strømforsyningen og til stel (ISO 16750-2, punkt 4.10)	216
5	**Prøver for elektromagnetisk kompatibilitet**		
5.1	Strålingsemission og følsomhed	Overensstemmelse med ECE-regulativ R10	218

▼B

Nr.	Prøve	Beskrivelse	Tilknyttede krav
5.2	Elektrostatisk udladning	Overensstemmelse med ISO 10605:2008 + Technical Corrigendum:2010 + AMD1:2014: +/– 4 kV for kontakt og +/– 8 kV for udladning i luften	218
5.3	Transient nedre ledningsoverførsel for strømforsyning	For 24V-udførelse: overensstemmelse med ISO 7637-2 og ECE-regulativ nr. 10, rev. 3: impuls 1a: Vs = – 450V, Ri = 50 ohm impuls 2a: Vs = + 37 V, Ri = 2 ohm impuls 2b: Vs = + 20V, Ri = 0,05 ohm impuls 3a: Vs = – 150V, Ri = 50 ohm impuls 3b: Vs = + 150V, Ri = 50 ohm impuls 4: Vs = – 16 V Va = – 12 V t6 = 100 ms impuls 5: Vs = + 120 V Ri = 2,2 ohm td = 250 ms For 12 V-udførelse: overensstemmelse med ISO 7637-1 og ECE-regulativ nr. 10, rev. 3: impuls 1: Vs = – 75V, Ri = 10 ohm impuls 2a: Vs = + 37 V, Ri = 2 ohm impuls 2b: Vs = + 10V, Ri = 0,05 ohm impuls 3a: Vs = – 112V, Ri = 50 ohm impuls 3b: Vs = + 75V, Ri = 50 ohm impuls 4: Vs = – 6 V Va = – 5 V t6 = 15 ms impuls 5: Vs = + 65 V Ri = 3 ohm td = 100 ms Impuls 5 skal kun afprøves for køretøjsenheder bestemt til montering i køretøjer uden ekstern fælles overbelastningsbeskyttelse For så vidt angår overbelastningsbeskyttelse henvises til ISO 16750-2, 4. udgave, afsnit 4.6.4.	218

6. PRØVNING AF FACILITETEN TIL FJERNKOMMUNIKATION

Nr.	Prøve	Beskrivelse	Tilknyttede krav
1.	**Administrativ undersøgelse**		
1.1	Dokumentation	Dokumentationens korrekthed	
2.	**Besigtigelse**		
2.1.	Overensstemmelse med dokumentationen		
2.2.	Identifikation/mærkning		225, 226
2.3	Materialer		219 til 223
4.	**Miljøprøver**		
4.1	Temperatur	Funktionaliteten eftervises gennem: Prøvning i overensstemmelse med ISO 16750-4, Chapter 5.1.1.2: Funktionsprøve ved lav temperatur (72 timer ved – 20 °C) For denne prøve henvises til IEC 60068-2-1: Environmental testing — Part 2-1: Tests — Test A: Cold	213

▼B

Nr.	Prøve	Beskrivelse	Tilknyttede krav
		Test i overensstemmelse med ISO 16750-4: Chapter 5.1.2.2: High temperature operation test (72 timer ved 70 °C) For denne prøve henvises til IEC 60068-2-2: Basic environmental testing procedures; part 2: tests; tests B: dry heat Prøvning i overensstemmelse med ISO 16750-4: Chapter 5.3.2: Rapid change of temperature with specified transition duration (– 20 °C/70 °C, 20 cyklusser, holdetid 1 time (?) ved hver temperatur) Et reduceret sæt prøvninger (af dem, som foreskrives i afsnit 3 af denne tabel) kan udføres ved den lave temperatur, den høje temperatur og med gennemgang af temperaturcyklusserne	
4.4	Beskyttelse mod vand og fremmedlegemer	Prøvning i overensstemmelse med ISO 20653: Road vehicles — Degree of protection (IP code) — Protection of electrical equipment against foreign objects, water and access (targeted value IP40)	220, 221
5	**Prøver for elektromagnetisk kompatibilitet**		
5.1	Strålingsemission og følsomhed	Overensstemmelse med ECE-regulativ R10	218
5.2	Elektrostatisk udladning	Overensstemmelse med ISO 10605:2008 + Technical Corrigendum:2010 + AMD1:2014: +/– 4 kV for kontakt og +/– 8 kV for udladning i luften	218
5.3	Transient nedre ledningsoverførsel for strømforsyning	For 24V-udførelse: overensstemmelse med ISO 7637-2 og ECE-regulativ nr. 10, rev. 3: impuls 1a: Vs = – 450V, Ri = 50 ohm impuls 2a: Vs = + 37 V, Ri = 2 ohm impuls 2b: Vs = + 20V, Ri = 0,05 ohm impuls 3a: Vs = – 150V, Ri = 50 ohm impuls 3b: Vs = + 150V, Ri = 50 ohm impuls 4: Vs = – 16 V Va = – 12 V t6 = 100 ms impuls 5: Vs = + 120 V Ri = 2,2 ohm td = 250 ms For 12 V-udførelse: overensstemmelse med ISO 7637-1 og ECE-regulativ nr. 10, rev. 3: impuls 1: Vs = – 75V, Ri = 10 ohm impuls 2a: Vs = + 37 V, Ri = 2 ohm impuls 2b: Vs = + 10V, Ri = 0,05 ohm impuls 3a: Vs = – 112V, Ri = 50 ohm impuls 3b: Vs = + 75V, Ri = 50 ohm impuls 4: Vs = – 6 V Va = – 5 V t6 = 15 ms impuls 5: Vs = + 65 V Ri = 3 ohm td = 100 ms Impuls 5 skal kun afprøves for køretøjsenheder bestemt til montering i køretøjer uden ekstern fælles overbelastningsbeskyttelse For så vidt angår overbelastningsbeskyttelse henvises til ISO 16750-2, 4. udgave, afsnit 4.6.4.	218

▼B

7. FUNKTIONSPRØVNING AF PAPIR

Nr.	Prøve	Beskrivelse	Tilknyttede krav
1.	**Administrativ undersøgelse**		
1.1	Dokumentation	Dokumentationens korrekthed	
2	**Generelle prøvninger**		
2.1	Antal tegn pr. linje	Visuel inspektion af udskrifter.	172
2.2	Mindste tegnstørrelse	Visuel inspektion af udskrift og tegn.	173
2.3	Understøttede tegnsæt	Printeren skal understøtte de tegnsæt, der er angivet i tillæg 1, kapitel 4 "Tegnsæt".	174
2.4	Udskrifters tydelighed	Kontrol af takografens typegodkendelse og visuel inspektion af udskrifter	174
2.5	Læsbarhed og identifikation af udskrifter	Inspektion af udskrifter Påvist gennem prøvningsrapporter og -protokoller fra fabrikanten. Alle typegodkendelsesnumre på takografer, som printerpapiret kan bruges sammen med, er påtrykt papiret.	175, 177, 178
2.6	Tilføjelse af håndskrevne noter	Visuel inspektion: Der findes et felt til førerens underskrift. Der findes felter til andre håndskrevne noter.	180
2.7	Yderligere oplysninger på papirudskrifter.	For- og bagsiden af papiret kan indeholde yderligere oplysninger. Disse yderligere oplysninger må ikke påvirke udskrifternes læsbarhed. Visuel inspektion.	177, 178
3	**Prøvning af holdbarhed ved opbevaring**		
3.1	Tør varme	Forkonditionering: 16 timer ved + 23 °C ± 2 °C/55 % ± 3 % relativ fugtighed Prøvningsmiljø: 72 timer ved + 70 °C ± 2 °C Genvinding: 16 timer ved + 23 °C ± 2 °C/55 % ±3 % relativ fugtighed	176, 178 IEC 60068-2-2-Bb
3.2	Fugtig varme	Forkonditionering: 16 timer ved + 23 °C ± 2 °C/55 % ± 3 % relativ fugtighed Prøvningsmiljø: 144 timer ved + 55 °C ± 2 °C og 93 % ±3 % relativ fugtighed Genvinding: 16 timer ved + 23 °C ± 2 °C/55 % ± 3 % relativ fugtighed	176, 178 IEC 60068-2-78-Cab

▼B

Nr.	Prøve	Beskrivelse	Tilknyttede krav
4	**Driftsprøvning af papir**		
4.1	Fugtighedsresistens, baggrund (blankt papir)	Forkonditionering: 16 timer ved + 23 °C ± 2 °C/55 % ± 3 % relativ fugtighed Prøvningsmiljø: 144 timer ved + 55 °C ± 2 °C og 93 % ± 3 % relativ fugtighed Genvinding: 16 timer ved + 23 °C ± 2 °C/55 % ± 3 % relativ fugtighed	176, 178 IEC 60068-2-78-Cab
4.2	Trykbarhed	Forkonditionering: 24 timer ved + 40 °C ± 2 °C/93 % ± 3 % relativ fugtighed Prøvningsmiljø: udskrift foretaget ved + 23 °C ± 2 °C Genvinding: 16 timer ved + 23 °C ± 2 °C/55 % ±3 % relativ fugtighed	176, 178
4.3	Varmebestandig-hed	Forkonditionering: 16 timer ved + 23 °C ± 2 °C/55 % ± 3 % relativ fugtighed Prøvningsmiljø: 2 timer ved +70 °C ± 2 °C, tør varme Genvinding: 16 timer ved + 23 °C ± 2 °C/55 % ± 3 % relativ fugtighed	176, 178 IEC 60068-2-2-Bb
4.4	Kuldebestandighed	Forkonditionering: 16 timer ved + 23 °C ± 2 °C/55 % ±3 % relativ fugtighed Prøvningsmiljø: 24 timer ved – 20 °C ± 3 °C, tør kulde Genvinding: 16 timer ved + 23 °C ± 2 °C/55 % ±3 % relativ fugtighed	176, 178 ISO 60068-2-1-Ab
4.5	Lysægthed	Forkonditionering: 16 timer ved + 23 °C ± 2 °C/55 % ± 3 % relativ fugtighed. Prøvningsmiljø: 100 timers belysning ved 5 000 lux og + 23 °C ± 2 °C/55 % ± 3 % relativ fugtighed 16 timer ved + 23 °C ± 2 °C/55 % ± 3 % relativ fugtighed	176, 178

Læsbarhedskriterier for prøvning 3.x og 4.x:

Udskriftens læsbarhed sikres, hvis den optiske tæthed ligger inden for følgende grænser:

Udskrevne tegn: min. 1,0

Baggrund (ubeskrevet papir): maks. 0,2

De frembragte udskrifters optiske tæthed skal måles i overensstemmelse med DIN EN ISO 534.

Udskrifterne må ikke udvise nogen dimensionsændringer og skal forblive klart læsbare.

8. INTEROPERABILITETSPRØVER

Nr.	Prøve	Beskrivelse
9.1 Interoperabilitetsprøver mellem køretøjsenheder og takografkort		
1	Gensidig ægthedsbekræftelse	Kontroller, at den gensidige ægthedsbekræftelse mellem køretøjs-enheden og takografkortet afvikles normalt

▼B

Nr.	Prøve	Beskrivelse
2	Skrive-/læseprøver	Gennemfør et typisk aktivitetsscenario på køretøjsenheden. Scenariet skal være tilpasset den afprøvede korttype og skal indebære skrivning på så mange af kortets elementærfiler som muligt Gennem dataoverførsel til køretøjsenheden kontrolleres det, at alle de tilsvarende registreringer er udført korrekt Gennem dataoverførsel fra kortet kontrolleres det, at alle de tilsvarende registreringer er udført korrekt Gennem daglige udskrifter kontrolleres det, at alle de tilsvarende registreringer kan læses korrekt.
	9.2 Interoperabilitetsprøver mellem køretøjsenheder og bevægelsesfølere	
1	Parring	Kontrollér, at parringen mellem køretøjsenheden og bevægelsesføleren afvikles normalt.
2	Aktivitetsprøvninger	Gennemfør et typisk aktivitetsscenario på bevægelsesføleren. Scenariet skal omfatte en normal aktivitet og frembringe så mange hændelser eller fejl som muligt. Gennem dataoverførsel til køretøjsenheden kontrolleres det, at alle de tilsvarende registreringer er udført korrekt Gennem dataoverførsel fra kortet kontrolleres det, at alle de tilsvarende registreringer er udført korrekt Gennem daglige udskrifter kontrolleres det, at alle de tilsvarende registreringer kan læses korrekt.
	9.3 Interoperabilitetsprøver mellem køretøjsenheder og eksternt GNSS-udstyr (hvor det er relevant)	
1	Gensidig ægthedsbekræftelse	Kontrollér, at den gensidige ægthedsbekræftelse mellem køretøjsenheden og det eksterne GNSS-modul afvikles normalt.
2	Aflæsning af registreringer	Gennemfør et typisk aktivitetsscenario på det eksterne GNSS-udstyr. Scenariet skal omfatte en normal aktivitet og frembringe så mange hændelser eller fejl som muligt Gennem dataoverførsel til køretøjsenheden kontrolleres det, at alle de tilsvarende registreringer udført korrekt. Gennem dataoverførsel fra kortet kontrolleres det, at alle de tilsvarende registreringer er udført korrekt Gennem daglige udskrifter kontrolleres det, at alle de tilsvarende registreringer kan læses korrekt

▼B

Tillæg 10

SIKKERHEDSKRAV

Dette tillæg beskriver it-sikkerhedsforskrifterne for det intelligente takografsystems komponenter (takograf af anden generation).

SEC_001 Følgende af det intelligente takografsystems komponenter skal sikkerhedsattesteres i overensstemmelse med de fælleseuropæiske kriterier:

— køretøjsenhed

— takografkort

— bevægelsesføler

— eksternt GNSS-udstyr.

SEC_002 De it-sikkerhedsforskrifter, der som minimum skal opfyldes af hver enkelt komponent, som skal sikkerhedsattesteres, skal fastlægges i en komponentsikringsprofil i overensstemmelse med de fælleseuropæiske kriterier.

SEC_003 Europa-Kommissionen skal sørge for, at følgende fire sikringsprofiler, som er i overensstemmelse med dette bilag, støttes, udvikles og godkendes af de statslige it-sikkerhedsattesteringsorganer, der er organiseret i den arbejdsgruppe om fælles fortolkning, som understøtter gensidig anerkendelse af attester inden for rammerne af SOGIS-MRA (den europæiske aftale om gensidig anerkendelse af it-sikkerhedsvurderingsattester), og at de registreres:

— sikringsprofil for køretøjsenhed

— sikringsprofil for takografkort

— sikringsprofil for bevægelsesføler

— sikringsprofil for eksternt GNSS-udstyr.

Sikringsprofilen for køretøjsenheden skal både anvendes i de tilfælde, hvor køretøjsenheden er beregnet til brug sammen med eksternt GNSS-udstyr, og i andre tilfælde. I førstnævnte tilfælde anføres sikkerhedsforskrifterne for det eksterne GNSS-udstyr i den dedikerede sikringsprofil.

SEC_004 For at opstille et sikkerhedsmål, som komponenterne kan sikkerhedsattesteres efter, skal komponentfabrikanterne efter behov udvikle og komplettere hensigtsmæssige komponentsikringsprofiler uden at ændre eller slette eksisterende risici, mål, proceduremæssige metoder eller forskrifter for sikkerhedsfunktioner.

SEC_005 I forbindelse med evalueringsprocessen skal det erklæres, at dette sikkerhedsmål i alle henseender stemmer overens med den tilsvarende sikringsprofil.

SEC_006 Sikkerhedsniveauet for hver sikringsprofil skal svare til EAL4 og de udvidede sikkerhedskomponenter ATE_DPT.2 og AVA_VAN.5.

▼B

Tillæg 11

FÆLLES SIKKERHEDSMEKANISMER

INDHOLDSFORTEGNELSE

PRÆAMBEL

DEL A TAKOGRAFSYSTEM AF FØRSTE GENERATION

1. INDLEDNING

1.1. Henvisninger

1.2. Notation og forkortelser

2. KRYPTOGRAFISKE SYSTEMER OG ALGORITMER

2.1. Kryptografiske systemer

2.2. Kryptografiske algoritmer

2.2.1 RSA-algoritme

2.2.2 Hash-algoritme

2.2.3 Algoritme til datakryptering

3. NØGLER OG CERTIFIKATER

3.1. Generering og distribution af nøgler

3.1.1 Generering og distribution af RSA-nøgler

3.1.2 RSA-prøvenøgler

3.1.3 Nøgler til bevægelsessensor

3.1.4 Generering og distribution af T-DES-sessionsnøgler

3.2. Nøgler

3.3. Certifikater

3.3.1 Certifikaters indhold

3.3.2 Udstedte certifikater

3.3.3 Verificering og udpakning af certifikater

4. MEKANISME TIL GENSIDIG ÆGTHEDSKONTROL

5. MEKANISMER TIL FORTROLIGHED, INTEGRITET OG ÆGTHEDSKONTROL VED DATAOVERFØRSEL PÅ KØRETØJSENHEDENS KORT

5.1. Sikker meddelelsesoverførsel

5.2. Håndtering af fejl ved sikker meddelelsesoverførsel

5.3. Algoritme til beregning af kryptografiske kontrolsummer

5.4. Algoritme til beregning af kryptogrammer til fortrolighedsdataobjekter

6. MEKANISMER TIL DIGITAL UNDERSKRIFT AF DATAOVERFØRSLER

6.1. Generering af underskrifter

▼B

6.2.	Verificering af underskrift
DEL B	TAKOGRAFSYSTEM AF ANDEN GENERATION
7.	INDLEDNING
7.1.	Henvisninger
7.2.	Notation og forkortelser
7.3.	Definitioner
8.	KRYPTOGRAFISKE SYSTEMER OG ALGORITMER
8.1.	Kryptografiske systemer
8.2.	Kryptografiske algoritmer
8.2.1	Symmetriske algoritmer
8.2.2	Asymmetriske algoritmer og standardiserede domæneparametre
8.2.3	Hash-algoritmer
8.2.4	Talrækker
9.	NØGLER OG CERTIFIKATER
9.1.	Asymmetriske nøglepar og certifikater for offentlige nøgler
9.1.1	Generelt
9.1.2	Europæisk niveau
9.1.3	Medlemsstatsniveau
9.1.4	Apparatniveau: Køretøjsenheder
9.1.5	Apparatniveau: Takografkort
9.1.6	Apparatniveau: Eksternt GNSS-udstyr
9.1.7	Oversigt: Udskiftning af certifikat
9.2.	Symmetriske nøgler
9.2.1	Nøgler til sikring af kommunikation mellem køretøjsenhed og bevægelsessensor
9.2.2	Nøgler til sikring af DSRC-kommunikation
9.3.	Certifikater
9.3.1	Generelt
9.3.2	Certifikaters indhold
9.3.3	Anmodning om certifikater
10.	GENSIDIG ÆGTHEDSKONTROL OG SIKKER MEDDELELSESOVERFØRSEL MELLEM KØRETØJSENHED OG KORT
10.1.	Generelt
10.2.	Gensidig certifikatkædeverificering
10.2.1	Kortcertifikatkædeverificering foretaget af køretøjsenheden

▼B

10.2.2 Kortcertifikatkædeverificering foretaget af kortet

10.3. Ægthedskontrol af køretøjsenhed

10.4. Ægthedskontrol af chip og overenstemmelseskontrol af sessionsnøgle

10.5. Sikker meddelelsesoverførsel

10.5.1 Generelt

10.5.2 Struktur af sikker meddelelse

10.5.3 Afbrydelse af en sikker meddelelsesoverførselssession

11. SAMMENKOBLING AF KØRETØJSENHED OG EKSTERNT GNSS-UDSTYR, GENSIDIG ÆGTHEDSKONTROL OG SIKKER MEDDELELSESOVERFØRSEL

11.1. Generelt

11.2. Sammenkobling af køretøjsenhed og eksternt GNSS-udstyr

11.3. Gensidig certifikatkædeverifikation

11.3.1 Generelt

11.3.2 Under sammenkobling af køretøjsenhed og EGF

11.3.3 Under normal drift

11.4. Ægthedskontrol af køretøjsenhed og chip samt sessionsnøgleoverensstemmelse

11.5. Sikker meddelelsesoverførsel

12. PARRING AF OG KOMMUNIKATION MELLEM KØRETØJSENHED OG BEVÆGELSESSENSOR

12.1. Generelt

12.2. Parring af køretøjsenhed og bevægelsessensor ved hjælp af forskellige nøglegenerationer

12.3. Parring af og kommunikation mellem køretøjsenhed og bevægelsessensor ved hjælp af AES

12.4. Parring af køretøjsenhed og bevægelsessensor til forskellige udstyrsgenerationer

13. SIKKERHED VED FJERNKOMMUNIKATION OVER DSRC

13.1. Generelt

13.2. Kryptering af takografindhold og MAC-generering

13.3. Verifikation og dekryptering af takografindhold

14. UNDERSKRIVELSE AF DATAOVERFØRSLER OG VERIFICERING AF UNDERSKRIFTER

14.1. Generelt

14.2. Generering af underskrifter

14.3. Verifikation af underskrift

▼B

PRÆAMBEL

Dette tillæg foreskriver de sikkerhedsmekanismer, som sikrer:

— gensidig ægthedskontrol mellem forskellige komponenter i det digitale takografsystem

— fortrolighed, integritet, ægthed og/eller uafviselighed af data overført mellem forskellige komponenter eller overført til eksterne lagringsmedier.

Dette tillæg består af to dele. I del A er sikkerhedsmekanismer for digitale takografsystemer af første generation (digitale takografer) defineret. I del B er sikkerhedsmekanismer for digitale takografsystemer af anden generation (intelligente takografer) defineret.

De mekanismer, der specificeres i del A i dette tillæg, finder anvendelse, hvis mindst en af takografsystemets komponenter, der anvendes ved en gensidig ægthedskontrol og/eller dataoverførselsproces, er af første generation.

De mekanismer, der specificeres i del B i dette tillæg, finder anvendelse, hvis begge takografsystemets komponenter, der anvendes ved en gensidig ægthedskontrol og/eller dataoverførselsprocessen, er af anden generation.

Tillæg 15 indeholder flere oplysninger om brugen af komponenter af første generation sammen med komponenter af anden generation.

DEL A

TAKOGRAFSYSTEM AF FØRSTE GENERATION

1. INDLEDNING

1.1. **Henvisninger**

I dette tillæg er følgende henvisninger anvendt:

SHA-1	National Institute of Standards and Technology (NIST). *FIPS Publication 180-1: Secure Hash Standard*. April 1995.
PKCS1	RSA Laboratories. PKCS # 1: *RSA Encryption Standard*. Version 2.0. October 1998.
TDES	National Institute of Standards og Technology (NIST). *FIPS Publication 46-3: Data Encryption Standard*. Draft 1999.
TDES-OP	ANSI X9.52, Triple Data Encryption Algorithm Modes of Operation. 1998.
ISO/IEC 7816-4	Information Technology — Identification cards — Integrated circuit(s) cards with contacts — Part 4: Interindustry commands for interexchange. First edition: 1995 + Amendment 1: 1997.
ISO/IEC 7816-6	Information Technology — Identification cards — Integrated circuit(s) cards with contacts — Part 6: Interindustry data elements. First edition: 1996 + Cor 1: 1998.
ISO/IEC 7816-8	Information Technology — Identification cards — Integrated circuit(s) cards with contacts — Part 8: Security related interindustry commands. First edition 1999.
ISO/IEC 9796-2	Information Technology — Security techniques — Digital signature schemes giving message recovery — Part 2: Mechanisms using a hash function. First edition: 1997.

▼B

ISO/IEC 9798-3	Information Technology — Security techniques — Entity authentication mechanisms — Part 3: Entity authentication using a public key algorithm. Second edition 1998.
ISO 16844-3	Road vehicles — Tachograph systems — Part 3: Motion sensor interface.

1.2. **Notation og forkortelser**

I dette tillæg bruges følgende notation og forkortelser:

(K_a, K_b, K_c)	Et nøglebundt til brug for den tredobbelte datakrypteringsalgoritme
CA	Certificeringsmyndighed
CAR	Henvisning til certificeringsmyndighed
CC	Kryptografisk kontrolsum
CG	Kryptogram
CH	Kommandoheader
CHA	Certifikatindehavers autorisation
CHR	Henvisning til certifikatindehaver
D()	Dekryptering med DES
DE	Dataelement
DO	Dataobjekt
d	Privat RSA-nøgle, privat eksponent
e	Offentlig RSA-nøgle, offentlig eksponent
E()	Kryptering med DES
EQT	Udstyr
Hash()	hash-værdi, et *Hash*-resultat
Hash	Hash-funktion
KID	Nøgle-identifikator
Km	TDES-nøgle. Hovednøgle defineret i ISO 16844-3
Km_{VU}	TDES-nøgle isat køretøjsenheder
Km_{WC}	TDES-nøgle isat værkstedskort
m	Repræsenterer en meddelelse, heltal mellem 0 og *n*-1
n	RSA-nøgler, modulus
PB	Udfyldningsbyte
Produktangivelse	Udfyldningsindikatorbyte (til brug i kryptogram til fortrolighedsdataobjekt)
PV	Ordinær dataværdi
s	Repræsenterer en underskrift, heltal mellem 0 og *n*-1
SSC	Sendesekvenstæller
SM	Sikker meddelelsesoverførsel
TCBC	TDEA-kryptografering med blokkædningsfunktion

▼B

TDEA	Algoritme til tredobbelt datakryptering
TLV	Mærkatlængde
VU	Køretøjsenhed
X.C	Certifikat for bruger X, udstedt af en certificeringsmyndighed
X.CA	Certificeringsmyndighed for bruger X
X.CA.PK $_{o}$ X.C	Operation, som består i at udpakke et certifikat for at udtrække en offentlig nøgle. Der er tale om en operator af infix-typen, der som venstre operand har certificeringsmyndighedens offentlige nøgle og som højre operand certifikatet udstedt af den pågældende certificeringsmyndighed. Resultatet er den offentlige nøgle for brugeren X, hvis certifikat er den højre operand
X.PK	Offentlig RSA-nøgle for bruger X
X.PK[I]	RSA-krypteringen af en vilkårlig oplysning I ved hjælp af den offentlige nøgle fra bruger X
X.SK	Privat RSA-nøgle for bruger X
X.SK[I]	RSA-kryptering af en vilkårlig oplysning I ved hjælp af den private nøgle fra bruger X
'xx'	Hexadecimal værdi
||	Sammenkædningsoperator

2. KRYPTOGRAFISKE SYSTEMER OG ALGORITMER

2.1. **Kryptografiske systemer**

CSM_001 Køretøjsenheder og takografkort skal anvende et kryptografisk system med en klassisk offentlig RSA-nøgle til at tilvejebringe følgende sikkerhedsmekanismer:

— ægthedskontrol mellem køretøjsenheder og kort

— transport af tredobbelte DES-sessionsnøgler mellem køretøjsenheder og takografkort

— digital underskrift af data, som er overført fra køretøjsenhederne eller fra takografkort til eksterne medier.

CSM_002 I køretøjsenheder og takografkort skal der anvendes et tredobbelt symmetrisk DES-kryptograferingssystem til sikring af dataintegritet under udveksling af brugerdata mellem køretøjsenheder og takografkort og til, i givet fald, at sikre fortroligheden af dataoverførsel mellem køretøjsenheder og takografkort.

2.2. **Kryptografiske algoritmer**

2.2.1 *RSA-algoritme*

CSM_003 RSA-algoritmen er fuldt defineret ved følgende relationer:

▼B

$$X.SK[m] = s = m^d \bmod n$$

$$X.PK[s] = m = s^e \bmod n$$

En mere fuldstændig beskrivelse af RSA-funktionen findes i henvisning [PKCS1]. Den offentlige eksponent, e, til RSA-beregninger er et heltal mellem 3 og n-1, som opfylder betingelsen gcd(e, lcm(p-1, q-1))=1.

2.2.2 *Hash-algoritme*

CSM_004 Mekanismerne til digital underskrift skal anvende SHA-1-hashalgoritmen som defineret i henvisning [SHA-1].

2.2.3 *Algoritme til datakryptering*

CSM_005 Der skal anvendes DES-baserede algoritmer i blokkædningsfunktionstilstand.

3. NØGLER OG CERTIFIKATER

3.1. **Generering og distribution af nøgler**

3.1.1 *Generering og distribution af RSA-nøgler*

CSM_006 RSA-nøgler skal genereres i tre funktionelle hierarkiske niveauer:

— europæisk niveau,

— medlemsstatsniveau

— apparatniveau.

CSM_007 På europæisk niveau skal der genereres et enkelt europæisk nøglepar (EUR.SK og EUR.PK). Den europæiske private nøgle skal anvendes til at certificere medlemsstaternes offentlige nøgler. Der skal føres registre over alle certificerede nøgler. Disse opgaver udføres af en europæisk certificeringsmyndighed under Europa-Kommissionens myndighed og ansvar.

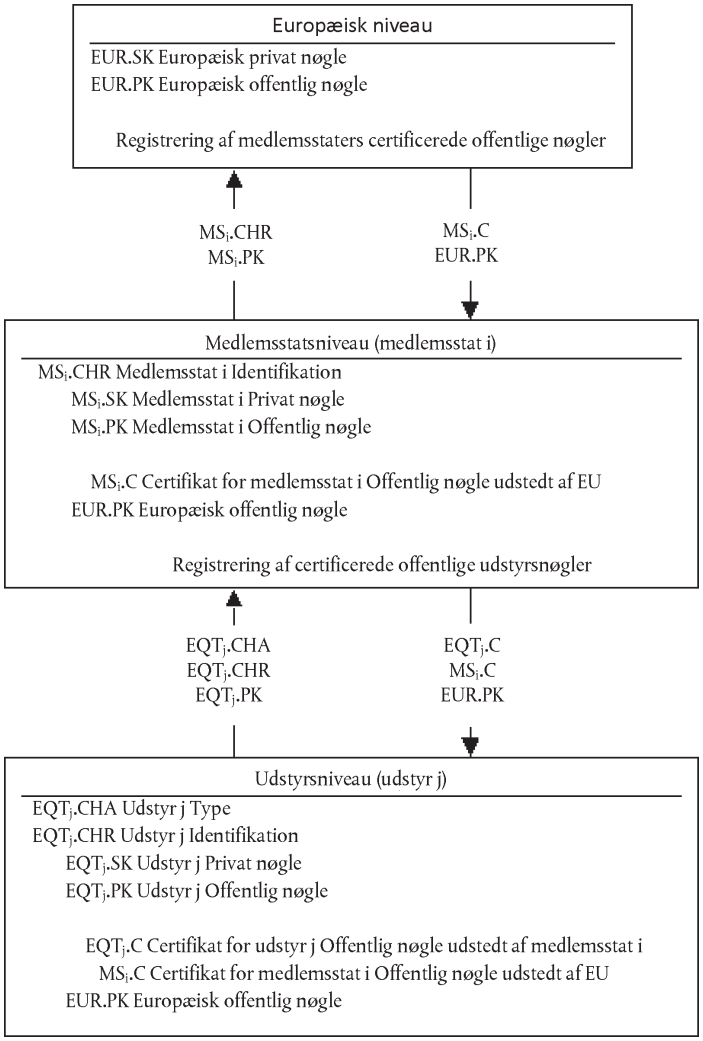
CSM_008 På medlemsstatsniveau skal der genereres et medlemsstatnøglepar (MS.SK og MS.PK). Medlemsstaternes offentlige nøgler skal være certificeret af den europæiske certificeringsmyndighed. Den private medlemsstatsnøgle anvendes til at certificere de offentlige nøgler, som skal isættes udstyret (køretøjsenhed eller takografkort). Der skal føres register over alle certificerede offentlige nøgler med identifikation af det udstyr, de er bestemt til. Disse opgaver varetages af en medlemsstats certificeringsmyndighed. En medlemsstat kan jævnligt ændre sit nøglepar.

CSM_009 På apparatniveau skal der genereres et enkelt nøglepar (EQT.SK og EQT.PK), som isættes hvert apparat. Apparatets offentlige nøgler skal certificeres af en medlemsstats certificeringsmyndighed. Disse opgaver kan varetages af udstyrsfabrikanter, leverandører af individuelle tilpasninger af udstyr eller medlemsstaternes myndigheder. Dette nøglepar anvendes til ægthedskontrol, digital underskrift og krypteringstjenester.

CSM_010 De private nøglers fortrolighed skal bibeholdes under generering, eventuel transport og opbevaring.

▼B

Følgende billede sammenfatter datastrømmen under denne proces:



3.1.2 *RSA-prøvenøgler*

CSM_011 Til afprøvning af udstyr (herunder interoperabilitetsprøvning) skal den europæiske certificeringsmyndighed generere et uens par europæiske prøvenøgler og mindst to par medlemsstatsprøvenøgler, af hvilke de offentlige nøgler skal certificeres med den europæiske private prøvenøgle. I det udstyr, som skal typegodkendes, skal fabrikanterne isætte prøvenøgler, som er certificeret med en af medlemsstaternes prøvenøgler.

3.1.3 *Nøgler til bevægelsessensor*

Generering, eventuel transport og opbevaring af de tre nedenfor beskrevne TDES-nøgler skal ske under iagttagelse af fuld fortrolighed.

For at understøtte takografkomponenter, som er i overensstemmelse med ISO 16844, skal den europæiske certificeringsmyndighed og medlemsstaternes certificeringsmyndigheder endvidere sikre følgende:

CSM_036 Den europæiske certificeringsmyndighed genererer KmVU og KmWC, to uafhængige og unikke tredobbelte DES-nøgler, og genererer Km som: $Km = Km_{VU} XOR Km_{WC}$.

Den europæiske certificeringsmyndighed fremsender disse nøgler under brug af tilbørligt sikrede procedurer til medlemsstaternes certificeringsmyndigheder på disses anmodning.

▼B

CSM_037 Medlemsstaternes certificeringsmyndigheder skal:

— Anvende Km til kryptering af bevægelsessensordata, som fabrikanter af bevægelsessensorer anmoder om (de data, som skal krypteres med Km, er fastlagt i ISO 16844-3)

— Fremsende Km_{VU} til fabrikanterne af køretøjsenheder under brug af behørigt sikrede procedurer til isætning i køretøjsenheder

— sørge for, at Km_{WC} isættes alle værkstedskort (`SensorInstallationSecData` i elementærfilen `Sensor_Installation_Data`) under personalisering af kortet.

3.1.4 *Generering og distribution af T-DES-sessionsnøgler*

CSM_012 Køretøjsenheder og takografkort skal som del af den gensidige ægthedskontrol generere og udveksle de nødvendige data til udarbejdelse af en tredobbelt fælles DES-sessionsnøgle. Denne dataudveksling skal være fortrolighedsbeskyttet ved RSA-kryptering.

CSM_013 Denne nøgle skal anvendes til alle efterfølgende kryptografiske operationer, hvor der anvendes sikker meddelelsesoverførsel. Dens gyldighed udløber ved sessionens afslutning (udtagning eller genindsætning af kort) og/eller efter 240 anvendelser (en anvendelse af nøglen = en kommando med sikker meddelelsesoverførsel sendt til kortet, samt det tilhørende svar).

3.2. **Nøgler**

CSM_014 RSA-nøgler (uanset niveau) skal have følgende længder: modulus *n* 1 024 bit, offentlig eksponent *e* højst 64 bit, privat eksponent *d* 1 024 bit.

CSM_015 Tredobbelte DES-nøgler har formen (K_a, K_b, K_a), hvor K_a og K_b er uafhængige nøgler med en længde på 64 bit. Der skal ikke sættes paritetsbit.

3.3. **Certifikater**

CSM_016 Certifikater med offentlig RSA-nøgle skal være »ikke-selvdeskriptive« og »verificerbare med kort« (ref.: ISO/IEC 7816-8) ISO/IEC 7816-8)

3.3.1 *Certifikaters indhold*

CSM_017 Certifikater med offentlig RSA-nøgle er opbygget med følgende data i følgende rækkefølge:

Data	Format	Byte	Bemærkning
CPI	INTEGER	1	Certifikatprofil-identifikator (‘01’ for denne version)
CAR	OCTET STRING	8	Henvisning til certificeringsmyndighed
CHA	OCTET STRING	7	Certifikatindehavers autorisation

▼B

Data	Format	Byte	Bemærkning
EOV	TimeReal	4	Certifikatets udløbsdato. Ikke obligatorisk, udfyldt med ‘FF’, hvis det ikke benyttes.
CHR	OCTET STRING	8	Henvisning til certifikatindehaver
n	OCTET STRING	128	Offentlig nøgle (modulus)
e	OCTET STRING	8	Offentlig nøgle (offentlig eksponent)
		164	

Bemærk:

1. »Certifikatprofil-identifikatoren« (CPI) beskriver den nøjagtige opbygning af et ægthedscertifikat. Den kan bruges som intern identifikator for udstyret i en relevant headerliste, som beskriver sammenkædningen af dataelementer i certifikatet.

   Den headerliste, der er knyttet til indholdet af dette certifikat, er som følger:

‘4D’	‘16’	‘5F 29’	‘01’	‘42’	‘08’	‘5F 4B’	‘07’	‘5F 24’	‘04’	‘5F 20’	‘08’	‘7F 49’	‘05’	‘81’	‘81 80’	‘82’	‘08’
Mærkat for udvidet headerliste	Længde af headerliste	CPI-mærkat	CPI-længde	CAR-mærkat	CAR-længde	CHA-mærkat	CHA-længde	EOV-mærkat	EOV-længde	CHR-mærkat	CHR-længde	Offentlig nøgle-mærkat (konstrueret)	Længde af efterfølgende dataobjekter	modulus-mærke	modulus-længde	offentlig eksponent-mærke	offentlig eksponent-længde

2. »Henvisning til certificeringsmyndighed« (CAR) har til formål at identificere den certifikatudstedende myndighed på en sådan måde, at dataelementet samtidig kan anvendes som identifikator for en myndigheds nøgle og henvise til certificeringsmyndighedens offentlige nøgle (vedrørende kodning henvises til nøgleidentifikatoren nedenfor).

3. »Certifikatindehavers autorisation« (CHA) anvendes til at identificere certifikatindehaverens rettigheder. Den indeholder fartskriverapplikationens ID og en angivelse af den type udstyr, som certifikatet er bestemt til (i henhold til dataelementet `EquipmentType`‘00’ for en medlemsstat).

▼B

4. 4. »Henvisning til certifikatindehaver« (CHR) har til formål at identificere certifikatindehaveren entydigt, således at dataelementet på en gang kan anvendes som identifikator for en persons nøgle og henvise til certifikatindehaverens offentlige nøgle.

5. Nøgleidentifikatorer identificerer entydigt certifikatindehaver eller certificeringsmyndighed. De kodes som følger:

5.1. Udstyr (køretøjsenhed eller kort):

Data	Udstyrets serienummer	Dato	Type	Fabrikant
Længde	4 byte	2 byte	1 byte	1 byte
Værdi	Heltal	mm yy binær decimalkode	Fabrikantspecifik	Fabrikantkode

For en køretøjsenhed kan producenten, når han anmoder om certifikater, være vidende eller uvidende om identifikationen af det udstyr, nøglerne vil blive isat.

I første tilfælde sender fabrikanten identifikationen af udstyret med den offentlige nøgle til den pågældende medlemsstats myndigheder til certificering. Certifikatet vil derefter indeholde identifikationen af udstyret, og fabrikanten skal sikre, at nøgler og certifikat isættes det udstyr, det er bestemt for. Nøgleidentifikatoren har den ovenfor viste form.

I sidstnævnte tilfælde skal fabrikanten entydigt identificere hver anmodning om certifikat og sende denne identifikation med den offentlige nøgle til den pågældende medlemsstats myndigheder til certificering. Certifikatet vil indeholde identifikationen af anmodningen. Fabrikanten skal melde tilbage til myndighederne i sin medlemsstat med tilordning af nøgle til udstyr (dvs. identifikation af anmodning om certifikat, identifikation af udstyr) efter installering af nøglen i udstyret. Nøgleidentifikatoren har følgende form:

Data	Serienummer på anmodning om certifikat	Dato	Type	Fabrikant
Længde	4 byte	2 byte	1 byte	1 byte
Værdi	Heltal	mm yy binær decimalkode	'FF'	Fabrikantkode

▼B

5.2. Certificeringsmyndighed:

Data	Identifikation af myndighed	Serienummer på nøgle	Yderligere oplysninger	Identifikator
Længde	4 byte	1 byte	2 byte	1 byte
Værdi	1 byte numerisk nation-kode 3 byte alfanumerisk nation-kode	Heltal	Tillægskode (CA-specifik) 'FF FF', hvis det ikke anvendes	'01'

Nøglens serienummer anvendes til at skelne mellem en medlemsstats forskellige nøgler, i tilfælde af at nøglen ændres.

6. Certifikatkontrollører skal implicit vide, at den certificerede offentlige nøgle er en RSA-nøgle, som er relevant for ægthedskontrol, verificering af digital underskrift og kryptering til fortrolighedstjenester (certifikatet indeholder ingen objektidentifikator til angivelse heraf).

3.3.2 *Udstedte certifikater*

CSM_018 Det udstedte certifikat er en digital underskrift med delvis genetablering af certifikatets indhold i overensstemmelse med ISO/IEC 9796-2, undtagen bilag A.4 dertil, med »henvisning til certificeringsmyndighed« vedhæftet.

$$X.C = X.CA.SK['6A' \parallel C_r \parallel \mathit{Hash}(Cc) \parallel 'BC'] \parallel C_n \parallel X.CAR$$

Med certifikatindhold = Cc = C_r || C_n

106 byte 58 byte

Bemærk:

1. Dette certifikat er 194 byte langt.

2. Henvisning til certificeringsmyndigheden (CAR), som er skjult af underskriften, er ligeledes vedhæftet underskriften, således at certificeringsmyndighedens offentlige nøgle kan vælges til verificering af certifikatet.

3. Certifikatkontrolløren skal implicit kende den algoritme, der af certificeringsmyndigheden er anvendt til at underskrive certifikatet.

4. Den headerliste, der er knyttet til dette udstedte certifikat, er som følger:

'7F 21'	'09'	'5F 37'	'81 80'	'5F 38'	'3A'	'42'	'08'
CV-certifikatmærkat (konstrueret)	Længde af efterfølgende dataobjekter	Underskrift-mærkat	Underskrift-længde	Rest-mærke	Rest-længde	CAR-mærkat	CAR-længde

▼B

3.3.3 *Verificering og udpakning af certifikater*

Certifikatverificering og -udpakning består i verificering af underskriften i overensstemmelse med ISO/IEC 9796-2, hentning af certifikatets indhold og den deri indeholdte offentlige nøgle: X.PK = X.CA.PK $_o$ X.C, og kontrol af certifikatets gyldighed.

CSM_019 Der indgår heri følgende trin:

Verificer underskrift og hent indhold:

— fra X.C hent Sign, C_n 'og CAR': X.C = Sign (128 byte) || C_n' (58 byte) || CAR' (8 byte)

— fra CAR' vælg korrekt offentlig nøgle for certificeringsmyndighed (hvis dette ikke er sket før på anden måde)

— åben Sign med certificeringsmyndighedens offentlige nøgle: Sr'= X.CA.PK [Sign],

— kontroller, at Sr' begynder med '6A' og ender på 'BC'

— beregn C_r' og H' af: Sr' = '6A' || C_r' (106 byte) || H' (20 byte) || 'BC'

— Hent indhold af certifikat C' = C_r' || C_n',

— kontroller, at *Hash*(C') = H'

Giver kontrollerne et tilfredsstillende resultat, er certifikatet ægte, dets indhold er C'.

Verificer gyldighed. Fra C':

— Kontroller i givet fald udløbsdatoen.

Hent og gem offentlig nøgle, nøgleidentifikator, certifikatindehavers autorisation og certifikatets udløbsdato fra C':

— X.PK = n || e

— X.KID = CHR

— X.CHA = CHA

— X.EOV = EOV

4. MEKANISME TIL GENSIDIG ÆGTHEDSKONTROL

Gensidig ægthedskontrol mellem kort og køretøjsenheder bygger på følgende princip:

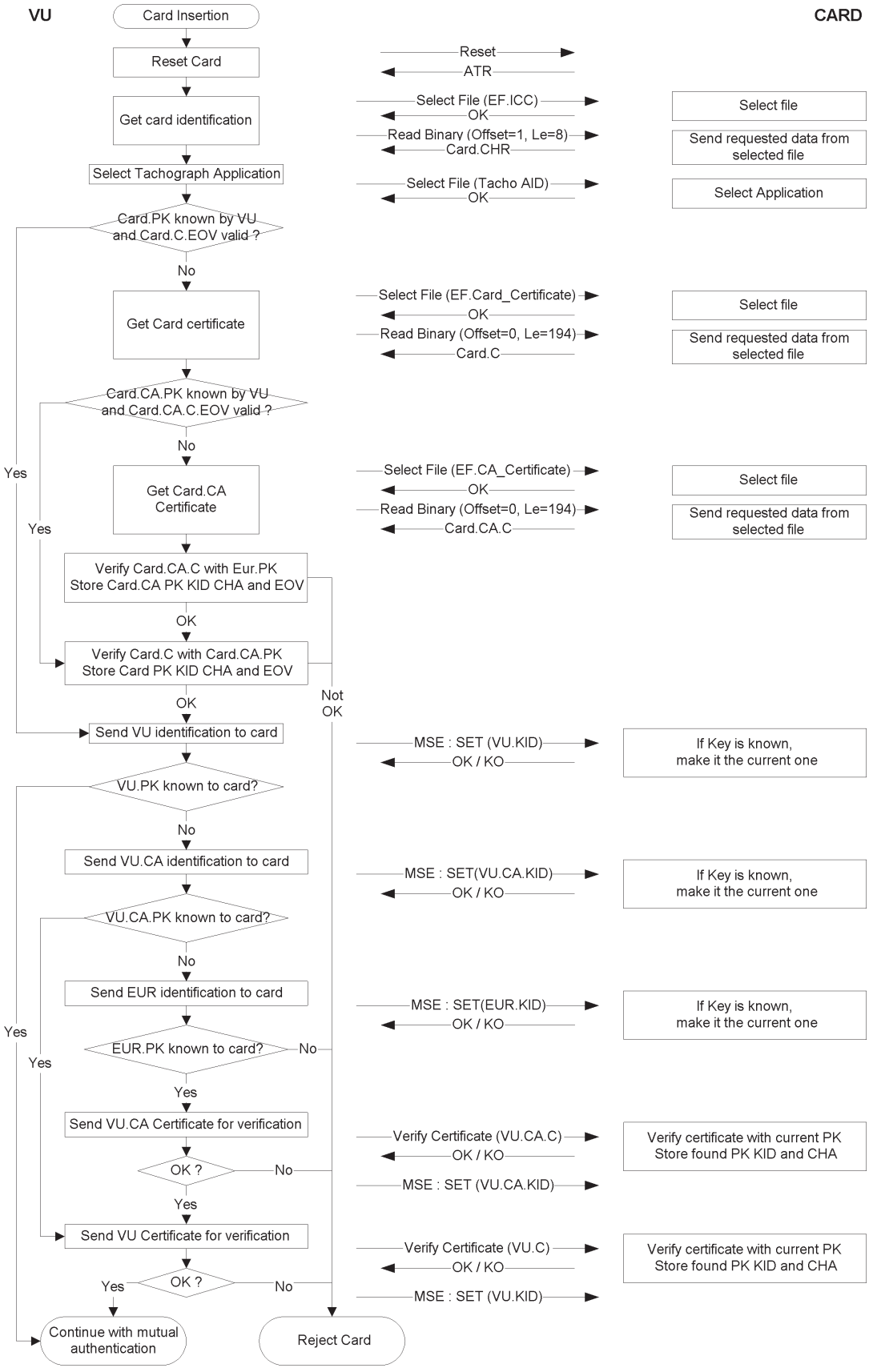
Hver part skal over for den anden godtgøre, at den er indehaver af en gyldig nøgle, hvis offentlige nøgle er certificeret af en af medlemsstaternes certificeringsmyndigheder, som selv er certificeret af den europæiske certificeringsmyndighed.

Dette sker ved, at der med den private nøgle underskrives et tilfældigt tal, afsendt af den anden part, som derefter skal genfinde det afsendte tilfældige tal ved verificering af denne underskrift.

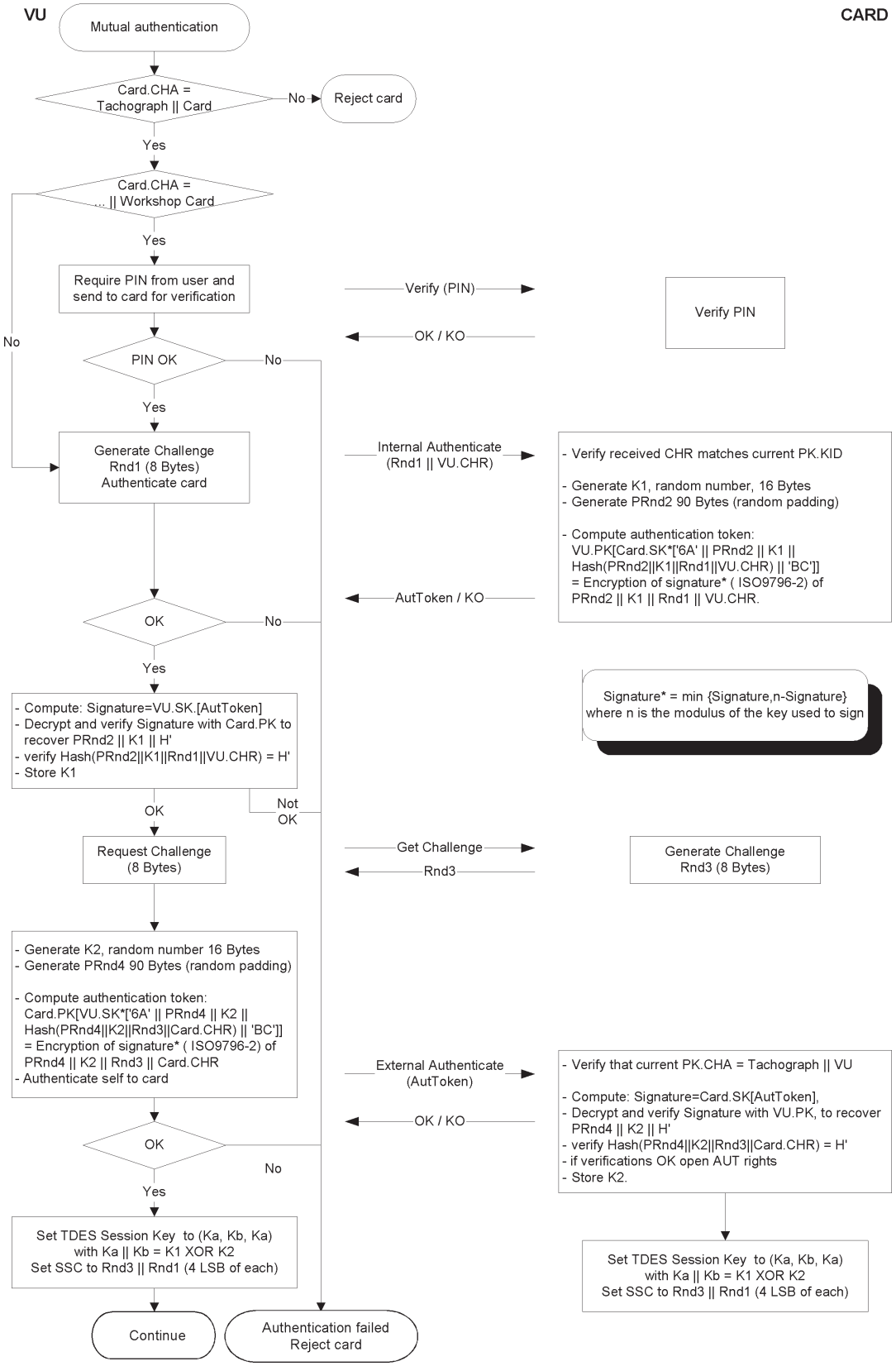
Mekanismen udløses af køretøjsenheden ved isætning af kortet. Den begynder med udveksling af certifikater og udpakning af offentlige nøgler og slutter med isætning af en sessionsnøgle.

▼B

CSM_020 Der skal anvendes følgende protokol (pilene angiver kommandoer og udvekslede data (se tillæg 2):



▼B


VU
CARD
Mutual authentication
Card.CHA = Tachograph || Card
No
Reject card
Yes
Card.CHA = ... || Workshop Card
Yes
Require PIN from user and send to card for verification
Verify (PIN)
Verify PIN
OK / KO
No
PIN OK
No
Yes
Generate Challenge Rnd1 (8 Bytes) Authenticate card
Internal Authenticate (Rnd1 || VU.CHR)
- Verify received CHR matches current PK.KID
- Generate K1, random number, 16 Bytes
- Generate PRnd2 90 Bytes (random padding)
- Compute authentication token: VU.PK[Card.SK*['6A' || PRnd2 || K1 || Hash(PRnd2||K1||Rnd1||VU.CHR) || 'BC']] = Encryption of signature* (ISO9796-2) of PRnd2 || K1 || Rnd1 || VU.CHR.
AutToken / KO
OK
No
Yes
Signature* = min {Signature,n-Signature} where n is the modulus of the key used to sign
- Compute: Signature=VU.SK.[AutToken]
- Decrypt and verify Signature with Card.PK to recover PRnd2 || K1 || H'
- verify Hash(PRnd2||K1||Rnd1||VU.CHR) = H'
- Store K1
OK
Not OK
Request Challenge (8 Bytes)
Get Challenge
Rnd3
Generate Challenge Rnd3 (8 Bytes)
- Generate K2, random number 16 Bytes
- Generate PRnd4 90 Bytes (random padding)
- Compute authentication token: Card.PK[VU.SK*['6A' || PRnd4 || K2 || Hash(PRnd4||K2||Rnd3||Card.CHR) || 'BC']] = Encryption of signature* (ISO9796-2) of PRnd4 || K2 || Rnd3 || Card.CHR
- Authenticate self to card
External Authenticate (AutToken)
- Verify that current PK.CHA = Tachograph || VU
- Compute: Signature=Card.SK[AutToken],
- Decrypt and verify Signature with VU.PK, to recover PRnd4 || K2 || H'
- verify Hash(PRnd4||K2||Rnd3||Card.CHR) = H'
- if verifications OK open AUT rights
- Store K2.
OK / KO
OK
No
Yes
Set TDES Session Key to (Ka, Kb, Ka) with Ka || Kb = K1 XOR K2 Set SSC to Rnd3 || Rnd1 (4 LSB of each)
Set TDES Session Key to (Ka, Kb, Ka) with Ka || Kb = K1 XOR K2 Set SSC to Rnd3 || Rnd1 (4 LSB of each)
Continue
Authentication failed Reject card

▼B

5. MEKANISMER TIL FORTROLIGHED, INTEGRITET OG ÆGTHEDSKONTROL VED DATAOVERFØRSEL PÅ KØRETØJS-ENHEDENS KORT

5.1. **Sikker meddelelsesoverførsel**

CSM_021 Ved overførsler af data på kort i køretøjsenheder skal dataintegriteten beskyttes gennem sikker meddelelsesoverførsel i overensstemmelse med henvisning [ISO/IEC 7816-4] og [ISO/IEC 7816-8].

CSM_022 Når der er behov for beskyttelse af data under overførsel, skal et dataobjekt med kryptografisk kontrolsum vedhæftes de dataobjekter, der udsendes inden for kommandoen eller svaret. Den kryptografiske kontrolsum skal verificeres af modtageren.

CSM_023 Den kryptografiske kontrolsum af data sendt inden for en kommando skal indeholde kommandoens header og alle de afsendte dataobjekter (= > CLA = '0C', og alle dataobjekter skal være indkapslet med mærkater, i hvilke b1 = 1).

CSM_024 Informationsbyte for svarstatus skal være beskyttet af en kryptografisk kontrolsum, når svaret ikke indeholder noget datafelt.

CSM_025 Kryptografiske kontrolsummer skal være 4 byte lange.

Kommandoer og svar har derfor følgende struktur ved brug af sikker meddelelsesoverførsel:

De anvendte dataobjekter er et delsæt af de dataobjekter for sikker meddelelsesoverførsel, som er beskrevet i ISO/IEC 7816-4:

Mærkat	Huskeværdi	Betydning
'81'	T_{PV}	Ordinær værdi af ikke BER-TLV-kodede data (skal beskyttes med kryptografisk kontrolsum)
'97'	**T_{LE}**	Værdien af Le i den ikke-sikrede kommando (skal beskyttes med kryptografisk kontrolsum)
'99'	T_{SW}	Status (skal beskyttes med kryptografisk kontrolsum)
'8E'	T_{CC}	Kryptografisk kontrolsum
'87'	$T_{PI\ CG}$	Byte med udfyldningsindikator || Kryptogram (ordinær værdi ikke kodet i BER-TLV)

▼B

Givet et ikke-sikret kommando/svar-par:

Kommandoheader				Kommandoindhold		
CLA	INS	P1	P2	[L_c-felt]	[Datafelt]	[L_e-felt]
Fire byte				L-byte, betegnet B_1 til B_L		

Svarindhold	Svarefterskrift	
[Datafelt]	SW1	SW2
L_r-databyte	To byte	

Det tilsvarende sikrede kommando/svar-par er:

Sikret kommando:

Kommandoheader (CH)				Kommandoindhold										
CLA	INS	P1	P2	[Nyt L_c-felt]	[Nyt datafelt]									[Nyt L_e-felt]
‘OC’				Længde af Nyt datafelt	T_{PV}	L_{PV}	PV	T_{LE}	L_{LE}	L_e	T_{CC}	L_{CC}	CC	‘00’
					‘81’	L_c	Datafelt	‘97’	‘01’	L_e	‘8E’	‘04’	CC	

Data, som skal integreres i kontrolsum = CH || PB || T_{PV} || L_{PV} || PV || T_{LE} || L_{LE} || L_e || PB

PB = Udfyldningsbyte (80 .. 00) i overensstemmelse med ISO-IEC 7816-4 og ISO 9797, metode 2.

Dataobjekterne PV og LE er kun til stede, når der er nogle tilsvarende data i den ikke-sikrede kommando.

Sikret svar:

1. Tilfælde, hvor svardatafeltet ikke er tomt og ikke behøver være fortrolighedsbeskyttet:

Svarindhold						Svarefterskrift
[Nyt datafelt]						ny SW1 SW2
T_{PV}	L_{PV}	PV	T_{CC}	L_{CC}	CC	
‘81’	L_r	Datafelt	‘8E’	‘04’	CC	

Data, der skal integreres i kontrolsum = T_{PV} || L_{PV} || PV || PB

2. Tilfælde, hvor svardatafeltet ikke er tomt og behøver være fortrolighedsbeskyttet:

▼B

Svarindhold						Svarefterskrift
[Nyt datafelt]						ny SW1 SW2
$T_{PI\ CG}$	$L_{PI\ CG}$	PI CG	T_{CC}	L_{CC}	CC	
'87'		PI ‖ CG	'8E'	'04'	CC	

Data, som skal bæres af CG: ikke-BER-TLV-kodede data og udfyldningsbyte.

Data, der skal integreres i kontrolsummen = $T_{PI\ CG}$ ‖ $L_{PI\ CG}$ ‖ PI CG ‖ PB

3. Tilfælde, hvor svardatafeltet er tomt:

Svarindhold						Svarefterskrift
[Nyt datafelt]						ny SW1 SW2
T_{SW}	L_{SW}	SW	T_{CC}	L_{CC}	CC	
'99'	'02'	Ny SW1 SW2	'8E'	'04'	CC	

Data, der skal integreres i kontrolsummen = T_{SW} ‖ L_{SW} ‖ SW ‖ PB

5.2. **Håndtering af fejl ved sikker meddelelsesoverførsel**

CSM_026 Når takografkortet konstaterer en fejl i fortolkningen af en kommando under sikker meddelelsesoverførsel, skal statusbytene returneres uden sikker meddelelsesoverførsel. I henhold til ISO/IEC 7816-4 er følgende statusbyte defineret til angivelse af fejl under sikker meddelelsesoverførsel:

'66 88': Verificering af kryptografisk kontrolsum mislykkedes

'69 87': Forventede dataobjekter i sikker meddelelsesoverførsel mangler

'69 88': Dataobjekter i sikker meddelelelsesoverførsel fejlbehæftede

CSM_027 Når takografkortet returnerer statusbyte uden dataobjekter for sikker meddelelsesoverførsel (SM) eller med et fejlbehæftet SM-dataobjekt, skal sessionen afbrydes af køretøjsenheden.

5.3. **Algoritme til beregning af kryptografiske kontrolsummer**

CSM_028 Kryptografiske kontrolsummer opbygget ved hjælp af en sædvanlig MAC i overensstemmelse med ANSI X9.19 med DES:

— Indledende trin: Den indledende kontrolblok y0 er E(Ka, SSC),

— Sekventielt trin: Kontrolblokkene y1, .., yn beregnes ved hjælp af Ka.

— Sluttrin: Den kryptografiske kontrolsum beregnes ved hjælp af den sidste kontrolblok yn på følgende måde: E(Ka, D(Kb, yn)).

hvor E() betyder kryptering med DES, og D() betyder dekryptering med DES.

De fire mest betydende byte i den kryptografiske kontrolsum overføres

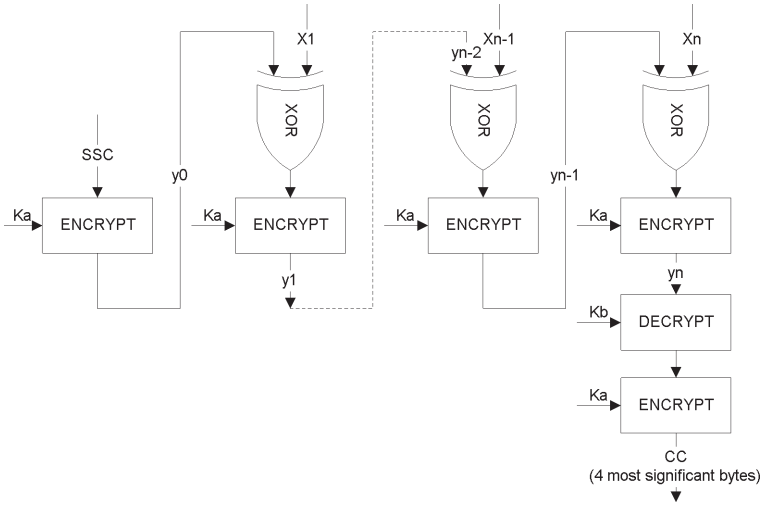
▼B

CSM_029 Sendesekvenstælleren (SSC) skal under kontrol af nøgleoverensstemmelse initialiseres med:

Startværdi af SSC: Rnd3 (fire mindst betydende byte) || Rnd1 (fire mindst betydende byte).

CSM_030 Sendesekvenstælleren skal hver gang forhøjes med 1 inden beregning af en MAC (dvs. SSC for den første kommando er startværdien af SSC + 1, SSC for det første svar er startværdien af SSC + 2).

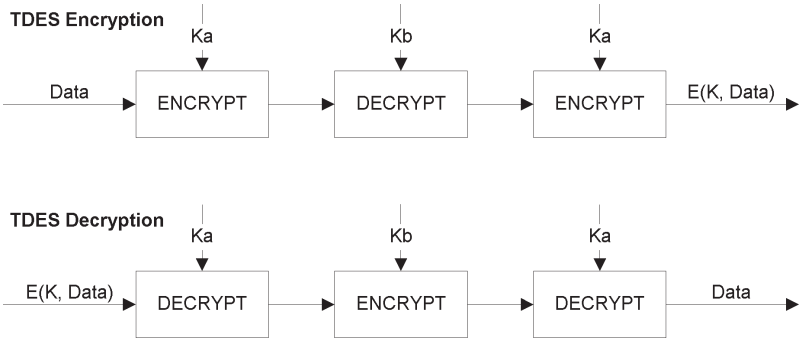
Følgende figur viser beregningen af MAC:



5.4. **Algoritme til beregning af kryptogrammer til fortrolighedsdataobjekter**

CSM_031 Kryptogrammer beregnes ved hjælp af TDEA i TCBC-funktionstilstand i overensstemmelse med henvisning [TDES] og [TDES-OP] og med nulvektoren som startværdiblok.

Følgende figur viser anvendelsen af nøgler i TDES:



▼B

6. MEKANISMER TIL DIGITAL UNDERSKRIFT AF DATAOVERFØRSLER

CSM_032 Det intelligente dedikerede udstyr (IDE) lagrer data, som er modtaget fra en enhed (køretøjsenhed eller kort) under en overførselssession, inden for en fysisk datafil. Denne fil skal indeholde certifikaterne MS_i.C og EQT.C. Filen indeholder digitale underskrifter af datablokke som foreskrevet i tillæg 7, Protokoller til dataoverførsel.

CSM_033 I digitale underskrifter af overførte data skal anvendes et digitalt underskriftssystem med appendiks, således at overførte data om ønsket kan læses uden dechifrering.

6.1. **Generering af underskrifter**

CSM_034 Ved generering af en dataunderskrift skal udstyret følge underskriftssystemet med appendiks som fastlagt i henvisning PKCS1 med SHA-1-hash-funktionen:

Underskrift = EQT.SK[‘00’ || ‘01’ || *PS* || ‘00’ || DER(SHA-1 (Data))]

PS = Udfyldningsstreng af oktetter, der har værdien ‘FF’, så længden er 128.

DER(SHA-1(*M*)) er kodningen af algoritme-ID'ens hash-værdi til en ASN.1-værdi af typen DigestInfo (distinguished encoding rules):

‘30’||‘21’||‘30’||‘09’||‘06’||‘05’||‘2B’||‘0E’||‘03’||‘02’||‘1A’||‘05’||‘00’||‘04’||‘14’||Hash-værdi.

6.2. **Verificering af underskrift**

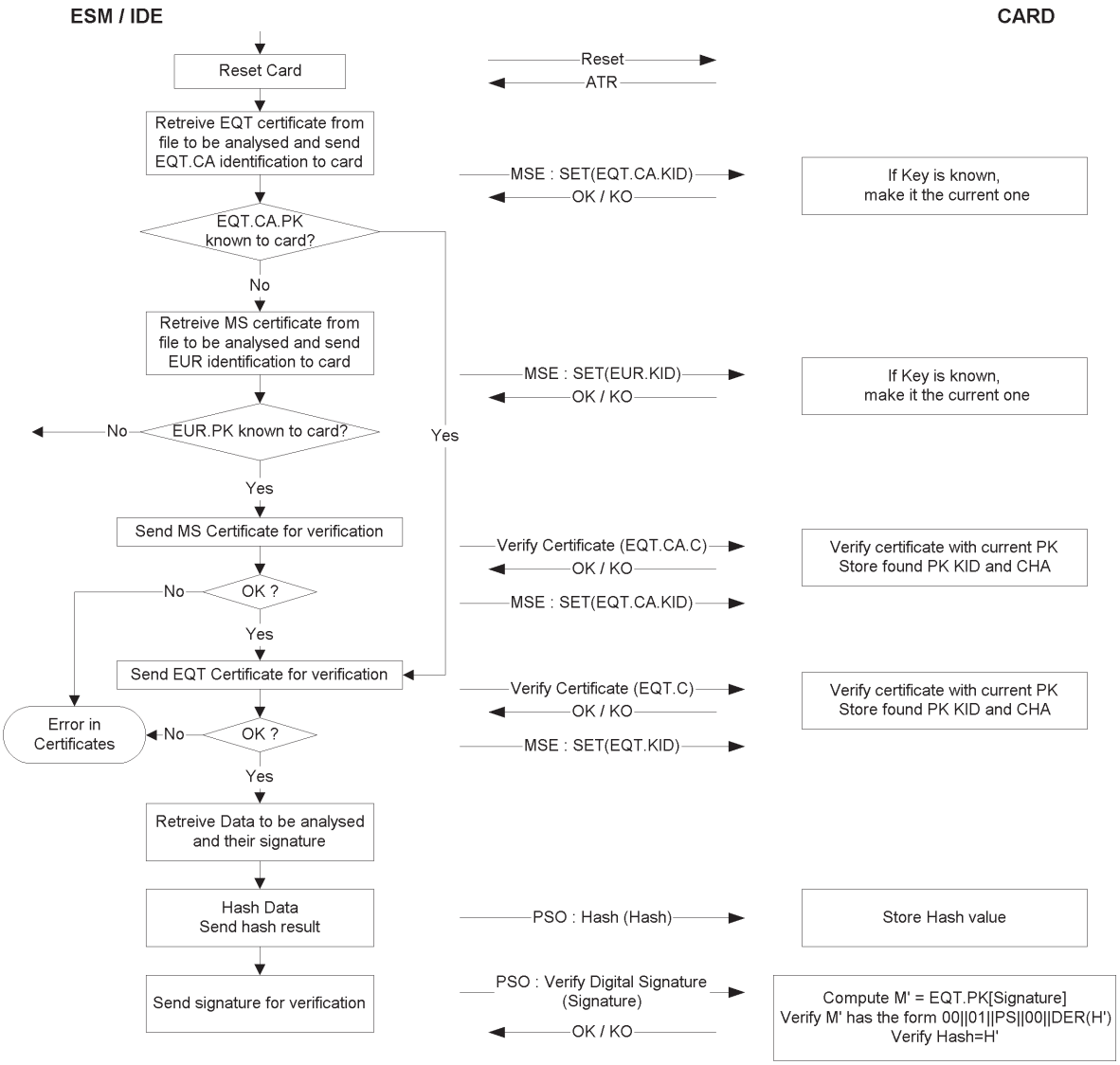
CSM_035 Ved verificering af dataunderskrift på overførte data skal udstyret følge underskriftssystemet med appendiks som defineret i henvisning [PKCS1] med SHA-1-hash-funktionen.

Den europæiske offentlige nøgle EUR.PK må uafhængigt (og betroet) kendes af kontrolløren.

Følgende tabel illustrerer den protokol, som en intelligent dedikeret enhed (IDE) med kontrolkort kan følge ved verificering af integriteten af data, som er overført og lagret på eksterne lagermedier. Kontrolkortet anvendes til at udføre dechifreringen af digitale underskrifter. Denne funktion behøver i dette tilfælde ikke være implementeret i det pågældende IDE.

Det udstyr, som har overført og underskrevet de data, der skal analyseres, benævnes EQT.

▼B



DEL B

TAKOGRAFSYSTEM AF ANDEN GENERATION

7. INDLEDNING

7.1. **Henvisninger**

Følgende henvisninger benyttes i denne del af dette tillæg.

AES	National Institute of Standards og 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), juli 2013
ISO 7816-4	ISO/IEC 7816-4, Identification cards — Integrated circuit cards — Part 4: Organization, security and commands for interchange. Third edition 2013-04-15
ISO 7816-8	ISO/IEC 7816-8, Identification cards — Integrated circuit cards — Part 8: Commands for security operations. Second edition 2004-06-01

▼B

ISO 8825-1	ISO/IEC 8825-1, Information technology — ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER). Fourth edition, 2008-12-15
ISO 9797-1	ISO/IEC 9797-1, Information technology — Security techniques — Message Authentication Codes (MACs) — Part 1: Mechanisms using a block cipher. Second edition, 2011-03-01
ISO 10116	ISO/IEC 10116, Information technology — Security techniques — Modes of operation of an *n*-bit block cipher. Third edition, 2006-02-01
ISO 16844-3	ISO/IEC 16844-3, Road vehicles — Tachograph systems — Part 3: Motion sensor interface. First edition 2004, including Technical Corrigendum 1 2006
RFC 5480	Elliptic Curve Cryptography Subject Public Key Information, marts 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), maj 2010
SHS	National Institute of Standards and Technology (NIST), FIPS PUB 180-4: Secure Hash Standard, marts 2012
SP 800-38B	National Institute of Standards and Technology (NIST), Special Publication 800-38B: Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication, 2005
TR-03111	BSI Technical Guideline TR-03111, Elliptic Curve Cryptography, version 2.00, 2012-06-28

7.2. **Notation og forkortelser**

I dette tillæg bruges følgende notation og forkortelser:

AES	Advanced Encryption Standard
CA	Certificeringsmyndighed
CAR	Henvisning til certificeringsmyndighed
CBC	Blokkædningsfunktion (funktionstilstand)
CH	Kommandoheader
CHA	Certifikatindehavers autorisation
CHR	Henvisning til certifikatindehaver
CV	Konstant vektor
DER	Distinguished Encoding Rules
DO	Dataobjekt
DSRC	Dedicated Short Range Communication
ECC	Elliptisk kurvekryptografi
ECDSA	Digital underskriftsalgoritme for elliptisk kurve
ECDH	Elliptisk kurve Diffie-Hellman (algoritme for nøgleoverensstemmelseskontrol)
EGF	Eksternt GNSS-udstyr
EQT	Udstyr

▼B

IDE	Intelligent dedikeret udstyr:
K_M	Hovednøgle for bevægelsessensor, der gør det muligt at parre en køretøjsenhed med en bevægelsessensor
K_{M-VU}	Nøgle isat køretøjsenheder, der giver en køretøjsenhed mulighed for at udlede hovednøglen til bevægelsessensoren, hvis der sættes et værkstedskort i køretøjsenheden
K_{M-WC}	Nøgle isat værkstedskort, der giver en køretøjsenhed mulighed for at udlede hovednøglen til bevægelsessensoren, hvis der sættes et værkstedskort i køretøjsenheden
MAC	Message Authentication Code
MoS	Bevægelsessensor
MSB	Mest betydende bit
PKI	Public key-infrastruktur
RCF	Fjernkommunikationsudstyr
SSC	Sendesekvenstæller
SM	Sikker meddelelsesoverførsel
TDES	Tredobbelt datakrypteringsstandard
TLV	Mærkatlængde
VU	Køretøjsenhed
X.C	offentligt nøglecertifikat for brugeren X
X.CA	certifikatmyndigheden, der har udstedt certifikatet for brugeren X
X.CAR	henvisning til certifikatmyndigheden, der er angivet i certifikatet for brugeren X
X.CHR	henvisning til certifikatindehaveren, der er angivet i certifikatet for brugeren X
X.PK	offentlig nøgle for brugeren X
X.SK	privat nøgle for brugeren X
$X.PK_{eph}$	midlertidig offentlig nøgle for brugeren X
$X.SK_{eph}$	midlertidig privat nøgle for brugeren X
'xx'	hexadecimal værdi
||	sammenkædningsoperator

7.3. **Definitioner**

Definitionerne af de begreber, der benyttes i dette tillæg, er medtaget i bilag 1C, afsnit I.

8. KRYPTOGRAFISKE SYSTEMER OG ALGORITMER

8.1. **Kryptografiske systemer**

CSM_38 Køretøjsenheder og takografkort skal anvende et elliptisk kurvebaseret kryptografisk system med en offentlig nøgle til at tilvejebringe følgende sikkerhedsmekanismer:

— gensidig ægthedskontrol mellem en køretøjsenhed og et kort

▼B

— kontrol af AES-sessionsnøglers overensstemmelse mellem en køretøjsenhed og et kort

— sikring af ægthed, integritet og uafviselighed af data, der er overført fra køretøjsenheder eller takografkort til eksterne medier.

CSM_39 Køretøjsenheder og eksternt GNSS-udstyr skal anvende et elliptisk kurvebaseret kryptografisk system med en offentlig nøgle til at tilvejebringe følgende sikkerhedsmekanismer:

— sammenkobling af en køretøjsenhed og eksternt GNSS-udstyr

— gensidig ægthedskontrol mellem en køretøjsenhed og eksternt GNSS-udstyr

— aftale om en AES-sessionsnøgle mellem en køretøjsenhed og eksternt GNSS-udstyr.

CSM_40 Køretøjsenheder og takografkort skal anvende et AES-baseret symmetrisk kryptografisk system med en offentlig nøgle til at tilvejebringe følgende sikkerhedsmekanismer:

— sikring af ægthed og integritet af data, der udveksles mellem en køretøjsenhed og et takografkort

— hvor det er relevant, sikring af fortrolighed af data udvekslet mellem en køretøjsenhed og et takografkort.

CSM_41 Køretøjsenheder og eksternt GNSS-udstyr skal anvende et AES-baseret symmetrisk kryptografisk system med en offentlig nøgle til at tilvejebringe følgende sikkerhedsmekanismer:

— sikring af ægthed og integritet af data udvekslet mellem en køretøjsenhed og eksternt GNSS-udstyr.

CSM_42 Køretøjsenheder og bevægelsessensorer skal anvende et AES-baseret symmetrisk kryptografisk system med en offentlig nøgle til at tilvejebringe følgende sikkerhedsmekanismer:

— parring af en køretøjsenhed og en bevægelsessensor

— gensidig ægthedskontrol mellem en køretøjsenhed og en bevægelsessensor

— sikring af fortrolighed af data udvekslet mellem en køretøjsenhed og en bevægelsessensor.

CSM_43 Køretøjsenheder og kontrolkort skal anvende et AES-baseret symmetrisk kryptografisk system med følgende sikkerhedsmekanismer på fjernkommunikationsinterfacet:

— sikring af fortrolighed, ægthed og integritet af data, der sendes fra en køretøjsenhed til et takografkort.

Bemærk:

— Data overføres egentlig fra en køretøjsenhed til en fjerninterrogator under kontrol af en kontrolførende ved hjælp af fjernkommunikationsudstyr, der kan være i eller uden for køretøjsenheden, se tillæg 14. Fjerninterrogatoren sender dog de modtagne data til

▼B

et kontrolkort til dekryptering og ægthedskontrol. Rent sikkerhedsmæssigt er fjernkommunikationsudstyret og fjerninterrogatoren helt gennemsigtige.

— Et værkstedskort giver samme sikkerhedsmekanismer til DSRC-interfacet som et kontrolkort. Derfor kan et værkstedskort kontrollere, at fjernkommunikationsinterfacet i en køretøjsenhed, herunder sikkerheden, fungerer korrekt. Der henvises til afsnit 9.2.2 for yderligere oplysninger.

8.2. **Kryptografiske algoritmer**

8.2.1 *Symmetriske algoritmer*

CSM_44 Køretøjsenheder, takografkort, bevægelsessensorer og eksterne GNSS-funktioner understøtter AES-algoritmen som defineret i [AES]; nøglelængder: 128, 192 og 256 bit.

8.2.2 *Asymmetriske algoritmer og standardiserede domæneparametre*

CSM_45 Køretøjsenheder, takografkort og eksterne GNSS-funktioner understøtter elliptisk kurvekryptografi, nøglestørrelse: 256, 384 og 512/521 bit.

CSM_46 Køretøjsenheder, takografkort og eksterne GNSS-funktioner understøtter ECDSA-underskriftsalgoritmen som specificeret i [DSS].

CSM_47 Køretøjsenheder, takografkort og eksterne GNSS-funktioner understøtter ECKA-EG-nøgleaftalealgoritmen som specificeret i [TR 03111].

CSM_48 Køretøjsenheder, takografkort og eksterne GNSS-funktioner understøtter alle standardiserede parametre som specificeret i nedenstående Tabel 1 for elliptisk kurvekryptografi.

Tabel 1

Standardiserede domæneparametre

Navn	Størrelse (bit)	Henvisning	Objektidentifikator
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

Bemærk: Objektidentifikatorerne i sidste kolonne i Tabel 1 er specificeret i [RFC 5639] for Brainpool-kurver og i [RFC 5480] for NIST-kurver

Eksempel 1: Objektidentifikatoren i BrainpoolP256r1-kurven er `{iso(1) identified-organization(3) teletrust(36) algorithm(3) signaturealgorithm(3) ecSign(2) ecStdCurvesAndGeneration (8) ellipticCurve(1) versionOne(1) 7}`.

eller i decimalangivelse: `1.3.36.3.3.2.8.1.1.7`.

Eksempel 2: Objektidentifikatoren for NIST P-384-kurven er `{iso(1) identified-organization(3) certicom(132) curve(0) 34}`.

eller i decimalangivelse: `1.3.132.0.34`.

8.2.3 *Hash-algoritmer*

CSM_49 Køretøjsenheder og takografkort understøtter SHA-256-, SHA-384- og SHA-512-algoritmerne i [SHS].

8.2.4 *Talrækker*

CSM_50 For en symmetrisk algoritme anvendes en asymmetrisk algoritme og/eller en hash-algoritme sammen som sikkerhedsprotokol, idet deres respektive nøglelængder og hashstørrelser er af (omtrent) samme styrke. Tabel 2 viser de tilladte talrækker:

Tabel 2

Tilladte talrækker

Talrække-ID	ECC-nøglestørrelse (bit)	AES-nøglelængde (bit)	Hash-altoritme	MAC-længde (byte)
CS#1	256	128	SHA-256	8
CS#2	384	192	SHA-384	12
CS#3	512/521	256	SHA-512	16

Bemærk: ECC-nøglestørrelser på 512 bit og 521 bit anses som værende af samme styrke i dette tillæg.

9. NØGLER OG CERTIFIKATER

9.1. **Asymmetriske nøglepar og certifikater for offentlige nøgler**

9.1.1 *Generelt*

Bemærk: De nøgler, der beskrives i dette afsnit, anvendes til gensidig ægthedskontrol og sikker meddelelsesoverførsel mellem køretøjsenheder og takografkort og mellem køretøjsenheder og eksterne GNSS-funktioner. Disse processer beskrives i detaljer i tillæggets kapitel 10 og 11.

CSM_51 I det europæiske digitale takografsystem genereres og forvaltes ECC-nøglepar og tilsvarende certifikater gennem tre hierarkiske funktionsniveauer:

— europæisk niveau

— medlemsstatsniveau

— apparatniveau.

▼B

CSM_52 I hele det europæiske intelligent takograf-system genereres, forvaltes og meddeles offentlige og private nøgler og certifikater under anvendelse af standardiserede, sikrede metoder.

9.1.2 *Europæisk niveau*

CSM_53 På europæisk niveau skal der genereres et enkelt europæisk nøglepar, der betegnes EUR. Det består af en privat nøgle (EUR.SK) og en offentlig nøgle (EUR.PK). Dette par udgør det basale nøglepar i hele PKI for den europæiske intelligente takograf. Opgaven udføres af en europæisk certificeringsmyndighed (ERCA) under Europa-Kommissionens myndighed og ansvar.

CSM_54 ERCA'en benytter den europæiske private nøgle til at underskrive et (selvunderskrevet) rodcertifikat for den europæiske offentlige nøgle og formidler dette europæiske rodcertifikat til alle medlemsstater.

CSM_55 ERCA'en benytter den europæiske private nøgle til at underskrive certifikaterne for medlemsstaternes offentlige nøgler, når den anmodes herom. ERCA'en fører registre over alle underskrevne nøglecertifikater tilhørende medlemsstaterne.

CSM_56 Som det fremgår af Figur 1 i afsnit 9.1.7 genererer ERCA'en et nyt europæisk rodnøglepar hvert 17. år. Hver gang ERCA'en genererer et nyt europæisk rodnøglepar, opretter den et nyt selvunderskrevet rodcertifikat for den nye europæiske offentlige nøgle. Gyldighedsperioden for et europæisk rodcertifikat er 34 år plus 3 måneder.

Bemærk: Indførelsen af et nyt rodnøglepar indebærer også, at ERCA vil generere en ny hovednøgle til bevægelsessensoren og en DSRC-hovednøgle, se afsnit 9.2.1.2 og 9.2.2.2.

CSM_57 Inden ERCA'en genererer et nyt europæisk rodnøglepar, foretager den en analyse af den kryptografiske styrke, der kræves for det nye nøglepar, eftersom det skal være sikkert i de næste 34 år. Om nødvendigt skal ERCA'en skifte til en talrække, der er stærkere end den nuværende, som specificeret i CSM_50.

CSM_58 Hver gang ERCA'en genererer et nyt europæisk rodnøglepar, opretter den et forbindelsescertifikat til den nye europæiske offentlige nøgle og underskriver det med den hidtidige europæiske private nøgle. Forbindelsescertifikatets gyldighedsperiode er 17 år. Dette fremgår ligeledes af Figur 1 i afsnit 9.1.7.

Bemærk: Eftersom et forbindelsescertifikat indeholder ERCA'ens offentlige nøgle af generation *X* og er underskrevet med ERCA'ens private nøgle af generation *X-1*, giver forbindelsescertifikatet mulighed for, at man gennem udstyr fremstillet under generation *X-1* også kan have tillid til udstyr fremstillet under generation *X*.

CSM_59 ERCA'en må ikke bruge den private nøgle for et rodnøglepar til noget formål efter det tidspunkt, hvor et nyt rodnøglecertifikat bliver gyldigt.

▼B

CSM_60 ERCA'en skal til enhver tid råde over følgende kryptografiske nøgler og certifikater:

— Det aktuelle EUR-nøglepar og det tilhørende certifikat

— Alle tidligere EUR-certifikater, der skal anvendes til verifikation af MSCA-certifikater, der stadig er gyldige

— Forbindelsescertifikater for alle generationer af EUR-certifikater undtagen den første.

9.1.3 *Medlemsstatsniveau*

CSM_61 På medlemsstatsniveau generer alle medlemsstater, der skal underskrive takografkortcertifikater, et eller flere entydige ECC-nøglepar, der betegnes et MSCA_Card. Alle medlemsstater, der skal underskrive certifikater til køretøjsenheder eller eksternt GNSS-udstyr, genererer desuden et eller flere andre entydige ECC-nøglepar, der betegnes MSCA_VU-EGF.

CSM_62 Opgaven med at generere medlemsstatens nøglepar varetages af en certificeringsmyndighed i medlemsstaten (MSCA). Når en MSCA genererer en medlemsstats nøglepar, sender den den offentlige nøgle til ERCA'en for at få et tilsvarende medlemsstatscertifikat underskrevet af ERCA'en.

CSM_63 En MSCA vælger styrken af en medlemsstats nøglepar, så den svarer til styrken af det europæiske rodnøglepar, der bruges til at underskrive den tilhørende medlemsstats certifikat.

CSM_64 Hvis der foreligger et MSCA_VU-EGF-nøglepar, består det af en privat nøgle, MSCA_VU-EGF.SK, og en offentlig nøgle, MSCA_VU-EGF.PK. En MSCA bruger udelukkende den private nøgle MSCA_VU-EGF.SK til at underskrive de offentlige nøglecertifikater for køretøjsenheder og eksternt GNSS-udstyr.

CSM_65 Et MSCA_Card-nøglepar består af den private nøgle MSCA_Card.SK og den offentlige nøgle MSCA_Card.PK. En MSCA benytter udelukkende den private nøgle MSCA_Card.SK til at underskrive de offentlige nøglecertifikater for takografkort.

CSM_66 En MSCA fører registre over alle underskrevne køretøjsenhedscertifikater, certifikater for ekstern GNSS-udstyr og kortcertifikater sammen med identifikation af det udstyr, som hvert certifikat er beregnet til.

CSM_67 Gyldighedsperioden for et MSCA_VU-EGF-certifikat er 17 år plus 3 måneder. Gyldighedsperioden for et MSCA_Card-certifikat er 7 år plus 1 måned.

CSM_68 Som det fremgår af Figur 1 i afsnit 9.1.7 skal den private nøgle for et MSCA_VU-EGF-nøglepar have en nøglebrugsperiode på to år.

▼B

CSM_69 En MSCA må ikke bruge den private nøgle for et MSCA_VU-EGF-nøglepar til noget formål, efter at dens brugstid er udløbet. En MSCA må heller ikke bruge den private nøgle i et MSCA_Card-nøglepar til andre formål, efter at dets brugstid er udløbet.

CSM_70 En MSCA skal til enhver tid råde over følgende kryptografiske nøgler og certifikater:

— Det aktuelle MSCA_Card-nøglepar og det tilhørende certifikat

— Alle tidligere MSCA_Card-certifikater, der skal anvendes til verifikation af certifikaterne for takografkort, der stadig er gyldige

— Det aktuelle EUR-certifikat, der skal anvendes til verifikation af det aktuelle MSCA-certifikat

— Alle tidligere EUR-certifikater, der skal anvendes til verifikation af alle MSCA-certifikater, der stadig er gyldige.

CSM_71 Hvis en MSCA skal underskrive certifikater for køretøjsenheder eller eksternt GNSS-udstyr, skal den endvidere råde over følgende nøgler og certifikater:

— Det aktuelle MSCA_VU-EGF-nøglepar og det tilhørende certifikat

— Alle tidligere MSCA_VU_EGF-certifikater, der skal anvendes til verifikation af certifikaterne for køretøjsenheder eller eksternt GNSS-udstyr, der stadig er gyldige.

9.1.4 *Apparatniveau: Køretøjsenheder*

CSM_72 Der skal genereres to entydige ECC-nøglepar for hver køretøjsenhed, som betegnes VU_MA og VU_Sign. Denne opgave varetages af køretøjsenhedsfabrikanterne. Når der genereres et køretøjsenhedsnøglepar, sender den part, der genererer nøglen den offentlige nøgle til MSCA'en i sit opholdsland for at få et tilhørende køretøjsenhedscertifikat underskrevet af MSCA'en. Den private nøgle må kun benyttes af køretøjsenheden.

CSM_73 VU_MA- og VU_Sign-certifikaterne for en givet køretøjsenhed skal have samme gyldighedsdato.

CSM_74 En fabrikant af en køretøjsenhed vælger styrken af et køretøjsenhedsnøglepar, så den svarer til styrken af det MSCA-nøglepar, der bruges til at underskrive det tilhørende køretøjsenhedscertifikat.

CSM_75 En køretøjsenhed må udelukkende benytte sit VU_MA-nøglepar, som består af en privat VU_MA.SK-nøgle og en offentlig VU_MA.PK-nøgle til at foretage ægthedskontrol af køretøjsenheden i forhold til takografkort og eksternt GNSS-udstyr, som specificeret i afsnit 10.3 og 11.4 i dette tillæg.

CSM_76 En køretøjsenhed skal kunne generere midlertidige ECC-nøglepar og må udelukkende bruge et midlertidigt nøglepar til at foretage kontrol af en sessionsnøgles overensstemmelse med et takografkort eller eksternt GNSS-udstyr, som specificeret i afsnit 10.4 og 11.4 i dette tillæg.

▼B

CSM_77 En køretøjsenhed må udelukkende anvende den private VU_Sign.SK-nøgle i sit VU_Sign-nøglepar til at underskrive overførte datafiler som specificeret i kapitel 14 i dette tillæg. Den tilhørende offentlige VU_Sign.PK-nøgle må udelukkende anvendes til at verificere underskrifter oprettet af køretøjsenheden.

CSM_78 Som vist i Figur 1 i afsnit 9.1.7 er gyldighedsperioden for et VU_MA-certifikat 15 år og 3 måneder. Gyldighedsperioden for et VU_Sign-certifikat er ligeledes 15 år og 3 måneder.

Bemærk:

— Den udvidede gyldighedsperiode for et VU_Sign-certifikat giver en køretøjsenhed mulighed for at oprette gyldige underskrifter over overførte data i de første tre måneder, efter at det er udløbet, jf. forordning (EU) nr. 581/2010.

— Den udvidede gyldighedsperiode for et VU_MA-certifikat er nødvendig for at give køretøjsenheden mulighed for at bekræfte ægtheden af et kontrolkort eller et virksomhedskort i løbet de første tre måneder, efter at det er udløbet, således at det er muligt at foretage dataoverførsel.

CSM_79 En køretøjsenhed må ikke bruge den private nøgle i et køretøjsenhedsnøglepar til noget formål, efter at det tilhørende certifikat er udløbet.

CSM_80 Køretøjsenhedsnøgleparrene (undtagen midlertidige nøglepar) og de tilhørende certifikater for en given køretøjsenhed må ikke erstattes eller fornys i marken, når først køretøjsenheden er taget i drift.

Bemærk:

— Midlertidige nøglepar er ikke medtaget i dette krav, eftersom en køretøjsenhed genererer et nyt midlertidigt nøglepar, hver gang der foretages ægthedskontrol af en chip og overensstemmelseskontrol af en sessionsnøgle, se afsnit 10.4. Bemærk, at midlertidige nøglepar ikke har tilhørende certifikater.

— Dette krav indeholder ikke forbud mod at erstatte statiske køretøjsenhedsnøglepar i forbindelse med en renovering eller reparation i et sikkert miljø under kontrol af fabrikanten af køretøjsenheden.

CSM_81 Når køretøjsenheder tages i drift, skal de indeholde følgende kryptografiske nøgler og certifikater:

— Den private VU_MA-nøgle med tilhørende certifikat

— Den private VU_Sign-nøgle med tilhørende certifikat

— MSCA_VU-EGF-certifikatet, der indeholder den offentlige MSCA_VU-EGF.PK-nøgle, der skal benyttes til verifikation af VU_MA-certifikatet og VU_Sign-certifikatet

▼B

— EUR-certifikatet, der indeholder den offentlige EUR.PK-nøgle, der skal benyttes til verifikation af MSCA_VU-EGF-certifikatet

— EUR-certifikatet, hvis gyldighedsperiode ligger umiddelbart forud for EUR-certifikatets gyldighedsperiode, som skal anvendes til at verificere MSCA_VU-EGF-certifikatet, hvis dette findes

— Forbindelsescertifikatet, der knytter disse to EUR-certifikater sammen, hvis dette findes.

CSM_82 Ud over de kryptografiske nøgler og certifikater, der står opført i CSM_81, skal køretøjsenhederne også indeholde de nøgler og certifikater, der specificeres i del A i dette tillæg, således at en køretøjsenhed kan interagere med takografkort af første generation.

9.1.5 *Apparatniveau: Takografkort*

CSM_83 Der genereres et entydigt ECC- nøglepar, som betegnes Card_MA, for hvert takografkort. Der genereres desuden endnu et entydigt ECC-nøglepar, som betegnes Card_Sign, for hvert førerkort og hvert værkstedskort. Denne opgave kan udføres af kortfabrikanter eller leverandører af individuelle tilpasninger af kort. Hver gang der genereres et kortnøglepar, skal den part, der genererer nøglen, sende den offentlige nøgle til MSCA'en i sit opholdsland for at få et tilhørende kortcertifikat underskrevet af MSCA'en. Den private nøgle må kun benyttes af takografkortet.

CSM_84 Card_MA- og Card_Sign-certifikaterne for et bestemt førerkort eller værkstedskort skal have samme gyldighedsdato.

CSM_85 En kortfabrikant eller en leverandør af individuelle tilpasninger af kort skal vælge styrken for et kortnøglepar, så den svarer til styrken af det MSCA-nøglepar, som anvendes til at underskrive det tilhørende kortcertifikat.

CSM_86 Et takografkort må udelukkende bruge sit Card_MA-nøglepar, som består af den private Card_MA.SK-nøgle og den offentlige Card_MA.PK-nøgle, til at foretage gensidig ægthedskontrol og kontrol af en sessionsnøgles overensstemmelse med køretøjsenheder som specificeret i afsnit 10.3 og 10.4 i dette tillæg.

CSM_87 Et førerkort eller værkstedskort må udelukkende bruge den private Card_Sign.SK-nøgle i sit Card_Sign-nøglepar til at underskrive overførte datafiler som specificeret i kapitel 14 i dette tillæg. Den tilhørende offentlige Card_Sign.PK-nøgle må udelukkende bruges til at verificere de underskrifter, som kortet opretter.

CSM_88 Et Card_MA-certifikat har følgende gyldighedsperiode:

— For førerkort: 5 år

— For virksomhedskort: 2 år

— For kontrolkort: 2 år

— For værkstedskort: Et år

▼B

CSM_89 Et Card_Sign-certifikat har følgende gyldighedsperiode:

— For førerkort: 5 år og 1 måned

— For værkstedskort: 1 år og 1 måned

Bemærk: Den udvidede gyldighedsperiode for et Card_Sign-certifikat giver et førerkort mulighed for at oprette gyldige underskrifter over overførte data i den første måned, efter at det er udløbet. Dette er nødvendigt i henhold til forordning (EU) nr. 581/2010, hvori det kræves, at en dataoverførsel fra et førerkort skal være mulig i op til 28 dage, efter at de seneste data er registreret.

CSM_90 Nøgleparrene og de tilhørende certifikater for et bestemt takografkort erstattes eller fornys ikke, når kortet er udstedt.

CSM_91 Når takografkort er udstedt, skal de indeholde følgende kryptografiske nøgler og certifikater:

— Den private Card_MA-nøgle med tilhørende certifikat

— For førerkort og værkstedskort desuden: den private Card_Sign-nøgle med tilhørende certifikat

— MSCA_Card-certifikatet, der indeholder den offentlige nøgle MSCA_Card.PK, der skal benyttes til verifikation af Card_MA-certifikatet og Card_Sign-certifikatet

— EUR-certifikatet, der indeholder den offentlige EUR.PK-nøgle, der skal benyttes til verifikation af MSCA_Card-certifikatet

— EUR-certifikatet, hvis gyldighedsperiode ligger umiddelbart forud for EUR-certifikatets gyldighedsperiode, som skal anvendes til at verificere MSCA_Card-certifikatet, hvis dette findes

— Forbindelsescertifikatet, der knytter disse to EUR-certifikater sammen, hvis dette findes.

CSM_92 Ud over de kryptografiske nøgler og certifikater, der står opført i CSM_91, skal takografkortene også indeholde de nøgler og certifikater, der specificeres i del A i dette tillæg, således at disse kort kan interagere med køretøjsenheder af første generation.

9.1.6 *Apparatniveau: Eksternt GNSS-udstyr*

CSM_93 Der genereres et entydigt ECC-nøglepar for hvert eksternt GNSS-udstyr, som betegnes EGF_MA. Denne opgave varetages af fabrikanter af eksternt GNSS-udstyr. Hver gang der genereres et EGF-MA-nøglepar, skal den offentlige nøgle sendes til MSCA'en i opholdslandet for at få et tilhørende EGF_MA-certifikat underskrevet af MSCA'en. Den private nøgle må kun benyttes af det eksterne GNSS-udstyr.

CSM_94 En EGF-fabrikant vælger styrken af et EGF_MA-nøglepar, så den svarer til styrken af det MSCA-nøglepar, der bruges til at underskrive det tilhørende EGF_MA-certifikat.

▼B

CSM_95 Eksternt GNSS-udstyr må udelukkende bruge sit EGF_MA-nøglepar, som består af den private nøgle EGF_MA.SK og den offentlige nøgle EGF_MA.PK til at foretage gensidig ægthedskontrol og kontrol af en sessionsnøgles overensstemmelse med køretøjsenheder som specificeret i afsnit 11.4 og 11.4 i dette tillæg.

CSM_96 EGF_MA-certifikatets gyldighedsperiode er 15 år.

CSM_97 Eksternt GNSS-udstyr må ikke bruge den private nøgle i et EGF_MA-nøglepar til opkobling til en køretøjsenhed, efter at det tilhørende certifikat er udløbet.

Bemærk: Som forklaret i afsnit 11.3.3 kan en EGF eventuelt bruge sin private nøgle til gensidig ægthedskontrol over for den køretøjsenhed, som den allerede er koblet op til, selv efter at det tilhørende certifikat er udløbet.

CSM_98 EGF_MA-nøgleparret og det tilhørende certifikat for givent eksternt GNSS-udstyr må ikke erstattes eller fornys i marken, når først EGF'en er taget i drift.

Bemærk: Dette krav indeholder ikke forbud mod at erstatte EGF-nøglepar i forbindelse med en renovering eller reparation i et sikkert miljø under kontrol af EGF-fabrikanten.

CSM_99 Når det eksterne GNSS-udstyr tages i drift, skal den indeholde følgende kryptografiske nøgler og certifikater:

— Den private EGF_MA-nøgle og tilhørende certifikat

— MSCA_VU-EGF-certifikatet, der indeholder den offentlige nøgle MSCA_VU-EUR.PK, der skal benyttes til verifikation af EGF_MA-certifikatet

— EUR-certifikatet, der indeholder den offentlige EUR.PK-nøgle, der skal benyttes til verifikation af MSCA_VU-EGF-certifikatet

— EUR-certifikatet, hvis gyldighedsperiode ligger umiddelbart forud for EUR-certifikatets gyldighedsperiode, som skal anvendes til at verificere MSCA_VU-EGF-certifikatet, hvis dette findes

— Forbindelsescertifikatet, der knytter disse to EUR-certifikater sammen, hvis dette findes.

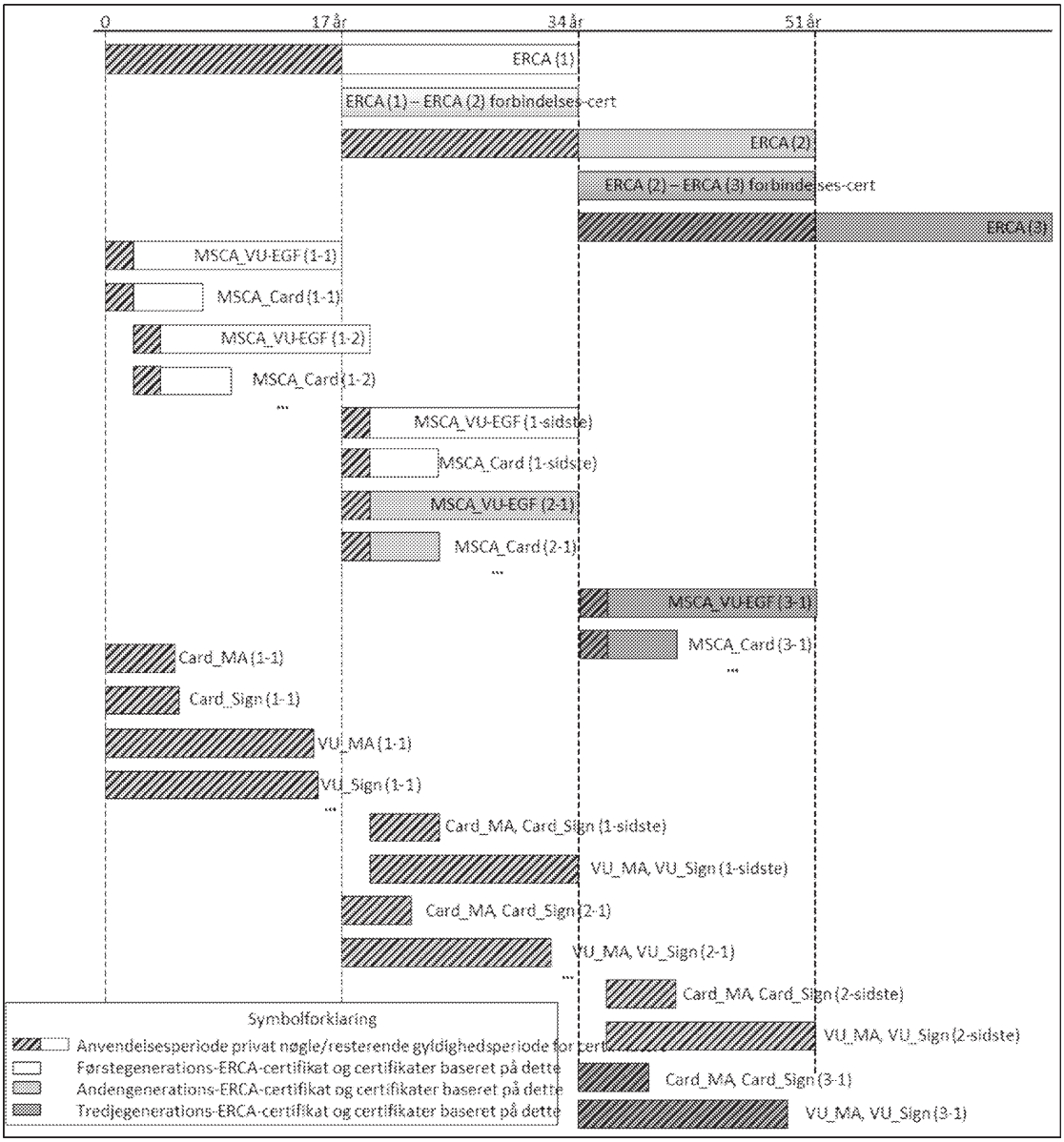
9.1.7 *Oversigt: Udskiftning af certifikat*

Figur 1 herunder viser, hvordan forskellige generationer af ERCA-rodcertifikater, ERCA-forbindelsescertifikater, MSCA-certifikater og udstyrscertifikater (køretøjsenhed og kort) udstedes og anvendes:

▼B

Figur 1

Udstedelse og brug af forskellige generationer af ERCA-rodcertifikater, ERCA-forbindelsescertifikater, MSCA-certifikater og udstyrscertifikater



Bemærkninger til Figur 1:

1. Forskellige generationer af rodcertifikatet angives med et tal i parentes. ERCA (1) er f.eks. første generation af ERCA-rodcertifikatet, ERCA (2) er anden generation osv.

2. Andre certifikater angives med to tal i parentes, hvoraf det første angiver generationen af rodcertifikat, under hvilken de er udstedt, det andet generationen for selve certifikatet. MSCA_Card (1-1) er f.eks. det første MSCA_Card-certifikat udstedt under ERCA (1), MSCA_Card (2-1) er det første MSCA_Card-certifikat udstedt under ERCA (2), MSCA_Card (2-last) er det sidste MSCA_Card-certifikat udstedt under ERCA (2), Card_MA(2-1) er det første kortcertifikat til gensidig ægthedskontrol, der er udstedt under ERCA (2) osv.

▼B

3. Certifikaterne MSCA_Card (2-1) og MSCA_Card (1-last) udstedes på næsten samme dato, men ikke præcis den samme. MSCA_Card (2-1) er det første MSCA_Card-certifikat udstedt under ERCA (2) og vil blive udstedt en smule senere end MSCA_Card (1-last), det sidste MSCA_Card-certifikat under ERCA (1).

4. Som det fremgår af figuren, kommer de første køretøjsenheds- og kortcertifikater udstedt under ERCA (2) næsten to år inden, de sidste køretøjsenheds- og kortcertifikater udstedt under ERCA (1) kommer frem. Dette skyldes, at køretøjsenheds- og kortcertifikater udstedes under et MSCA-certifikat og ikke direkte under ERCA-certifikatet. MSCA (2-1)-certifikatet vil blive udstedt umiddelbart efter, at ERCA (2) bliver gyldigt, men MSCA (1-last)-certifikatet udstedes kun ganske kort tid inden dette tidspunkt, nemlig lige inden ERCA (1)-certifikatet udløber. Derfor vil disse to MSCA-certifikater have næsten samme gyldighedsperiode, selv om de kommer fra forskellige generationer.

5. Den viste gyldighedsperiode for kort gælder for førerkort (5 år).

6. Af pladshensyn vises forskellen i gyldighedsperiode mellem Card_MA- og Card_Sign-certifikaterne og mellem VU_MA- og VU_Sign-certifikaterne kun for første generation.

9.2. **Symmetriske nøgler**

9.2.1 *Nøgler til sikring af kommunikation mellem køretøjsenhed og bevægelsessensor*

9.2.1.1 *Generelt*

Bemærk: Læserne af dette afsnit formodes at være fortrolige med indholdet af [ISO 16844-3], som indeholder en beskrivelse af interfacet mellem en køretøjsenhed og en bevægelsessensor. Parringsprocessen mellem en køretøjsenhed og en bevægelsessensor beskrives nærmere i kapitel 12 i dette tillæg.

CSM_100 Der skal bruges et antal symmetriske nøgler til parring af køretøjsenheder og bevægelsessensorer, til gensidig ægthedskontrol mellem køretøjsenheder og bevægelsessensorer og til kryptering af kommunikation mellem køretøjsenheder og bevægelsessensorer som vist i Tabel 3. Alle disse nøgler skal være AES-nøgler med en nøglelængde, der er lig med længden af bevægelsessensorens hovednøgle, som er knyttet til længden af det (planlagte) europæiske rodnøglepar som beskrevet i CSM_50.

Tabel 3

Nøgler til sikring af kommunikation mellem køretøjsenhed og bevægelsessensor

Forklaring	Symbol	Genereret af	Genereringsmetode	Gemt af
Hovednøgle til bevægelsessensoren — køretøjsenhedens del	$K_{M\text{-}VU}$	ERCA	Tilfældig	ERCA, MSCA'er, der udsteder certifikater for køretøjsenheder, fabrikanter af køretøjsenheder, køretøjsenheder
Hovednøglen til bevægelsessensoren — værkstedsdel	$K_{M\text{-}WC}$	ERCA	Tilfældig	ERCA, MSCA'er, kortfabrikanter, værkstedskort

▼B

Forklaring	Symbol	Genereret af	Genereringsmetode	Gemt af
Hovednøgle til bevægelsessensoren	K_M	Genereres ikke uafhængigt	Beregnet som $K_M = K_{M\text{-}VU}$ XOR $K_{M\text{-}WC}$	ERCA, MSCA'er, der er involveret i udstedelse af bevægelsessensornøglepar (valgfrit) (*)
Identifikationsnøgle	K_{ID}	Genereres ikke uafhængigt	Beregnet som $K_{ID} = K_M$ XOR CV, hvor CV specificeres i CSM_106	ERCA, MSCA'er, der er involveret i udstedelse af bevægelsessensornøglepar (valgfrit) (*)
Parringsnøgle	K_P	Fabrikant af bevægelsessensor	Tilfældig	En bevægelsessensor
Sessionsnøgle	K_S	Køretøjsenhed (under parring af køretøjsenhed og bevægelsessensor)	Tilfældig	En køretøjsenhed og en bevægelsessensor

(*) Det er valgfrit, om man vil gemme K_M og K_{ID}, eftersom disse nøgler kan udledes fra $K_{M\text{-}VU}$, $K_{M\text{-}WC}$ og CV.

CSM_101 Den europæiske certificeringsmyndighed genererer $K_{M\text{-}VU}$ og $K_{M\text{-}WC}$, to tilfældige og entydige AES-nøgler, ud fra hvilke bevægelsessensorens hovednøgle K_M kan beregnes som $K_{M\text{-}VU}$ XOR $K_{M\text{-}WC}$. ERCA'en sender K_M, $K_{M\text{-}VU}$ og $K_{M\text{-}WC}$ til medlemsstatens certificeringsmyndighed efter anmodning fra disse.

CSM_102 ERCA'en tildeler hver af bevægelsessensorernes hovednøgler K_M et entydigt versionsnummer, som ligeledes gælder for de indgående nøgler $K_{M\text{-}VU}$ og $K_{M\text{-}WC}$ og den tilhørende identifikationsnøgle K_{ID}. ERCA'en underretter MSCA'erne om versionsnummeret, når den sender $K_{M\text{-}VU}$ og $K_{M\text{-}WC}$ til dem.

Bemærk: Versionsnummeret benyttes til at skelne mellem forskellige generationer af disse nøgler som forklaret nærmere i afsnit 9.2.1.2.

CSM_103 En medlemsstats certificeringsmyndighed fremsender $K_{M\text{-}VU}$ sammen med dens versionsnummer til fabrikanter af køretøjsenheder efter anmodning fra disse. Fabrikanterne af køretøjsenhederne indsætter $K_{M\text{-}VU}$ og dens versionsnummer i alle fremstillede køretøjsenheder.

CSM_104 En medlemsstats certificeringsmyndighed sikrer, at $K_{M\text{-}WC}$ sammen med dens versionsnummer indsættes i alle værkstedskort, som den har ansvaret for at udstede.

Bemærk:

— Se beskrivelsen af datatypen `SensorInstallationSecData` i tillæg 2.

— Som forklaret i afsnit 9.2.1.2 kan det være nødvendigt at indsætte flere generationer af $K_{M\text{-}WC}$ på et og samme værkstedskort.

▼B

CSM_105 Ud over AES-nøglen, som specificeres i CSM_104, skal en MSCA sikre, at TDES-nøglen $Km_{WC,}$ der specificeres i krav CSM_037 i del A i dette tillæg, indsættes i alle værkstedskort, som den har ansvaret for at udstede.

Bemærk:

— Dette gør det muligt at sammenkoble et værkstedskort af anden generation med en køretøjsenhed af første generation.

— Et værkstedskort af anden generation vil indeholde to forskellige applikationer — en, der er i overensstemmelse med del B i dette tillæg, og en, der er i overensstemmelse med del A. Sidstnævnte indeholder TDES-nøglen Km_{WC}.

CSM_106 En MSCA, der beskæftiger sig med at udstede bevægelsessensorer, skal hente identifikationsnøglen fra bevægelsessensorens hovednøgle ved at udføre en XOR-operation på den med en konstant vektor (CV). Værdien af CV er som følger:

— For 128-bit hovednøgler til bevægelsessensorer: CV = ‘B6 44 2C 45 0E F8 D3 62 0B 7A 8A 97 91 E4 5E 83’

— For 192-bit hovednøgler til bevægelsessensorer: 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’

— For 256-bit hovednøgler til bevægelsessensorer: 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’

Bemærk: De konstante vektorer er genereret som følger:

Pi_10 = de første 10 byte af decimaldelen af den matematiske konstant π = ‘24 3F 6A 88 85 A3 08 D3 13 19’

CV_128-bit = første 16 byte af SHA-256(Pi_10)

CV_192-bit = første 24 byte af SHA-384(Pi_10)

CV_256-bit = første 32 byte af SHA-512(Pi_10)

CSM_107 Fabrikanter af bevægelsessensorer genererer en tilfældig og entydig parringsnøgle K_P til hver bevægelsessensor og sender hver enkelt parringsnøgle til en medlemsstats certificeringsmyndighed. MSCA'en krypterer hver parringsnøgle separat med bevægelsessensorens hovednøgle K_M og returnerer den krypterede nøgle til fabrikanten af bevægelsessensoren. For hver krypteret nøgle meddeler MSCA'en fabrikanten af bevægelsessensoren versionsnummeret for den tilhørende K_M.

Bemærk: Som forklaret i afsnit 9.2.1.2 skal en fabrikant af en bevægelsessensor muligvis generere flere entydige parringsnøgler til den samme bevægelsessensor.

▼B

CSM_108 Fabrikanter af bevægelsessensorer genererer et entydigt serienummer til hver bevægelsessensor og sender alle serienumre til en medlemsstats certificeringsmyndighed. MSCA'en krypterer hvert serienummer separat med identifikationsnøglen K_{ID} og returnerer det krypterede serienummer til fabrikanten af bevægelsessensoren. For hvert krypteret serienummer meddeler MSCA'en fabrikanten af bevægelsessensoren versionsnummeret for den tilhørende K_{ID}.

CSM_109 For krav CSM_107 og CSM_108 skal MSCA'en benytte AES-algoritmen i blokkædningsfunktionen som defineret i [ISO 10116] med en indskudt parameter m = 1 og en initialiseringsvektor SV = '00' {16}, dvs. 16 byte med en binær værdi på 0. Om nødvendigt skal MSCA'en benytte udfyldningsmetode 2, som defineres i [ISO 9797-1].

CSM_110 Fabrikanten af bevægelsessensoren gemmer den krypterede parringsnøgle og det krypterede serienummer i den planlagte bevægelsessensor sammen med de tilhørende klartekstværdier og versionsnummeret for K_M og K_{ID}, som benyttes til kryptering.

Bemærk: Som forklaret i afsnit 9.2.1.2 skal en fabrikant af en bevægelsessensor muligvis indsætte flere krypterede parringsnøgler og flere krypterede serienumre i en og samme bevægelsessensor.

CSM_111 Ud over det AES-baserede kryptografiske materiale, der specificeres i CSM_110, kan en fabrikant af en bevægelsessensor ligeledes gemme det TDES-baserede kryptografiske materiale, der specificeres i krav CSM_037 i del A i dette tillæg, i hver bevægelsessensor.

Bemærk: Dette betyder, at en bevægelsessensor af anden generation kan kobles sammen med en køretøjsenhed af første generation.

CSM_112 Længden af sessionsnøglen K_S, som en bevægelsessensor genererer under parringen med en bevægelsessensor, skal kædes sammen med længden af dens $K_{M\text{-}VU}$ som beskrevet i CSM_50.

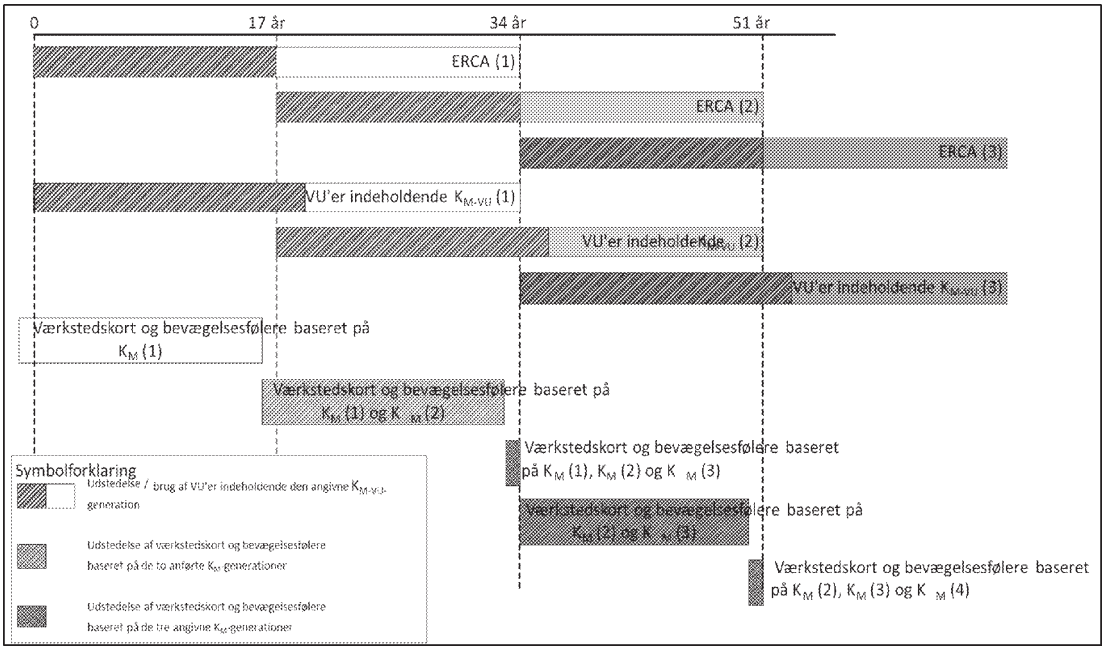
9.2.1.2 *Udskiftning af hovednøglen til bevægelsessensoren i udstyr af anden generation*

CSM_113 Hver hovednøgle til bevægelsessensoren og alle tilhørende nøgler (se Tabel 3) er knyttet til en bestemt generation af ERCA-rodnøglepar. Derfor skal disse nøgler udskiftes hvert 17. år. Gyldighedsperioden for hver hovednøglegeneration for bevægelsessensoren indledes et år inden, det tilhørende ERCA-rodnøglepar bliver gyldigt, og afsluttes, når det tilhørende ERCA-rodnøglepar udløber. Dette fremgår af Figur 2.

▼B

Figur 2

Udstedelse og brug af forskellige generationer af hovednøgler til bevægelsessensorer i køretøjsenheder, bevægelsessensorer og værkstedskortkort



CSM_114 Mindst et år inden genereringen af et nyt europæisk rodnøglepar som beskrevet i CSM_56 genererer ERCA'en en ny hovednøgle til bevægelsessensoren K_M ved at generere en ny K_{M-VU} og K_{M-WC}. Længden af bevægelsessensorens hovednøgle kædes sammen med den planlagte styrke af det nye europæiske rodnøglepar i henhold til CSM_50. ERCA'en sender de nye K_M, K_{M-VU} og K_{M-WC} til MSCA'en efter anmodning fra disse sammen med deres versionsnummer.

CSM_115 En MSCA skal sikre, at alle gyldige generationer af K_{M-WC} gemmes i alle værkstedskort, der udstedes under dens myndighed, sammen med deres versionsnumre som vist i Figur 2.

Bemærk: Dette betyder, at værkstedskortene i det sidste år af et ERCA-certifikats gyldighedsperiode vil blive udstedt med tre forskellige generationer af K_{M-WC} som vist i Figur 2.

CSM_116 Med hensyn til den proces, der beskrives i CSM_107 og CSM_108 ovenfor: En MSCA skal kryptere hver parringsnøgle K_P, som den modtager fra en fabrikant af en bevægelsessensor separat med hver gyldig generation af hovednøgler til bevægelsessensoren K_M. En MSCA skal ligeledes kryptere hvert serienummer, som den modtager fra en fabrikant af en bevægelsessensor, separat med hver gyldig generation af identifikationsnøglen K_{ID}. En fabrikant af en bevægelsessensor gemmer alle krypteringer af parringsnøglen og alle krypteringer af serienummeret i den planlagte bevægelsessensor sammen med de tilhørende klartekstværdier og versionsnummer/-numre for K_M og K_{ID}, som benyttes til kryptering.

▼B

Bemærk: Dette betyder, at i det sidste år af et ERCA-certifikats gyldighedsperiode, vil bevægelsessensorerne blive udstedt med krypterede data baseret på tre forskellige generationer af K_M som vist i Figur 2.

CSM_117 Med hensyn til den proces, som beskrives i CSM_107 ovenfor: Eftersom længden af parringsnøglen K_P skal være kædet sammen med længden af K_M (se CSM_100), skal en fabrikant af en bevægelsessensor muligvis generere op til tre forskellige parringsnøgler (af forskellig længde) til samme bevægelsessensor, hvis efterfølgende generationer af K_M har forskellige længder. I dette tilfælde skal fabrikanten sende hver parringsnøgle til MSCA'en. MSCA'en skal sikre, at hver parringsnøgle er krypteret med den korrekte generation af bevægelsessensorens hovednøgle, dvs. den med samme længde.

Bemærk: Hvis fabrikanten af bevægelsessensoren vælger at generere en TDES-baseret parringsnøgle til en bevægelsessensor af anden generation (se CSM_111), skal fabrikanten over for MSCA'en angive, at den TDES-baserede hovednøgle til bevægelsessensoren skal benyttes til kryptering af denne parringsnøgle. Dette skyldes, at længden af en TDES-nøgle kan være lig med længden af en AES-nøgle, så MSCA'en kan ikke vurdere dette alene ud fra nøglelængden.

CSM_118 Fabrikanter af køretøjsenheder må kun isætte en generation af $K_{M\text{-}VU}$ i hver køretøjsenhed sammen med dens versionsnummer. Denne $K_{M\text{-}VU}$-generation kædes sammen med det ERCA-certifikat, som køretøjsenhedens certifikater er baseret på.

Bemærk:

— En køretøjsenhed baseret på et ERCA-certifikat af generation *X* skal kun indeholde $K_{M\text{-}VU}$ af generation *X*, selv om det er udstedt efter indledningen af gyldighedsperioden for ERCA-certifikatet af generation *X+1*. Dette illustreres i Figur 2.

— En køretøjsenhed af generation *X* kan ikke parres med en bevægelsessensor af generation *X-1*.

— Eftersom værkstedskort har en gyldighedsperiode på et år, er resultatet af CSM_113-CSM_118, at alle værkstedskort vil indeholde den nye $K_{M\text{-}WC}$ på det tidspunkt, hvor den første køretøjsenhed, der indeholder den nye $K_{M\text{-}VU}$, udstedes. Derfor vil en sådan køretøjsenhed altid kunne beregne den nye K_M. Desuden vil de fleste nye bevægelsessensorer på det tidspunkt også indeholde krypterede data baseret på den nye K_M.

9.2.2 *Nøgler til sikring af DSRC-kommunikation*

9.2.2.1 *Generelt*

CSM_119 Ægtheden og fortroligheden af data, der sendes fra en køretøjsenhed til en kontrolmyndighed via en DSRC-fjernkommunikationskanal, skal sikres ved hjælp af et sæt køretøjsenhedsspecifikke AES-nøgler, der er udledt af en enkelt DSRC-hovednøgle, KM_{DSRC}.

▼B

CSM_120 DSRC-hovednøglen KM_{DSRC} skal være en AES-nøgle, som ERCA'en genererer, gemmer og distribuerer sikkert. Nøglens længde kan være 128, 192 eller 256 bit og skal være kædet sammen med længden af det europæiske rodnøglepar som beskrevet i CSM_50.

CSM_121 ERCA'en sender DSRC-hovednøglen til medlemsstatens certificeringsmyndigheder på en sikker måde efter anmodning fra disse for at give dem mulighed for at udlede køretøjsenhedsspecifikke DSRC-nøgler og for at sikre, at DSRC-hovednøglen isættes alle kontrolkort og værkstedskort, der udstedes under deres ansvar.

CSM_122 ERCA'en tildeler hver DSRC-hovednøgle et entydigt versionsnummer. ERCA'en underretter MSCA'erne om versionsnummeret, når de fremsender DSRC-hovednøglen til dem.

Bemærk: Versionsnummeret benyttes til at skelne mellem forskellige generationer af DSRC-hovednøgler som forklaret nærmere i afsnit 9.2.2.2.

CSM_123 For hver køretøjsenhed skal fabrikanten af køretøjsenheden oprette et entydigt serienummer for køretøjsenheden og sende dette nummer til sin medlemsstats certificeringsmyndighed med en anmodning om at få et sæt bestående af to køretøjsenhedsspecifikke DSRC-nøgler. Køretøjsenhedens serienummer har datatypen `VuSerialNumber`, og Distinguished Encoding Rules (DER) i henhold til [ISO 8825-1] skal anvendes til kodningen.

CSM_124 Efter at have modtaget en anmodning om køretøjsenhedsspecifikke DSRC-nøgler udleder MSCA'en to AES-nøgler til køretøjsenheden, som kaldes $K_VU_{DSRC}_ENC$ og $K_VU_{DSRC}_MAC$. Disse køretøjsenhedsspecifikke nøgler skal have samme længde som DSRC-hovednøglen. MSCA'en skal benytte den nøgleudledningsfunktion, der defineres i [RFC 5869]. Hash-funktionen, der skal benyttes til at instantiere HMAC-hash-funktionen, skal være knyttet til længden af DSRC-hovednøglen som beskrevet i CSM_50. Nøgleudledningsfunktionen i [RFC 5869] skal anvendes som følger:

Trin 1 (Udtræk):

— *PRK* = HMAC-Hash (*salt, IKM*), hvor *salt* er en tom streng ‘’, og *IKM* er KM_{DSRC}.

Trin 2 (Udvid):

— *OKM* = *T(1)*, hvor

T(1) = HMAC-Hash (*PRK*, *T(0)* || *info* || ‘01’) med

▼B

— *T(0)* = en tom streng (‘’)

— *info* = køretøjsenhedens serienummer som specificeret i CSM_123

— K_VU_{DSRC}_ENC = første *L* oktetter af *OKM* og

K_VU_{DSRC}_MAC = sidste *L* oktetter af *OKM*,

hvor *L* er den krævede længde af K_VU_{DSRC}_ENC og K_VU_{DSRC}_MAC i oktetter.

CSM_125 MSCA'en distribuerer K_VU_{DSRC}_ENC og K_VU_{DSRC}_MAC til fabrikanten af køretøjsenheden på en sikker måde med henblik på indsættelse i den planlagte køretøjsenhed.

CSM_126 Når en køretøjsenhed udstedes, skal den have K_VU_{DSRC}_ENC og K_VU_{DSRC}_MAC lagret i sin sikre hukommelse for at kunne sikre integriteten, ægtheden og fortroligheden af de data, der sendes via fjernkommunikationskanalen. En køretøjsenhed skal ligeledes gemme versionsnummeret på DSRC-hovednøglen, der benyttes til at udlede disse køretøjsenhedsspecifikke nøgler.

CSM_127 Når kontrolkort og værkstedskort udstedes, skal de have KM_{DSRC} lagret i deres sikre hukommelse for at kunne verificere integriteten og ægtheden af data, som sendes af en køretøjsenhed via fjernkommunikationskanalen, og dekryptere disse data. Kontrolkort og værkstedskort skal ligeledes have versionsnummeret for DSRC-hovednøglen lagret.

Bemærk: Som forklaret i afsnit 9.2.2.2 skal flere generationer af KM_{DSRC} muligvis indsættes på et og samme værkstedskort eller kontrolkort.

CSM_128 MSCA'en fører registre over alle køretøjsenhedsspecifikke DSRC-nøgler, som den har genereret, deres versionsnummer og identifikationen af den køretøjsenhed, som de enkelte nøglesæt er beregnet til.

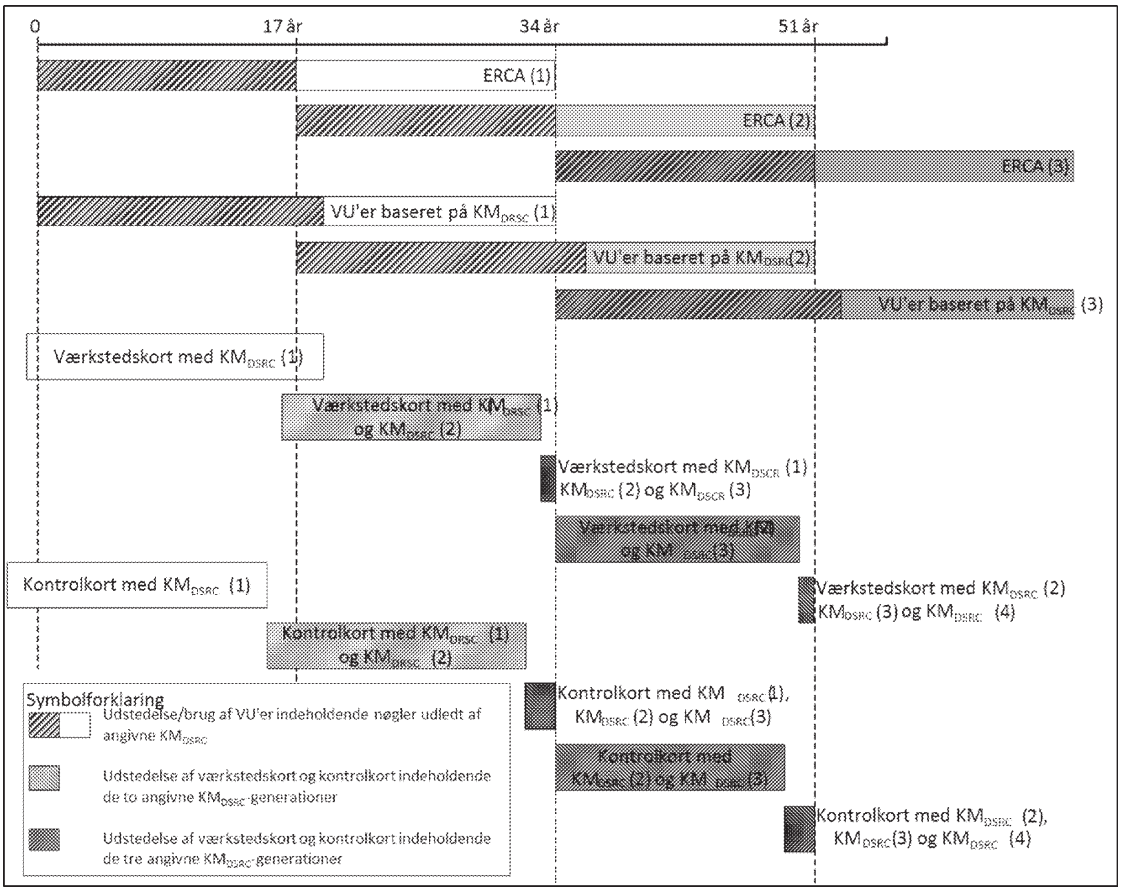
9.2.2.2 *Udskiftning af DSRC-hovednøgle*

CSM_129 Hver DSRC-hovednøgle er knyttet til en bestemt generation af ERCA-rodnøglepar. Derfor skal ERCA'en udskifte DSRC-hovednøglen hvert 17. år. Gyldighedsperioden af hver DSRC-hovednøglegeneration indledes to år inden, det tilhørende ERCA-rodnøglepar bliver gyldigt, og afsluttes, når det tilhørende ERCA-rodnøglepar udløber. Dette fremgår af Figur 3.

▼B

Figur 3

Udstedelse og brug af forskellige generationer af DSRC-hovednøglen i køretøjsenheder, værkstedskort og kontrolkort



CSM_130 Mindst to år før ERCA'en genererer et nyt europæisk rodnøglepar som beskrevet i CSM_56, skal den generere en ny DSRC-hovednøgle. Længden af DSRC-nøglen kædes sammen med den planlagte styrke af det nye europæiske rodnøglepar i henhold til CSM_50. ERCA'en sender den nye DSRC-hovednøgle til MSCA'erne på anmodning fra disse sammen med dens versionsnummer.

CSM_131 En MSCA skal sikre, at alle gyldige generationer af K_{DSRC} gemmes i alle kontrolkort, der udstedes under dens myndighed, sammen med deres versionsnumre som vist i Figur 3.

Bemærk: Dette betyder, at kontrolkortet i det sidste år af et ERCA-certifikats gyldighedsperiode vil blive udstedt med tre forskellige generationer af K_{DSRC} som vist i Figur 3.

CSM_132 En MSCA skal sikre, at alle generationer af K_{DSRC}, der har været gyldige i mindst et år, gemmes i alle værkstedskort, der udstedes under dens myndighed, sammen med deres versionsnumre som vist i Figur 3.

▼B

Bemærk: Dette betyder, at værkstedskort i det sidste år af et ERCA-certifikats gyldighedsperiode vil blive udstedt med tre forskellige generationer af K_{DSRC} som vist i Figur 2.

CSM_133 Fabrikanter af køretøjsenheder må kun sætte et sæt køretøjsenhedsspecifikke DSRC-nøgler i hver køretøjsenhed sammen med dens versionsnummer. Dette sæt nøgler udledes fra den KM_{DSRC}-generation, der er knyttet til det ERCA-certifikat, som køretøjsenhedens certifikater er baseret på.

Bemærk:

— Dette indebærer, at en køretøjsenhed baseret på et ERCA-certifikat af generation *X* kun må indeholde K_VU_{DSRC} og K_VU_{DSRC}_MAC af generation *X*, selv om køretøjsenheden udstedes efter indledningen af gyldighedsperioden for ERCA-certifikatet af generation *X+1*. Dette illustreres i Figur 3.

— Eftersom værkstedskort har en gyldighedsperiode på et år og kontrolkort på to år, er resultatet af CSM_131-CSM_133, at værkstedskort og kontrolkort vil indeholde den nye DSRC-hovednøgle på det tidspunkt, hvor den første køretøjsenhed, der indeholder køretøjsenhedsspecifikke nøgler baseret på den pågældende hovednøgle, udstedes.

9.3. **Certifikater**

9.3.1 *Generelt*

CSM_134 Alle certifikater i det europæiske intelligent takograf-system er selvbeskrivende, kort-verificerbare (CV) certifikater i henhold til [ISO 7816-4] og [ISO 7816-8].

CSM_135 Distinguished Encoding Rules (DER) i henhold til [ISO 8825-1] skal anvendes til kodning af både ASN.1-datastrukturer og (applikationsspecifikke) dataobjekter inden for certifikater.

Bemærk: Denne kodning medfører følgende mærkat-længde-værdi- (TLV) struktur:

Mærkat: Mærkaten kodet i en eller to oktetter med angivelse af indholdet.

Længde: Længden kodet som et ikke-underskrevet heltal i en, to eller tre oktetter, hvilket giver en maksimal længde på 65 535 oktetter. Det mindste antal oktetter skal benyttes.

Værdi: Værdien kodet i nul eller flere oktetter

9.3.2 *Certifikaters indhold*

CSM_136 Alle certifikater skal følge den struktur, der vises i certifikatprofilen i Tabel 4.

Tabel 4

Certifikatprofil version 1

Felt	Felt-ID	Mærkat	Længde (byte)	ASN.1-datatype (se tillæg 1)
ECC-certifikat	C	'7F 21'	var	
ECC-certifikattekst	B	'7F 4E'	var	

▼B

Felt	Felt-ID	Mærkat	Længde (byte)	ASN.1-datatype (se tillæg 1)
Certifikatprofil-identifikator	CPI	'5F 29'	'01'	INTEGER(0..255)
Henvisning til certificeringsmyndighed	CAR	'42'	'08'	KeyIdentifier
Certifikatindehavers autorisation	CHA	'5F 4C'	'07'	CertificateHolder Authorisation
Offentlig nøgle	PK	'7F 49'	var	
Domæneparametre	DP	'06'	var	OBJECT IDENTIFIER
Offentligt punkt	PP	'86'	var	OCTET STRING
Henvisning til certifikatindehaver	CHR	'5F 20'	'08'	KeyIdentifier
Certifikatets gyldighedsdato	CEfD	'5F 25'	'04'	TimeReal
Certifikatets udløbsdato	CExD	'5F 24'	'04'	TimeReal
ECC-certifikatunderskrift	S	'5F 37'	var	OCTET STRING

Bemærk: Felt-ID vil blive brugt i senere afsnit i dette tillæg til at angive de individuelle felter i et certifikat, f.eks. er X.CAR henvisningen til certifikatmyndigheden, som nævnes i certifikatet for brugeren X.

9.3.2.1 Certifikatprofil-identifikator

CSM_137 Certifikater skal anvende en certifikatprofil-identifikator til at angive den benyttede certifikatprofil. Version 1, som specificeret i Tabel 4, identificeres med en værdi på '00'.

9.3.2.2 Henvisning til certificeringsmyndighed

CSM_138 Henvisningen til certificeringsmyndigheden benyttes til at identificere den offentlige nøgle, der skal bruges til at verificere certifikatets underskrift. Henvisningen til certificeringsmyndigheden skal derfor være lig med henvisningen til certifikatindehaveren i certifikatet for den tilhørende certifikatmyndighed.

CSM_139 Et ERCA-rodcertifikat skal være selvunderskrevet, dvs. at henvisningen til certificeringsmyndigheden og henvisningen til certifikatindehaveren i certifikatet skal være den samme.

▼B

CSM_140 For et ERCA-forbindelsescertifikat skal henvisningen til certificeringsmyndigheden være lig med CHR for det nye ERCA-rodcertifikat. Henvisningen til certificeringsmyndigheden for et forbindelsescertifikat skal være lig med CHR for det tidligere ERCA-rodcertifikat.

9.3.2.3 Certifikatindehavers autorisation

CSM_141 Certifikatindehavers autorisation anvendes til at identificere typen af certifikat. Den består af de seks mest betydende byte i takografens applikations-ID sammenføjet med den type udstyr, som certifikatet er beregnet til.

9.3.2.4 Offentlig nøgle

Den offentlige nøgle indeholder to dataelementer: de standardiserede domæneparametre, der skal bruges sammen med den offentlige nøgle i certifikatet, og værdien af det offentlige punkt.

CSM_142 Dataelementet Domæneparametre skal indeholde en af de objektidentifikatorer, der specificeres i Tabel 1, for at henvise til et sæt standardiserede domæneparametre.

CSM_143 Dataelementet Offentligt punkt indeholder det offentlige punkt. Offentlige punkter i form af elliptiske kurver skal konverteres til oktetstrenge som specificeret i [TR-03111]. Det ukomprimerede kodningsformat skal benyttes. Når man genopretter et elliptisk kurvepunkt fra dets kodede format, skal de valideringer, der beskrives i [TR-03111], altid foretages.

9.3.2.5 Henvisning til certifikatindehaver

CSM_144 Henvisningen til certifikatindehaveren er en identifikator for den offentlige nøgle, som certifikatet indeholder. Den skal bruges som henvisning til denne offentlige nøgle i andre certifikater.

CSM_145 For kortcertifikater og certifikater for eksternt GNSS-udstyr skal henvisningen til certifikatindehaveren have datatypen `ExtendedSerialNumber`, som specificeres i tillæg 1.

CSM_146 For køretøjsenheder kender fabrikanten ved anmodning om et certifikat eventuelt det fabrikantspecifikke serienummer på køretøjsenheden, som det pågældende certifikat og den tilhørende private nøgle er beregnet til. I førstnævnte tilfælde skal henvisningen til certifikatindehaveren have datatypen `ExtendedSerialNumber`, der specificeres i tillæg 1. I sidstnævnte tilfælde skal henvisningen til certifikatindehaveren have datatypen `CertificateRequestID`, der specificeres i tillæg 1.

CSM_147 For ERCA- og MSCA-certifikater skal henvisningen til certifikatindehaveren have datatypen `CertificationAuthorityKID`, der specificeres i tillæg 1.

▼B

9.3.2.6 Certifikatets gyldighedsdato

CSM_148 Certifikatets gyldighedsdato angiver startdato og -tidspunkt for certifikatets gyldighedsperiode. Certifikatets gyldighedsdato er datoen for generering af certifikatet.

9.3.2.7 Certifikatets udløbsdato

CSM_149 Certifikatets udløbsdato angiver slutdato og -tidspunkt for certifikatets gyldighedsperiode.

9.3.2.8 Certifikatunderskrift

CSM_150 Underskriften på certifikatet skal oprettes over den kodede certifikattekst, inklusive certifikattekstens mærkat og længde. Underskriftslogaritmen er ECDSA som specificeret i [DSS] ved hjælp af hash-algoritmen, der er knyttet til den underskrivende myndigheds nøglestørrelse som specificeret i CSM_50. Underskriftsformatet skal være klartekst som specificeret i [TR-03111].

9.3.3 *Anmodning om certifikater*

CSM_151 Når man anmoder om et certifikat, skal følgende data sendes til certificeringsmyndigheden:

— Certifikatprofilidentifikatoren for det ønskede certifikat

— Henvisningen til den certificeringsmyndighed, som forventes anvendt til at underskrive certifikatet.

— Den offentlige nøgle, der skal underskrives.

CSM_152 Ud over dataene i CSM_151 skal en MSCA sende følgende data til ERCA'en i anmodningen om et certifikat, således at ERCA'en får mulighed for at oprette henvisningen til certifikatindehaveren for det nye MSCA-certifikat:

— Den numeriske landekode for certificeringsmyndigheden (datatype `NationNumeric` defineret i tillæg 1)

— Den alfanumeriske landekode for certificeringsmyndigheden (datatyp `NationAlpha` defineret i tillæg 1)

— Serienummeret på 1 byte, som bruges til at skelne mellem certificeringsmyndighedens forskellige nøgler, hvis nøglerne skal skiftes

— Feltet på 2 byte, der indeholder specifikke supplerende oplysninger om certificeringsmyndigheden.

CSM_153 Ud over dataene i CSM_151 skal en udstyrsfabrikant sende følgende data til en MSCA i anmodningen om et certifikat, således at MSCA'en får mulighed for at oprette henvisningen til certifikatindehaveren for det nye udstyrscertifikat:

— En fabrikantspecifik identifikator for udstyrstypen

— Hvis dette kendes (se CSM_154), et serienummer for udstyret, som er entydigt for fabrikanten, udstyrstypen og produktionsmåneden. Ellers en entydig identifikator for certifikatanmodningen

▼B

— Måned og år for produktionen af udstyret eller for anmodningen om certifikatet.

Fabrikanten skal sikre, at disse data er korrekte, og at det certifikat, der sendes tilbage af MSCA'en, sættes i det planlagte udstyr.

CSM_154 For køretøjsenheder kender fabrikanten ved anmodning om et certifikat eventuelt det fabrikantspecifikke serienummer for køretøjsenheden, som det pågældende certifikat og den tilhørende private nøgle er beregnet til. Hvis serienummeret er kendt, skal fabrikanten af køretøjsenheden sende dette til MSCA'en. Hvis det ikke er kendt, skal fabrikanten entydigt identificere hver enkelt certifikatanmodning og sende serienummeret på denne certifikatanmodning til MSCA'en. Det resulterende certifikat vil herefter indeholde serienummeret på certifikatanmodningen. Efter at have isat certifikatet i en specifik køretøjsenhed skal fabrikanten give MSCA'en meddelelse om forbindelsen mellem serienummeret på certifikatanmodningen og køretøjsenhedens identifikationsnummer.

10. GENSIDIG ÆGTHEDSKONTROL OG SIKKER MEDDELELSESOVERFØRSEL MELLEM KØRETØJSENHED OG KORT

10.1. **Generelt**

CSM_155 På et højt niveau er sikker kommunikation mellem en køretøjsenhed og et takografkort baseret på følgende trin:

— Først skal hver part demonstrere over for den anden part, at den ejer et gyldigt offentligt nøglecertifikat underskrevet af en medlemsstats certificeringsmyndighed. Herefter skal MSCA'ens offentlige nøglecertifikat underskrives af den europæiske certificeringsmyndighed. Dette trin kaldes certifikatkædeverificering og specificeres nærmere i afsnit 10.2

— For det andet skal køretøjsenheden over for kortet påvise, at den er i besiddelse af den private nøgle, der svarer til den offentlige nøgle i det fremlagte certifikat. Dette sker ved at underskrive et tilfældigt nummer, som fremsendes af kortet. Kortet verificerer underskriften over det tilfældige tal. Hvis denne verifikation lykkes, er køretøjsenhedens ægthed bekræftet. Dette trin kaldes ægthedskontrol af køretøjsenhed og specificeres nærmere i afsnit 10.3

— For det tredje beregner begge parter uafhængigt af hinanden to AES-sessionsnøgler ved hjælp af en asymmetrisk nøgleoverensstemmelsesalgoritme. Ved hjælp af disse sessionsnøgler opretter kortet en kode, der bekræfter meddelelsens ægthed (MAC), over nogle data, der sendes af køretøjsenheden. Køretøjsenheden verificerer MAC'en. Hvis denne verifikation lykkes, er kortets ægthed bekræftet. Dette trin kaldes ægthedskontrol af kort og specificeres nærmere i afsnit 10.4

— For det fjerde skal køretøjsenheden og kortet bruge de sessionsnøgler, for hvilke der er udført overensstemmelseskontrol, for at sikre fortroligheden, integriteten og ægtheden af alle udvekslede meddelelser. Dette kaldes sikker meddelelsesoverførsel og specificeres nærmere i afsnit 10.5.

CSM_156 Mekanismen, der beskrives i CSM_155, udløses af køretøjsenheden, når der sættes et kort i en af kortlæserne.

▼B

10.2. **Gensidig certifikatkædeverificering**

10.2.1 *Kortcertifikatkædeverificering foretaget af køretøjsenheden*

CSM_157 Køretøjsenheder skal anvende den protokol, der beskrives i Figur 4, til at verificere takografkorts certifikatkæde.

Bemærkninger til Figur 4:

— Kortcertifikaterne og de offentlige nøgler, der nævnes i figuren, er dem, der anvendes til gensidig ægthedskontrol. I afsnit 9.1.5 betegnes disse som Card_MA.

— Card.CA-certifikaterne og de offentlige nøgler, der nævnes i figuren, er dem, der anvendes til underskrift af kortcertifikater, og det angives i kortcertifikatets CAR. I afsnit 9.1.3 betegnes disse som MSCA_Card.

— Card.CA.EUR-certifikatet, der nævnes i figuren, er det europæiske rodcertifikat, der angives i Card.CA-certifikatets CAR.

— Card.Link-certifikatet, der nævnes i figuren, er kortets linkcertifikat, hvis dette findes. Som beskrevet i afsnit 9.1.2 er dette et forbindelsescertifikat til et europæisk rodnøglepar, som er oprettet af ERCA'en og underskrevet med den tidligere europæiske private nøgle.

— Card.Link.EUR-certifikatet, der nævnes i figuren, er det europæiske rodcertifikat, der angives i Card.Link-certifikatets CAR.

CSM_158 Som afbilledet i Figur 4 skal verifikationen af kortets certifikatkæde indledes, når kortet isættes. Køretøjsenheden skal læse henvisningen til kortindehaveren (`cardExtendedSerialNumber`) fra elementærfilen ICC. Køretøjsenheden kontrollerer, om den kender kortet, dvs. om den tidligere har verificeret kortets certifikatkæde og gemt den til senere brug. Hvis dette er tilfældet, og kortets certifikat stadig er gyldigt, fortsættes processen med verifikation af certifikatkæden for køretøjsenheden. Ellers skal køretøjsenheden gradvist læse fra kortets MSCA_Card-certifikat, som skal benyttes til at verificere kortets certifikat, Card.CA.EUR-certifikatet, som skal bruges til at verificere MSCA_Card-certifikatet, og eventuelt forbindelsescertifikatet, indtil den finder et certifikat, den kender eller kan verificere. Hvis den finder et sådant certifikat, skal køretøjsenheden bruge dette certifikat til at verificere de underliggende kortcertifikater, som den har læst fra kortet. Hvis dette lykkes, fortsætter processen med verifikationen af certifikatkæden for køretøjsenheden. Hvis det ikke lykkes, ignorerer køretøjsenheden kortet.

▼B

Bemærk: Der er tre muligheder for, at køretøjsenheden kender Card.CA.EUR-certifikatet:

— Card.CA.EUR-certifikatet er det samme certifikat som køretøjsenhedens eget EUR-certifikat

— Card.CA.EUR-certifikatet er tidligere end køretøjsenhedens eget EUR-certifikat, og køretøjsenheden havde allerede dette certifikat på tidspunktet for udstedelsen (se CSM_81)

— Card.CA.EUR-certifikatet er senere end køretøjsenhedens eget EUR-certifikat, og køretøjsenheden har tidligere modtaget et forbindelsescertifikat fra et andet takografkort, verificeret det og gemt det til senere brug.

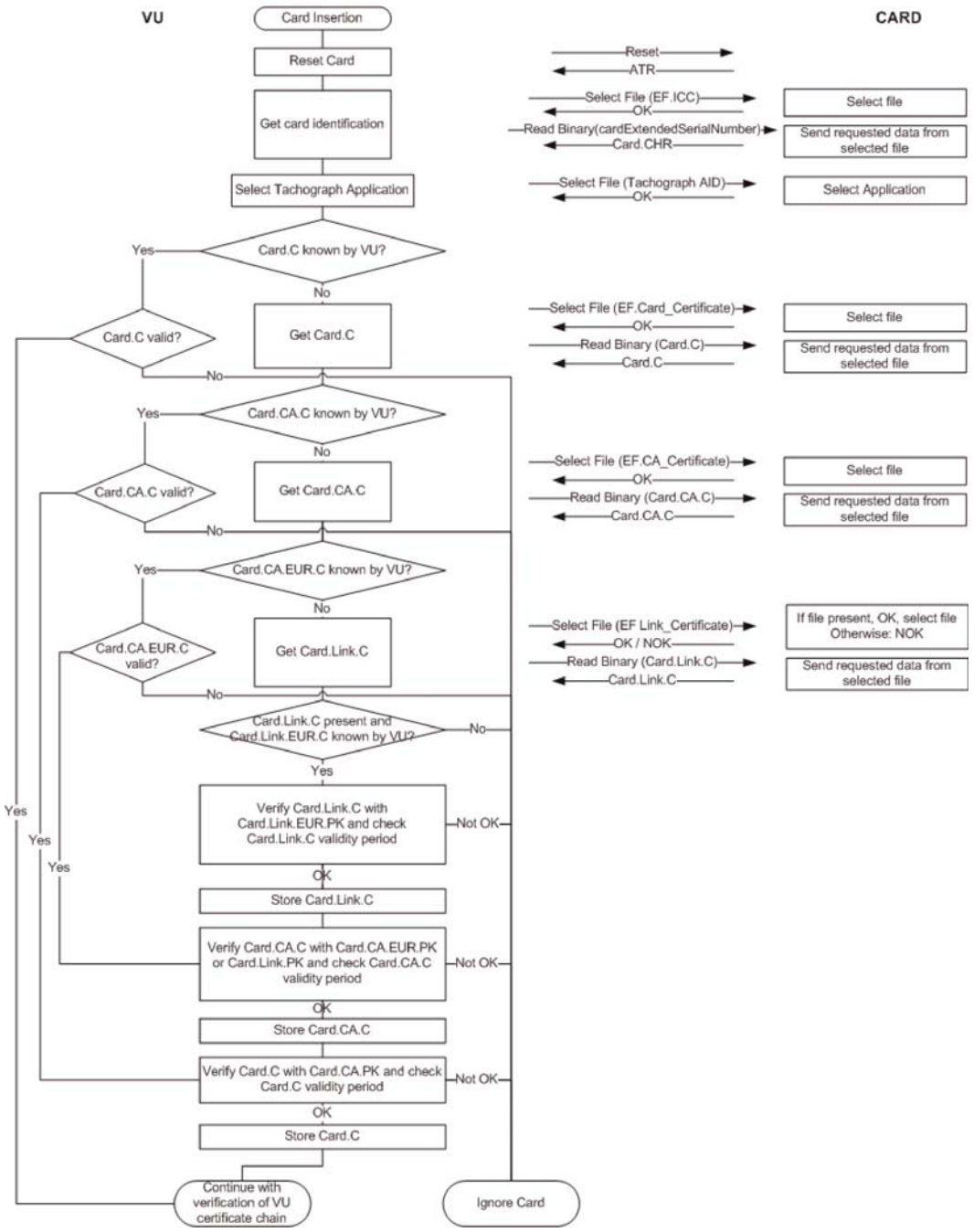
CSM_159 Som anført i Figur 4 kan køretøjsenheden, så snart den har verificeret ægtheden og gyldigheden af et hidtil ukendt certifikat, gemme dette certifikat til senere brug, så det ikke er nødvendigt at verificere det pågældende certifikats ægthed, hvis køretøjsenheden præsenteres for det igen. I stedet for at gemme hele certifikatet kan en køretøjsenhed vælge kun at gemme indholdet af certifikatteksten som angivet i afsnit 9.3.2.

CSM_160 Køretøjsenheden verificerer den tidsmæssige gyldighed af alle certifikater, der læses fra kortet eller er gemt i hukommelsen, og afviser udløbne certifikater. Køretøjsenheden anvender sit interne ur til at verificere den tidsmæssige gyldighed af et certifikat, som sendes af kortet.

▼B

Figur 4

Protokol til køretøjsenhedens verifikation af kortets certifikatkæde



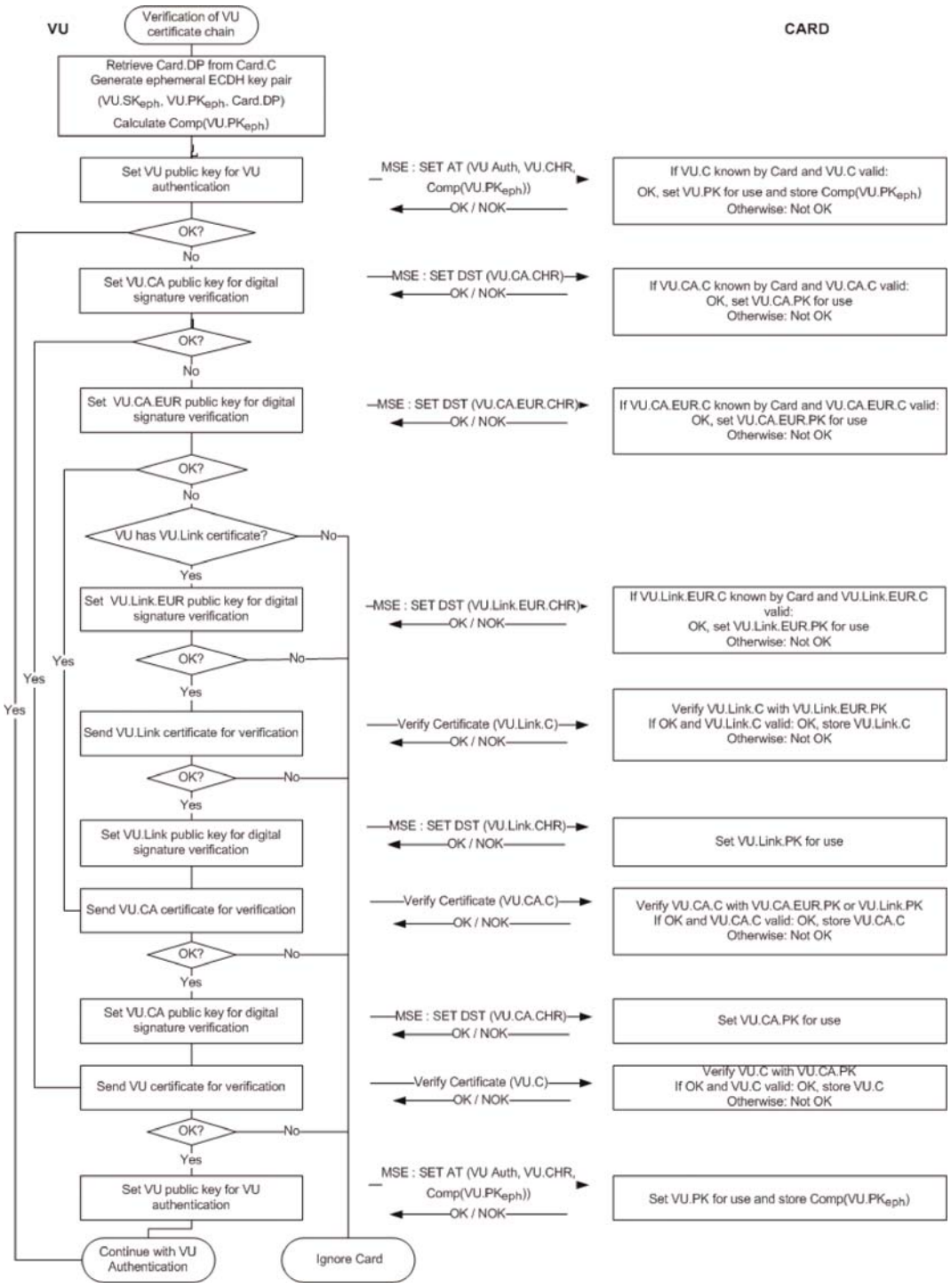
10.2.2 *Kortcertifikatkædeverificering foretaget af kortet*

CSM_161 Takografkort skal benytte den protokol, der illustreres i Figur 5 til verifikation af en køretøjsenheds certifikatkæde.

▼B

Figur 5

Protokol til kortets verifikation af køretøjsenhedens certifikatkæde



Bemærkninger til Figur 5:

— Køretøjsenhedens certifikater og de offentlige nøgler, der nævnes i figuren, er dem, der anvendes til gensidig ægthedskontrol. I afsnit 9.1.4 betegnes disse som VU_MA.

▼B

— VU.CA-certifikaterne og de offentlige nøgler, der nævnes i figuren, er dem, der anvendes til underskrift af køretøjsenhedscertifikater og certifikater for eksternt GNSS-udstyr. I afsnit 9.1.3 betegnes disse som MSCA_VU_EGF.

— VU.CA.EUR-certifikatet, der nævnes i figuren, er det europæiske rodcertifikat, der angives i VU.CA-certifikatets CAR.

— VU.Link-certifikatet, der nævnes i figuren, er køretøjsenhedens forbindelsescertifikat, hvis dette findes. Som beskrevet i afsnit 9.1.2 er dette et forbindelsescertifikat til et europæisk rodnøglepar, som er oprettet af ERCA'en og underskrevet med den tidligere europæiske private nøgle.

— VU.Link.EUR-certifikatet, der nævnes i figuren, er det europæiske rodcertifikat, der angives i VU.Link-certifikatets CAR.

CSM_162 Som beskrevet i Figur 5 begynder verifikationen af køretøjsenhedens certifikatkæde med, at køretøjsenheden forsøger at anvende sin egen offentlige nøgle i takografkortet. Hvis dette lykkes, betyder det, at kortet tidligere har verificeret køretøjsenheden og har gemt køretøjsenhedscertifikatet til fremtidig brug. I dette tilfælde benyttes køretøjsenhedscertifikatet, og processen fortsætter med ægthedskontrol af køretøjsenheden. Hvis kortet ikke kender køretøjsenhedens certifikat, skal køretøjsenheden først fremsende det VU.CA-certifikat, som skal benyttes til at verificere dens køretøjsenhedscertifikat, VU.CA.EUR-certifikatet, som skal bruges til at verificere VU.CA-certifikatet og eventuelt forbindelsescertifikatet for at finde et certifikat, som kortet kender eller kan verificere. Hvis den finder et sådant certifikat, skal kortet bruge dette certifikat til at verificere de underliggende køretøjsenhedscertifikater, som det præsenteres for. Hvis det lykkes, vælger køretøjsenheden endeligt sin offentlige nøgle til brug i takografkortet. Hvis det ikke lykkes, ignorerer køretøjsenheden kortet.

Bemærk: Der er tre muligheder for, at koret kender VU.CA.EUR-certifikatet:

— VU.CA.EUR-certifikatet er det samme certifikat som kortets eget EUR-certifikat

— VU.CA.EUR-certifikatet er tidligere end kortets eget EUR-certifikat, og kortet havde allerede dette certifikat på tidspunktet for udstedelsen (se CSM_91)

— VU.CA.EUR-certifikatet er senere end kortets eget EUR-certifikat, og kortet har tidligere modtaget et forbindelsescertifikat fra en anden køretøjsenhed, verificeret det og gemt det til senere brug.

CSM_163 Køretøjsenheden bruger kommandoen MSE: Set AT til at angive sin offentlige nøgle til brug i takografkortet. Som angivet i tillæg 2 indeholder denne kommando en indikation af den kryptografiske mekanisme, der skal bruges sammen med den nøgle, der er fastlagt. Denne mekanisme er »ægthedskontrol af køretøjsenhed ved brug af ECDSA-algoritmen kombineret med hash-algoritmen kombineret med nøglestørrelsen af køretøjsenhedens VU_MA-nøglepar som specificeret i CSM_50«.

▼B

CSM_164 Kommandoen MSE: Set AT indeholder ligeledes en indikation af det midlertidige nøglepar, som køretøjsenheden skal bruge ved overensstemmelseskontrol af sessionsnøglen (se afsnit 10.4). Inden køretøjsenheden sender kommandoen MSE: Set AT, genererer den således et midlertidigt ECC-nøglepar. Ved generering af det midlertidige nøglepar bruger køretøjsenheden de standardiserede domæneparametre, der er angivet i kortets certifikat. Det midlertidige nøglepar betegnes ($VU.SK_{eph}$, $VU.PK_{eph}$, Card.DP). Køretøjsenheden anvender x-koordinaten i det midlertidige offentlige punkt for ECDH som nøgleidentifikation; dette kaldes den komprimerede gengivelse af den offentlige nøgle og betegnes Comp($VU.PK_{eph}$).

CSM_165 Hvis kommandoen MSE: Set AT giver et positivt resultat, angiver kortet den angivne VU.PK til efterfølgende brug under ægthedskontrol af køretøjet og gemmer Comp($VU.PK_{eph}$) midlertidigt. Hvis der sendes to eller flere vellykkede MSE: Set AT-kommandoer, inden overensstemmelseskontrollen af sessionsnøglen gennemføres, gemmer kortet kun den seneste modtagne Comp($VU.PK_{eph}$).

CSM_166 Kortet verificerer den tidsmæssige gyldighed af alle certifikater, som køretøjsenheden sender eller henviser til, mens de er gemt i kortets hukommelse, og afviser udløbne certifikater.

CSM_167 Med henblik på verificering af den tidsmæssige gyldighed af et certifikat, som fremsendes af køretøjsenheden, gemmer hvert takografkort internt nogle data, der repræsenterer det aktuelle tidspunkt. Disse data kan ikke ajourføres direkte af en køretøjsenhed. Ved udstedelsen sættes det aktuelle tidspunkt for et kort til at være lig med den aktuelle dato for kortets Card_MA-certifikat. Et kort ajourfører sit aktuelle tidspunkt, hvis en køretøjsenhed fremsender den faktiske dato for et autentisk »gyldig tidsangiver«-certifikat, som er nyere end kortets aktuelle tidspunkt. I dette tilfælde indstiller kortet sit aktuelle tidspunkt til den faktiske dato på det pågældende certifikat. Kortet accepterer kun følgende certifikater som gyldig tidsangiver:

— ERCA-forbindelsescertifikater af anden generation

— MSCA-certifikater af anden generation

— køretøjsenhedscertifikater af anden generation, som er udstedt af samme land som kortets eget/egne kortcertifikat(er).

Bemærk: Det seneste krav indebærer, at et kort skal kunne genkende køretøjsenhedscertifikatets CAR, dvs. MSCA_VU-EGF-certifikatet. Dette vil ikke være det samme som CAR for kortets eget certifikat, som er MSCA_Card-certifikatet.

CSM_168 Som anført i Figur 5 kan kortet, så snart det har verificeret ægtheden og gyldigheden af et hidtil ukendt certifikat, gemme dette certifikat til senere brug, så det ikke er

▼B

nødvendigt at verificere det pågældende certifikats ægthed, hvis kortet præsenteres for det igen. I stedet for at gemme hele certifikatet kan et kort vælge kun at gemme indholdet af certifikatteksten som angivet i afsnit 9.3.2.

10.3. **Ægthedskontrol af køretøjsenhed**

CSM_169 Køretøjsenheder og kort skal benytte den protokol til ægthedskontrol af køretøjsenhed, som beskrives i Figur 6, til at bekræfte køretøjsenhedens ægthed over for kortet. Ægthedskontrollen af køretøjsenheden giver takografkortet mulighed for udtrykkeligt at verificere, at køretøjsenheden er ægte. For at gøre dette benytter køretøjsenheden sin private nøgle til at underskrive en anmodning, som genereres af kortet.

CSM_170 Ud over kortets anmodning skal køretøjsenheden i underskriften medtage henvisningen til kortindehaveren hentet fra kortets certifikat.

Bemærk: Dette sikrer, at det kort, som køretøjsenheden bekræfter sig over for, er det samme kort, hvis certifikatkæde køretøjsenheden tidligere har verificeret.

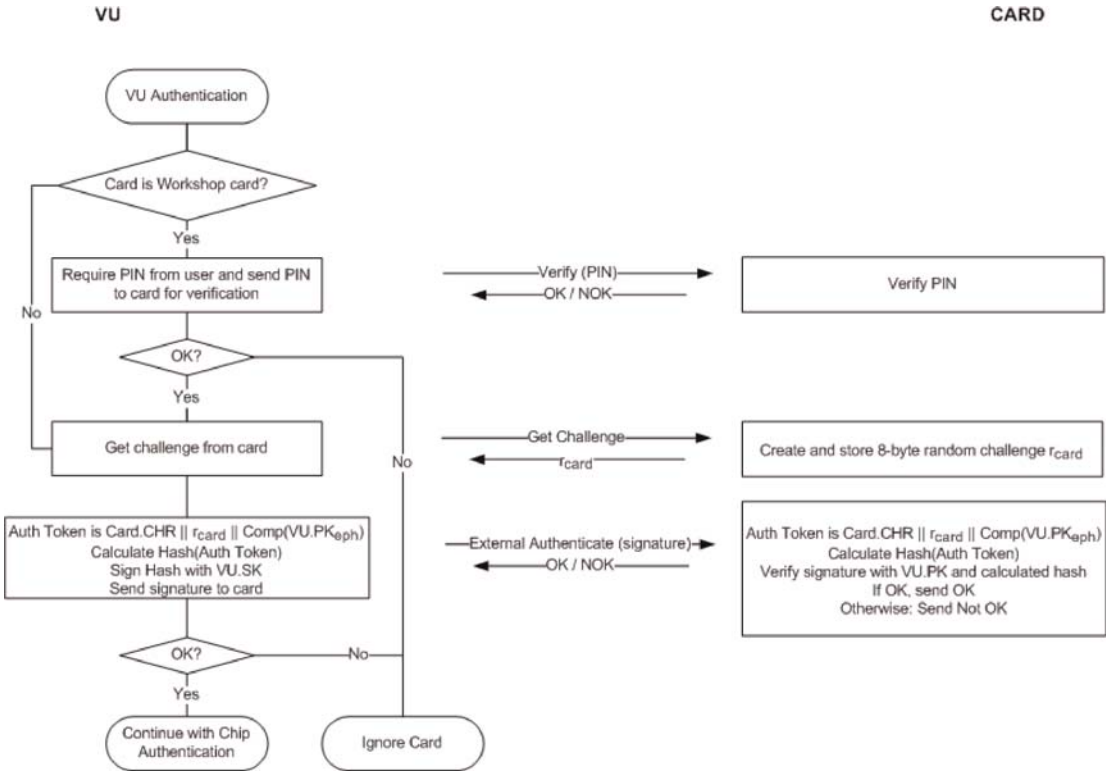
CSM_171 I underskriften medtager køretøjsenheden også identifikatoren for den midlertidige offentlige nøgle Comp($VU.PK_{eph}$), som køretøjsenheden bruger til sikker meddelelsesoverførsel under ægthedskontrol af en chip, der beskrives i afsnit 10.4.

Bemærk: Dette sikrer, at den køretøjsenhed, som et kort kommunikerer med under en sikker meddelelsessession, er den samme køretøjsenhed, som kortet har foretaget ægthedskontrol af.

▼B

Figur 6

Protokol til ægthedskontrol af køretøjsenhed



CSM_172 Hvis køretøjsenheden sender flere GET CHALLENGE-kommandoer under ægthedskontrollen af køretøjsenheden, returnerer kortet hver gang en ny tilfældig anmodning på 8 byte, men gemmer kun den seneste anmodning.

CSM_173 Underskriftsalgoritmen, som køretøjsenheden anvender til ægthedskontrol af køretøjsenheden, er ECDSA som specificeret i [DSS] ved hjælp af hash-algoritmen, der er knyttet til nøglestørrelsen af køretøjsenhedens VU_MA-nøglepar som specificeret i CSM_50. Underskriftsformatet skal være klartekst som specificeret i [TR-03111]. Køretøjsenheden sender den resulterende underskrift til kortet.

CSM_174 Efter modtagelsen af køretøjsenhedens underskrift i en EXTERNAL AUTHENTICATE-kommando gør kortet følgende:

— Beregner token for ægthedskontrol ved at sammenføre Card.CHR, kortets anmodning r_{card} og identifikatoren for køretøjsenhedens midlertidige offentlige nøgle $Comp(VU.PK_{eph})$

— Beregner hash-værdien over token for ægthedskontrollen ved hjælp af hash-algoritmen, der er sammenkædet med nøglestørrelsen af køretøjsenhedens VU_MA-nøglepar som specificeret i CSM_50

— Verificerer køretøjsenhedens underskrift ved at benytte ECDSA-algoritmen i kombination med VU.PK og den beregnede hash-værdi.

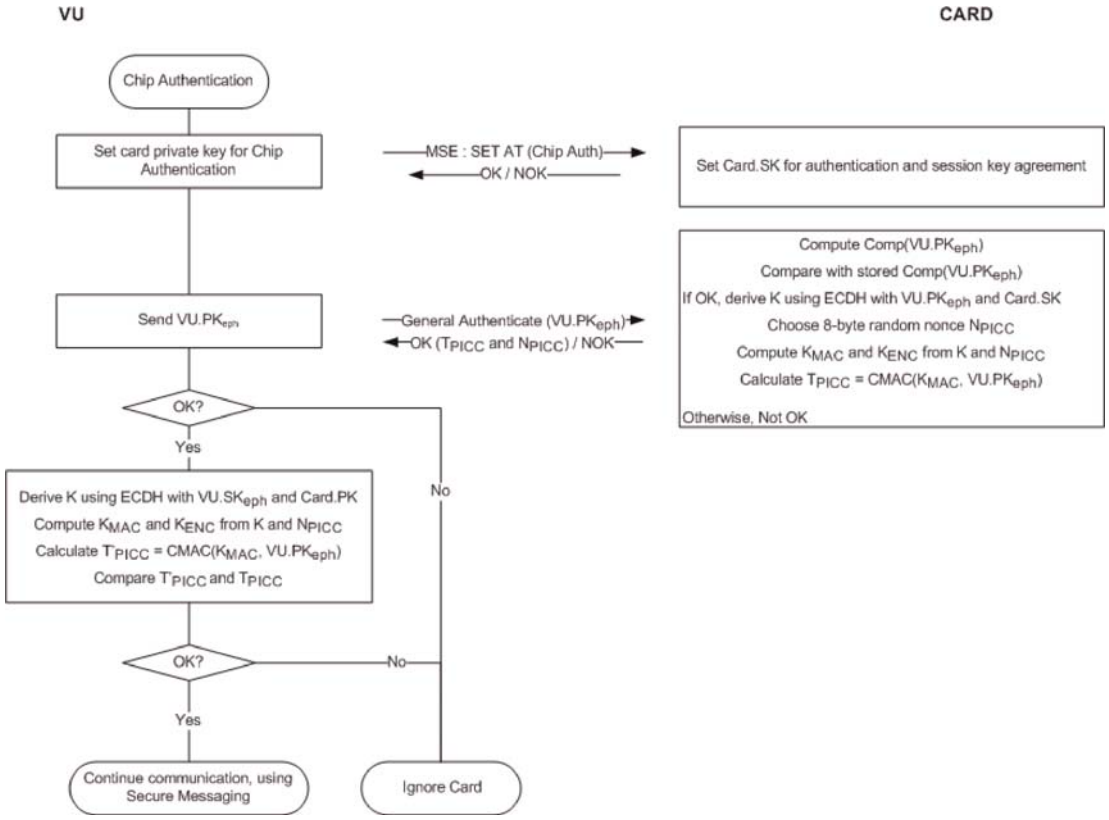
▼B

10.4. **Ægthedskontrol af chip og overenstemmelseskontrol af sessionsnøgle**

CSM_175 Køretøjsenheder og kort skal benytte den protokol til ægthedskontrol af chip, som beskrives i **Figur 7**, til bekræfte ægtheden af kortet over for køretøjsenheden. Ægthedskontrol af chippen giver køretøjsenheden mulighed for udtrykkeligt at verificere, at kortet er ægte.

Figur 7

Ægthedskontrol af chip og kontrol af sessionsnøgleoverensstemmelse



CSM_176 Køretøjsenheden og kortet gennemfører følgende trin:

1. Køretøjsenheden indleder ægthedskontrollen af chippen ved at sende kommandoen MSE: Set AT med angivelsen »Ægthedskontrol af chip med ECDH-algoritmen, der giver en AES-sessionsnøgle, som er sammenkædet med nøglestørrelsen på kortets Card_MA-nøglepar som specificeret i CSM_50«. Køretøjsenheden fastlægger størrelsen af kortets nøglepar ud fra kortets certifikat.

2. Køretøjsenheden sender det offentlige punkt $VU.PK_{eph}$ for sit midlertidige nøglepar til kortet. Som forklaret i CSM_164 genererede køretøjsenheden dette midlertidige nøglepar inden verifikationen af køretøjsenhedens certifikatkæde. Køretøjsenheden sendte identifikatoren for den midlertidige offentlige nøgle Comp($VU.PK_{eph}$) til kortet, og kortet gemte den.

▼B

3. Kortet beregner Comp(VU.PK_{eph}) ud fra VU.PK_{eph} og sammenligner med den gemte værdi for Comp(VU.PK_{eph}).

4. Ved hjælp af ECDH- algoritmen kombineret med kortets statiske private nøgle og køretøjsenhedens midlertidige offentlige nøgle, beregner kortet en hemmelig K.

5. Kortet vælger en tilfældig 8 byte stor engangsstreng N_{PICC} og bruger den til at udlede to AES-sessionsnøgler K_{MAC} og K_{ENC} af K. Se CSM_179.

6. Ved hjælp af K_{MAC} beregner kortet et token til ægthedskontrol ud fra identifikatoren for køretøjsenhedens midlertidige offentlige nøgle: T_{PICC} = CMAC(K_{MAC}, VU.PK_{eph}). Kortet sender N_{PICC} og T_{PICC} til køretøjsenheden.

7. Ved hjælp af ECDH-algoritmen kombineret med kortets statiske private nøgle og køretøjsenhedens midlertidige private nøgle beregner køretøjsenheden den samme hemmelige K, som kortet beregnede i trin 4.

8. VU'en udleder sessionsnøglerne K_{MAC} og K_{ENC} af K og N_{PICC}; se CSM_179.

9. VU'en verificerer token for ægthedskontrollen T_{PICC}.

CSM_177 I trin 3 ovenfor beregner kortet Comp(VU.PKeph) som x-koordinaten for det offentlige punkt i VU.PKeph.

CSM_178 I trin 4 og 7 ovenfor benytter kortet og køretøjsenheden ECKA-EG-algoritmen som defineret i [TR-03111].

CSM_179 I trin 5 og 8 ovenfor benytter kortet og køretøjsenheden nøgleudledningsfunktionen for AES-sessionsnøgler, som defineres i [TR-03111], med følgende præciseringer og ændringer:

— Tællerens værdi er '00 00 00 01' for K_{ENC} og '00 00 00 02' for K_{MAC}.

— Den valgfrie engangsstreng *r* skal anvendes og skal være lig med N_{PICC}.

— Til udledning af 128-bit AES-nøgler benyttes hash-algoritmen SHA-256.

— Til udledning af 192-bit AES-nøgler benyttes hash-algoritmen SHA-384.

— Til udledning af 256-bit AES-nøgler benyttes hash-algoritmen SHA-512.

Sessionsnøglernes længde (dvs. længden, hvor hash-værdien trunkeres) sammenkædes med størrelsen af Card_MA-nøgleparret som specificeret i CSM_50.

▼B

CSM_180 I trin 6 og 9 ovenfor benytter kortet og køretøjsenheden AES-algoritmen i CMAC-tilstand som specificeret i [SP 800-38B]. Længden af T_{PICC} kædes sammen med længden af AES-sessionsnøglerne som specificeret i CSM_50.

10.5. **Sikker meddelelsesoverførsel**

10.5.1 *Generelt*

CSM_181 Alle kommandoer og svar, der udveksles mellem en køretøjsenhed og et takografkort efter vellykket ægthedskontrol af chippen og frem til afslutningen af sessionen, skal beskyttes ved hjælp af sikker meddelelsesoverførsel.

CSM_182 Undtagen ved læsning af en fil med adgangsbetingelsen SM-R-ENC-MAC-G2 (se tillæg 2, afsnit 4) skal sikker meddelelsesoverførsel anvendes i tilstanden »Kun ægthedskontrol«. I denne tilstand tilføjes en kryptografisk kontrolsum (også betegnet MAC) til alle kommandoer og svar for at sikre meddelelsens ægthed og integritet.

CSM_183 Ved læsning fra en fil med adgangsbetingelsen SM-R-ENC-MAC-G2 skal sikker meddelelsesoverførsel anvendes i tilstanden »Krypter-derefter-autentificer«, dvs. svardataene krypteres først for at sikre meddelelsens fortrolighed, og herefter beregnes der en MAC ud fra de formaterede krypterede data for at garantere ægtheden og integriteten.

CSM_184 Sikker meddelelsesoverførsel anvender AES som defineret i [AES] sammen med sessionsnøglerne K_{MAC} og K_{ENC}, for hvilke der blev foretaget overensstemmelseskontrol under ægthedskontrol af chippen.

CSM_185 Et ikke underskrevet heltal skal bruges som sendefrekvenstæller (SSC) for at forhindre replay-angreb. Sendefrekvenstællerens størrelse er lig med AES-blokstørrelsen, dvs. 128 bit. Sendefrekvenstælleren skal være i MSB-first-format. Sendefrekvenstælleren initialiseres til nul (dvs '00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00'), når den sikre meddelelsesoverførsel indledes. Sendefrekvenstælleren forøges trinvist hver gang, inden der genereres en kommando- eller et svar-APDU, hvilket vil sige, at eftersom startværdien for sendefrekvenstælleren i en SM-session er 0, vil værdien af sendefrekvenstælleren i den første kommando være 1. Værdien i sendefrekvenstælleren for det første svar vil være 2.

CSM_186 Til kryptering af meddelelser skal K_{ENC} anvendes sammen med AES i blokkædningsfunktionstilstand (CBC) som defineret i [ISO 10116] med en indskudt parameter $m = 1$ og en initialiseringsvektor $SV = E(K_{ENC}, SSC)$, dvs. den aktuelle værdi af sendesekvenstælleren krypteret med K_{ENC}.

CSM_187 Ved ægthedskontrol af meddelelser anvendes K_{MAC} sammen med AES i CMAC-tilstand som specificeret i [SP 800-38B]. Længden af MAC'en sammenkædes med længden af AES-sessionsnøglerne som specificeret i CSM_50. Sendesekvenstælleren skal medtages i MAC'en ved at indsætte den på forhånd, inden ægtheden af datagrammet bekræftes.

▼B

10.5.2 *Struktur af sikker meddelelse*

CSM_188 Sikker meddelelsesoverførsel må udelukkende benytte dataobjekter til sikker meddelelsesoverførsel (se [ISO 7816-4]), som står opført i Tabel 5. I alle meddelelser skal disse dataobjekter anvendes i den rækkefølge, der angives i denne tabel.

Tabel 5

Dataobjekter til sikker meddelelsesoverførsel

Navn på dataobjekt	Mærkat	Tilstedeværelse (O)bligatorisk, (B)etinget eller (F)orbudt i	
		Kommandoer	Svar
Ordinær værdi ikke kodet i BER-TLV	'81'	B	B
Ordinær værdi kodet i BER-TLV, men ikke inklusive SM-dataobjekter	'B3'	B	B
Indikator med udfyldningsindhold efterfulgt af kryptogram, ordinær værdi ikke kodet i BER-TLV	'87'	B	B
Beskyttet Le	'97'	B	F
Behandlingsstatus	'99'	F	O
Kryptografisk kontrolsum	'8E'	O	O

Bemærk: Som angivet i tillæg 2 kan takografkort understøtte kommandoerne READ BINARY og UPDATE BINARY med en ulige INS-byte ('B1' hhv. 'D7'). Disse kommandovarianter skal bruges til at læse og ajourføre filer på 32 768 byte eller mere. Hvis man benytter en sådan variant, skal man anvende et dataobjekt med mærkatet 'B3' i stedet for et objekt med mærkatet '81'. Se tillæg 2 for flere oplysninger.

CSM_189 Alle SM-dataobjekter skal kodes i DER TLV som specificeret i [ISO 8825-1]. Denne kodning medfører følgende mærkat-længde-værdi-struktur (TLV-struktur):

Mærkat: Mærkaten kodet i en eller to oktetter med angivelse af indholdet.

Længde: Længden kodet som et ikke underskrevet heltal i en, to eller tre oktetter, hvilket giver en maksimal længde på 65 535 oktetter. Det mindste antal oktetter skal benyttes.

Værdi: Værdien kodet i nul eller flere oktetter

CSM_190 APDU'er, der er beskyttet med sikker meddelelsesoverførsel, oprettes som følger:

— Kommandoheaderen skal medtages i MAC-beregningen, og derfor anvendes værdien '0C' til klassebyten CLA.

▼B

— Som specificeret i tillæg 2 skal alle INS-byte være lige, med ulige INS-byte til kommandoerne READ BINARY og UPDATE BINARY som en mulig undtagelse.

— Den faktiske værdi af Lc vil blive ændret til Lc' efter brugen af sikker meddelelsesoverførsel.

— Datafeltet består af SM-dataobjekter.

— I den beskyttede kommando-APDU sættes den nye Le-byte til '00'. Om nødvendigt medtages et dataobjekt '97' i datafeltet for at formidle den oprindelige værdi af Le.

CSM_191 Alle dataobjekter, der skal krypteres, udfyldes i henhold til [ISO 7816-4] med udfyldningsindikatoren '01'. Ved beregningen af MAC'en skal hvert dataobjekt i APDU'en ligeledes udfyldes separat i henhold til [ISO 7816-4].

Bemærk: Udfyldning til sikker meddelelsesoverførsel udføres altid af det sikre meddelelseslag, ikke af CMAC- eller CBC-algoritmerne.

Sammenfatning og eksempler

En kommando-APDU med anvendt sikker meddelelsesoverførsel vil have følgende struktur afhængigt af alternativet for den respektive ikke-sikrede kommando (DO står for dataobjekt):

Alternativ 1:	CLA INS P1 P2 || Lc' || DO '8E' || Le
Alternativ 2:	CLA INS P1 P2 || Lc' || DO '97' || DO'8E' || Le
Alternativ 3 (lige INS-byte):	CLA INS P1 P2 || Lc' || DO '81' || DO'8E' || Le
Alternativ 3 (ulige INS-byte):	CLA INS P1 P2 || Lc' || DO 'B3' || DO'8E' || Le
Alternativ 4 (lige INS-byte):	CLA INS P1 P2 || Lc' || DO '81' || DO'97' || DO'8E' || Le
Alternativ 4 (ulige INS-byte):	CLA INS P1 P2 || Lc' || DO 'B3' || DO'97' || DO'8E' || Le

hvor Le = '00' eller '00 00' afhængigt af, hvorvidt der benyttes felter med kort længde eller felter med udvidet længde; se [ISO 7816-4].

En svar-APDU med anvendt sikker meddelelsesoverførsel vil have følgende struktur afhængigt af alternativet for det respektive ikke-sikrede svar:

Alternativ 1 eller 3:	DO '99' || DO '8E' || SW1SW2
Alternativ 2 eller 4 (lige INS-byte) med kryptering:	DO '81' || DO '99' || DO '8E' || SW1SW2
Alternativ 2 eller 4 (lige INS-byte) uden kryptering:	DO '87' || DO '99' || DO '8E' || SW1SW2
Alternativ 2 eller 4 (ulige INS-byte) uden kryptering:	DO 'B3' || DO '99' || DO '8E' || SW1SW2

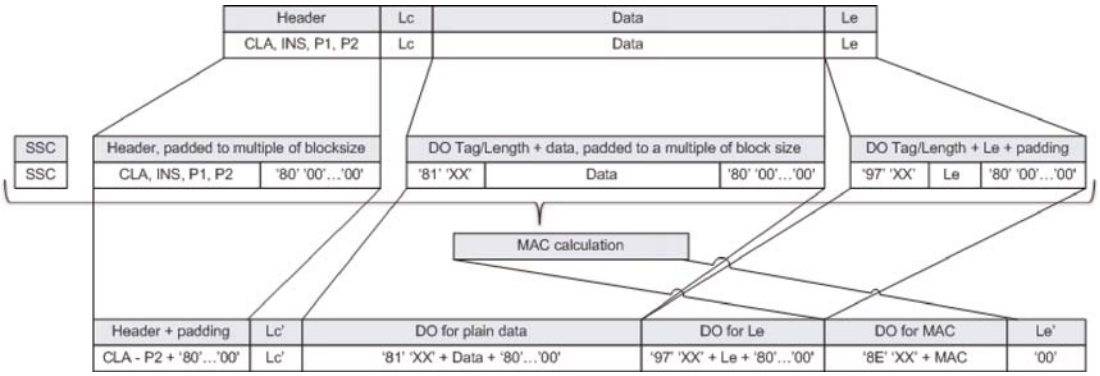
Bemærk: Alternativ 2 eller 4 (ulige INS-byte) med kryptering anvendes aldrig i kommunikationen mellem en køretøjsenhed og et kort.

▼B

Herunder gives tre eksempler på APDU-transformationer for kommandoer med lige INS-kode. Figur 8 viser en autentificeret Alternativ 4-kommando-APDU, Figur 9 viser en autentificeret Alternativ 2-/Alternativ 4-svar-APDU, og Figur 10 viser en krypteret og autentificeret Alternativ 2-/Alternativ 4-svar-APDU.

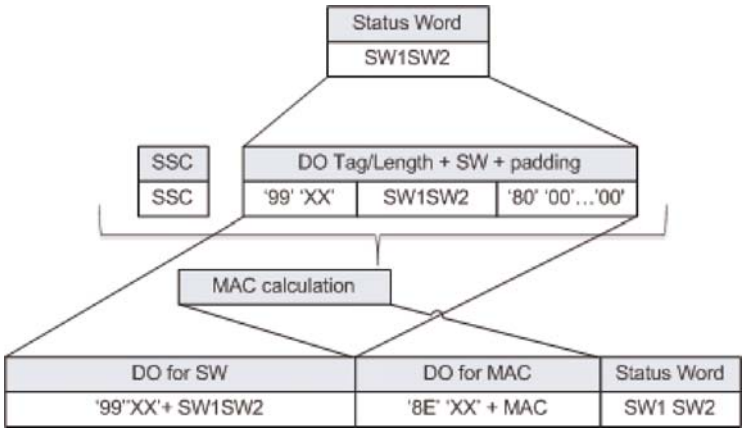
Figur 8

Transformation af en autentificeret Alternativ 4-kommando-APDU



Figur 9

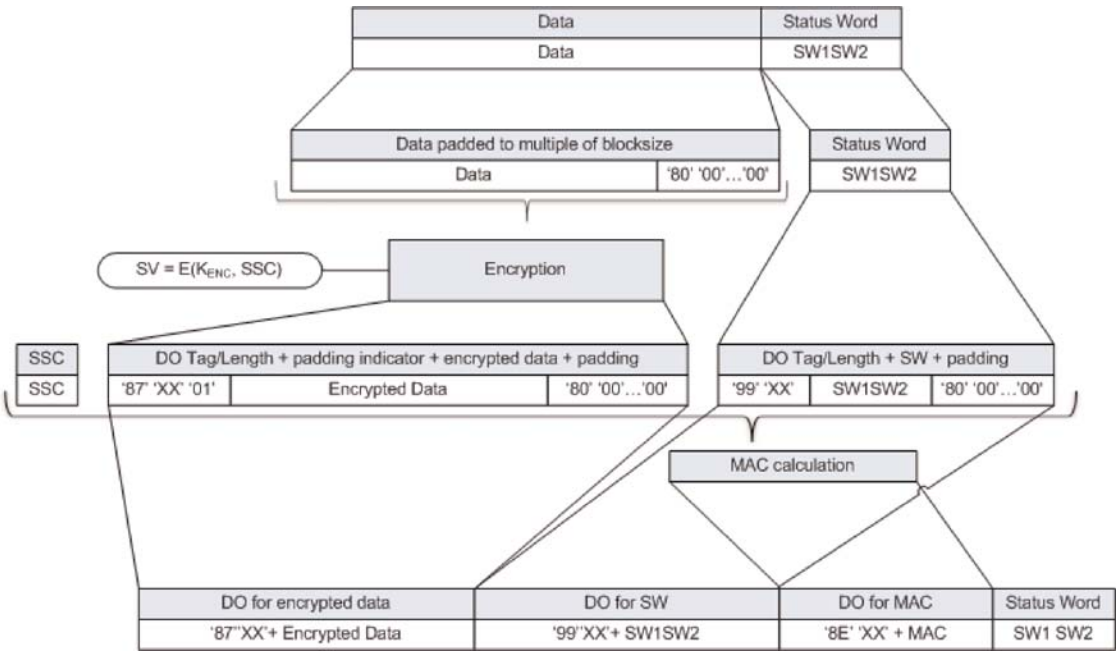
Transformation af en autentificeret Alternativ 1- / Alternativ 3-svar-APDU



▼B

Figur 10

Transformation af et krypteret og autentificeret Alternativ 2-/Alternativ 4-svar-APDU



10.5.3 *Afbrydelse af en sikker meddelelsesoverførselssession*

CSM_192 En køretøjsenhed afbryder en igangværende sikker meddelelsesoverførselssession, hvis, og kun hvis et af følgende forhold gør sig gældende:

— Den modtager en APDU med et svar i klartekst.

— Den konstaterer en fejl i den sikre meddelelsesoverførsel i en svar-APDU:

  — Et forventet dataobjekt i en sikker meddelelsesoverførsel mangler, rækkefølgen af dataobjekter er forkert, eller der er medtaget et ukendt dataobjekt.

  — Dataobjektet i en sikker meddelelsesoverførsel er forkert, f.eks. er MAC-værdien forkert, TLV-strukturen er forkert, eller udfyldingsindikatoren i mærkat '87' er ikke lig med '01'.

— Kortet sender en statusbyte, der viser, at det har konstateret en SM-fejl (se CSM_194).

— Grænsen for antallet af kommandoer og tilhørende svar inden for den aktuelle session er nået. For en bestemt køretøjsenhed defineres denne grænse af fabrikanten under hensyntagen til sikkerhedskravene for den anvendte hardware med et maksimum på 240 SM-kommandoer og tilhørende svar pr. session.

▼B

CSM_193 Et takografkort afbryder en igangværende sikker meddelelsesoverførselssession, hvis, og kun hvis et af følgende forhold gør sig gældende:

— Det modtager en APDU-kommando i klartekst.

— Det konstaterer en fejl i den sikre meddelelsesoverførsel i en kommando-APDU:

— Et forventet dataobjekt i en sikker meddelelsesoverførsel mangler, rækkefølgen af dataobjekter er forkert, eller der er medtaget et ukendt dataobjekt.

— Et dataobjekt i en sikker meddelelsesoverførsel er forkert, f.eks. er MAC-værdien forkert, eller TLV-strukturen er forkert.

— Strømmen afbrydes, eller enheden nulstilles.

— Køretøjsenheden vælger en applikation på kortet.

— Køretøjsenheden indleder processen med ægthedskontrol af køretøjsenheden.

— Grænsen for antallet af kommandoer og tilhørende svar inden for den aktuelle session er nået. For et bestemt kort defineres denne grænse af fabrikanten under hensyntagen til sikkerhedskravene for det anvendte hardware med et maksimum på 240 SM-kommandoer og tilhørende svar pr. session.

CSM_194 Vedrørende SM-fejlhåndtering foretaget af et takografkort:

— Hvis der mangler visse dataobjekter til sikker meddelelsesoverførsel i en kommando-APDU, rækkefølgen af dataobjekter er forkert, eller der er medtaget ukendte dataobjekter, svarer et takografkort med statusbyte '69 87'.

— Hvis et dataobjekt i en kommando-APDU ved sikker meddelelsesoverførsel er forkert, svarer et takografkort med statusbyte '69 88'.

I dette tilfælde returneres de pågældende statusbyte uden brug af SM.

CSM_195 Hvis en sikker meddelelsesoverførselssession mellem en køretøjsenhed og et takografkort afbrydes, ødelægger køretøjsenheden og takografen

— de gemte sessionsnøgler på en sikker måde

— og opretter øjeblikkelig en ny sikker meddelelsesoverførselssession som beskrevet i afsnit 10.2-10.5.

CSM_196 Hvis køretøjsenheden af en eller anden grund beslutter at genstarte den gensidige ægthedskontrol over for et isat kort, genstartes processen med verifikation af kortets certifikatkæde som beskrevet i afsnit 10.2 og fortsætter som beskrevet i afsnit 10.2-10.5.

▼B

11. SAMMENKOBLING AF KØRETØJSENHED OG EKSTERNT GNSS-UDSTYR, GENSIDIG ÆGTHEDSKONTROL OG SIKKER MEDDELELSESOVERFØRSEL

11.1. **Generelt**

CSM_197 GNSS-udstyret, som en køretøjsenhed bruger til at fastslå sin position, kan være intern (dvs. indbygget i køretøjsenhedens hus og kan ikke afmonteres), eller den kan være et eksternt modul. I førstnævnte tilfælde er der ikke behov for at standardisere den interne kommunikation mellem GNSS-udstyret og køretøjsenheden, og kravene i dette kapitel finder ikke anvendelse. I sidstnævnte tilfælde skal kommunikationen mellem køretøjsenheden og det eksterne GNSS-udstyr standardiseres og beskyttes som beskrevet i dette kapitel.

CSM_198 Sikker kommunikation mellem en køretøjsenhed og eksternt GNSS-udstyr finder sted på samme måde som sikker kommunikation mellem en køretøjsenhed og et takografkort, hvor det eksterne GNSS-udstyr (EGF) overtager kortets rolle. Alle krav, der nævnes i kapitel 10 for takografkort, skal opfyldes af en EGF under hensyntagen til de afvigelser, præciseringer og tilføjelser, der nævnes i dette kapitel. Det gælder navnlig, at gensidig verifikation af certifikatkæden, ægthedskontrol af køretøjsenhed og chip udføres som beskrevet i afsnit 11.3 og 11.4.

CSM_199 Kommunikation mellem en køretøjsenhed og en EGF adskiller sig fra kommunikation mellem en køretøjsenhed og et kort ved, at en køretøjsenhed og en EGF skal sammenkobles en gang på et værksted, inden køretøjsenheden og EGF'en kan udveksle GNSS-baserede data under normal drift. Sammenkoblingsprocessen beskrives i afsnit 11.2.

CSM_200 Ved kommunikation mellem en køretøjsenhed og en EGF skal APDU-kommandoer og -svar baseret på [ISO 7816-4] og [ISO 7816-8] benyttes. Den præcise struktur for disse APDU'er defineres i tillæg 2 til dette bilag.

11.2. **Sammenkobling af køretøjsenhed og eksternt GNSS-udstyr**

CSM_201 En køretøjsenhed og en EGF i et køretøj skal sammenkobles af et værksted. Kun en sammenkoblet køretøjsenhed og EGF skal kunne kommunikere ved normal drift.

CSM_202 Sammenkoblingen af køretøjsenhed og en EGF må kun være mulig, når køretøjsenheden er i kalibreringstilstand. Koblingen skal indledes af køretøjsenheden.

CSM_203 Et værksted kan til enhver tid sammenkoble en køretøjsenhed med en anden EGF eller med den samme EGF. Under gensammenkoblingen skal køretøjsenheden ødelægge det eksisterende EGF_MA-certifikat i sin hukommelse på en sikker måde og gemme EGF_MA-certifikatet for den EGF, som den skal kobles sammen med.

CSM_204 Et værksted kan til enhver tid sammenkoble eksternt GNSS-udstyr med en anden køretøjsenhed eller med den samme køretøjsenhed. Under gensammenkoblingen skal EGF'en ødelægge det eksisterende VU_MA-certifikat i sin hukommelse på en sikker måde og gemme VU_MA-certifikatet for den køretøjsenhed, som den skal kobles sammen med.

▼B

11.3. **Gensidig certifikatkædeverifikation**

11.3.1 *Generelt*

CSM_205 Gensidig certifikatkædeverifikation mellem en køretøjsenhed og en EGF må kun finde sted under sammenkoblingen af køretøjsenheden og EGF'en på et værksted. Under normal drift for en sammenkoblet køretøjsenhed og EGF verificeres der ingen certifikater. I stedet har køretøjsenheden og EGF'en tillid til de certifikater, som de har gemt under sammenkoblingen efter at have kontrolleret den midlertidige gyldighed af disse certifikater. Køretøjsenheden og EGF'en accepterer ikke andre certifikater til beskyttelse af kommunikationen mellem køretøjsenheden og EGF'en under normal drift.

11.3.2 *Under sammenkobling af køretøjsenhed og EGF*

CSM_206 Under sammenkoblingen med en EGF benytter en køretøjsenhed den protokol, der fremgår af Figur 4 (afsnit 10.2.1), til verifikation af det eksterne GNSS-udstyrs certifikatkæde.

Bemærkninger til Figur 4 i denne sammenhæng:

— Kommunikationskontrol ligger uden for dette tillægs område. En EGF er imidlertid ikke et intelligent kort, og derfor vil køretøjsenheden formentlig ikke sende en Reset-kommando for at indlede kommunikationen og vil ikke modtage en ATR.

— Kortcertifikaterne og de offentlige nøgler, der nævnes i figuren, fortolkes som EGF'ens certifikater og offentlige nøgler til gensidig ægthedskontrol. I afsnit 9.1.6 betegnes disse som EGF_MA.

— Card.CA-certifikaterne og de offentlige nøgler, som nævnes i figuren, fortolkes som MSCA'ens certifikater og offentlige nøgler til underskrift af EGF-certifikater. I afsnit 9.1.3 betegnes disse som MSCA_VU_EGF.

— Card.CA.EUR-certifikatet, der nævnes i figuren, skal fortolkes som det europæiske rodcertifikat, der angives i MSCA_VU-EFT-certifikatets CAR.

— Card.Link-certifikatet, der nævnes i figuren, skal fortolkes som EGF'ens forbindelsescertifikat, hvis dette findes. Som beskrevet i afsnit 9.1.2 er dette et forbindelsescertifikat til et europæisk rodnøglepar, som er oprettet af ERCA'en og underskrevet af den tidligere europæiske private nøgle.

— Card.Link.EUR-certifikatet, der nævnes i figuren, er det europæiske rodcertifikat, der angives i Card.Link-certifikatets CAR.

— I stedet for `cardExtendedSerialNumber`, læser køretøjsenheden `sensorGNSSserialNumber` fra elementærfilen ICC.

— I stedet for at vælge takograf-AID'en vælger køretøjsenheden EGF-AID'en.

— »Ignore Card« fortolkes som »Ignore EGF«.

▼B

CSM_207 Når køretøjsenheden har verificeret EGF_MA-certifikatet, gemmer den dette certifikat til brug under normal drift; se afsnit 11.3.3.

CSM_208 Under sammenkoblingen med en køretøjsenhed benytter eksternt GNSS-udstyr den protokol, der beskrives i Figur 5 (afsnit 10.2.2) til verifikation af køretøjsenhedens certifikatkæde.

Bemærkninger til Figur 5 i denne sammenhæng:

— Køretøjsenheden genererer en nyt midlertidigt nøglepar ved hjælp af domæneparametrene i EGF-certifikatet.

— Køretøjsenhedens certifikater og de offentlige nøgler, der nævnes i figuren, er dem, der anvendes til gensidig ægthedskontrol. I afsnit 9.1.4 betegnes disse som VU_MA.

— VU.CA-certifikaterne og de offentlige nøgler, der nævnes i figuren, er dem, der anvendes til underskrift af køretøjsenhedscertifikater og certifikater for eksternt GNSS-udstyr. I afsnit 9.1.3 betegnes disse som MSCA_VU_EGF.

— VU.CA.EUR-certifikatet, der nævnes i figuren, er det europæiske rodcertifikat, der angives i VU.CA-certifikatets CAR.

— VU.Link-certifikatet, der nævnes i figuren, er køretøjsenhedens linkcertifikat, hvis dette findes. Som beskrevet i afsnit 9.1.2 er dette et forbindelsescertifikat til et europæisk rodnøglepar, som er oprettet af ERCA'en og underskrevet af den tidligere europæiske private nøgle.

— VU.Link.EUR-certifikatet, der nævnes i figuren, er det europæiske rodcertifikat, der angives i VU.Link-certifikatets CAR.

CSM_209 Som en afvigelse fra krav CSM_167 skal en EGF anvende GNSS'ens klokkeslæt til at verificere den tidsmæssige gyldighed af ethvert fremlagt certifikat.

CSM_210 Når det eksterne GNSS-udstyr har verificeret VU_MA-certifikatet, gemmer den dette certifikat til brug under normal drift; se afsnit 11.3.3.

11.3.3 *Under normal drift*

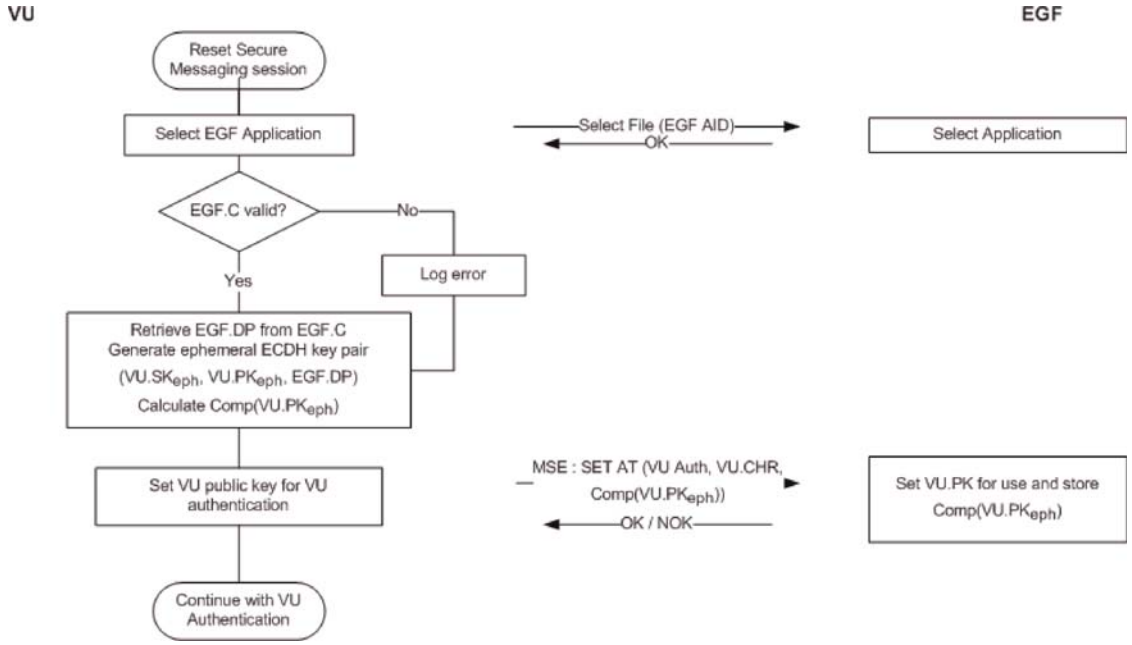
CSM_211 Under normal drift benytter en køretøjsenhed og en EGF den protokol, der beskrives i Figur 11 til verifikation af den tidsmæssige gyldighed af de gemte EGF_MA- og VU_MA-certifikater og til at indstille den offentlige VU_MA-nøgle til efterfølgende ægthedskontrol af køretøjsenheden. Der foretages ingen yderligere gensidig verificering af certifikatkæderne under normal drift.

Bemærk, at Figur 11 i alt væsentligt består af de første trin, der beskrives i Figur 4 og Figur 5. Igen skal man bemærke, at eftersom en EGF ikke er et intelligent kort, vil køretøjsenheden formentlig ikke sende en Reset-kommando for at indlede kommunikationen og vil ikke modtage en ATR. Under alle omstændigheder ligger dette uden for dette tillægs område.

▼B

Figur 11

Gensidig verificering af et certifikats tidsmæssige gyldighed ved normal drift af køretøjsenhed og EGF



CSM_212 Som vist i Figur 11 logger køretøjsenheden en fejl, hvis EGF_MA-certifikatet ikke længere er gyldigt. Den gensidige ægthedskontrol, nøgleoverensstemmelse og den efterfølgende kommunikation via sikker meddelelsesoverførsel foregår som normalt.

11.4. **Ægthedskontrol af køretøjsenhed og chip samt sessionsnøgleoverensstemmelse**

CSM_213 Ægthedskontrol af køretøjsenhed og chip og kontrol af sessionsnøgleoverensstemmelse mellem en køretøjsenhed og en EGF foregår under sammenkobling, og når en sikker meddelelsesoverførselssession genetableres under normal drift. Køretøjsenheden og EGF'en udfører de processer, der beskrives i afsnit 10.3 og 10.4. Alle krav i disse afsnit finder anvendelse.

11.5. **Sikker meddelelsesoverførsel**

CSM_214 Alle kommandoer og svar, der udveksles mellem en køretøjsenhed og eksternt GNSS-udstyr efter vellykket ægthedskontrol af chippen og frem til afslutningen af sessionen, skal beskyttes ved hjælp af sikker meddelelsesoverførsel i tilstanden »Kun ægthedskontrol«. Alle krav i afsnit 10.5 finder anvendelse.

CSM_215 Hvis en sikker meddelelsesoverførselssession mellem en køretøjsenhed og en EGF afbrydes, etablerer køretøjsenheden øjeblikkelig en ny sikker meddelelsesoverførselssession som beskrevet i afsnit 11.3.3 og 11.4.

12. PARRING AF OG KOMMUNIKATION MELLEM KØRETØJSENHED OG BEVÆGELSESSENSOR

12.1. **Generelt**

CSM_216 En køretøjsenhed og en bevægelsessensor kommunikerer ved hjælp af den interfaceprotokol, der specificeres i [ISO 16844-3], under parring og ved normal drift med de ændringer, der beskrives i dette kapitel og i afsnit 9.2.1.

▼B

Bemærk: Læsere af dette kapitel formodes at være fortrolige med indholdet af [ISO 16844-3].

12.2. **Parring af køretøjsenhed og bevægelsessensor ved hjælp af forskellige nøglegenerationer**

Som forklaret i afsnit 9.2.1 udskiftes bevægelsessensorens hovednøgle og alle tilhørende nøgler regelmæssigt. Dette betyder, at op til tre bevægelsessensor-relaterede AES-nøgler K_{M-WC} (af på hinanden følgende nøglegenerationer) er til stede på værkstedskortene. Tilsvarende kan op til tre forskellige AES-baserede datakrypteringer (baseret på hinanden følgende generationer af bevægelsessensorens hovednøgle K_M) være til stede i bevægelsessensorer. En køretøjsenhed indeholder kun en bevægelsessensor-relateret nøgle $K_{M-VU.}$

CSM_217 En køretøjsenhed af anden generation og en bevægelsessensor af anden generation parres på følgende måde (sammenlign med tabel 6 i [ISO 16844-3]):

1. Et værkstedskort af anden generation sættes i køretøjsenheden, og køretøjsenheden tilsluttes bevægelsessensoren.

2. Køretøjsenheden læser alle tilgængelige K_{M-WC}-nøgler fra værkstedskortet, undersøger deres nøgleversionsnumre og vælger den, der passer til versionsnummeret for køretøjsenhedens K_{M-VU}-nøgle. Hvis der ikke er nogen passende K_{M-WC}-nøgle til stede på værkstedskortet, afbryder køretøjsenheden parringsprocessen og viser en relevant fejlmeddelelse til indehaveren af værkstedskortet.

3. Køretøjsenheden beregner bevægelsessensorens hovednøgle K_M ud fra K_{M-VU} og K_{M-WC} og identifikationsnøglen K_{ID} ud fra K_M som specificeret i afsnit 9.2.1.

4. Køretøjsenheden sender instruktionen om at indlede parringsprocessen til bevægelsessensoren, som beskrevet i [ISO 16844-3], og krypterer det serienummer, den modtager fra bevægelsessensoren med identifikationsnøglen $K_{ID.}$ Køretøjsenheden sender det krypterede serienummer tilbage til bevægelsessensoren.

5. Bevægelsessensoren sammenligner det krypterede serienummer med hver af krypteringerne af serienummeret, som den har lagret internt. Hvis den finder et, der passer, bekræftes køretøjsenhedens ægthed. Bevægelsessensoren noterer den generation af K_{ID}, som køretøjsenheden anvender, og returnerer den passende krypterede version af sin parringsnøgle, dvs. den kryptering, der blev oprettet med den samme generation af $K_{M.}$

6. Køretøjsenheden dekrypterer parringsnøglen med K_{M}, genererer en sessionsnøgle $K_{S,}$ krypterer den med parringsnøglen og sender resultatet til bevægelsessensoren. Bevægelsessensoren dekrypterer K_S.

7. Køretøjsenheden samler parringsoplysningerne som defineret i [ISO 16844-3], krypterer oplysningerne med parringsnøglen og sender resultatet til bevægelsessensoren. Bevægelsessensoren dekrypterer parringsoplysningerne.

8. Bevægelsessensoren krypterer de modtagne parringsoplysninger med den modtagne K_S og returnerer dem til køretøjsenheden. Køretøjsenheden verificerer, at parringsoplysningerne er det samme oplysninger, som

▼B

køretøjsenheden sendte til bevægelsessensoren i det foregående trin. Hvis dette er tilfældet, beviser det, at bevægelsessensoren brugte den samme K_S som køretøjsenheden og dermed i trin 5 sendte sin parringsnøgle krypteret med den korrekte generation af K_M. Dermed er bevægelsessensorens ægthed bekræftet.

Bemærk, at trin 2 og 5 er forskellige fra standardprocessen i [ISO 16844-3], mens de øvrige trin er standard.

Eksempel: Det forudsættes, at en parring finder sted i ERCA- (3) certifikatets første gyldighedsår; se Figur 2 i afsnit 9.2.1.2. Det

— forudsættes desuden, at bevægelsessensoren blev udstedt i ERCA- (1) certifikatets sidste gyldighedsår. Den indeholder derfor følgende nøgler og data:

  — $N_s[1]$: dens serienummer krypteret med generation 1 af K_{ID}

  — $N_s[2]$: dens serienummer krypteret med generation 2 af K_{ID}

  — $N_s[3]$: dens serienummer krypteret med generation 3 af K_{ID}

  — $K_P[1]$: dens generation 1-parringsnøgle ([1]) krypteret med generation 1 af K_M

  — $K_P[2]$: dens generation 2-parringsnøgle krypteret med generation 2 af K_M

  — $K_P[3]$: dens generation 3-parringsnøgle krypteret med generation 3 af K_M.

— Det forudsættes, at værkstedskortet blev udstedt i ERCA- (3) certifikatets første gyldighedsår. Det vil derfor indeholde generation 2 og generation 3 af K_{M-WC}-nøglen.

— Det forudsættes, at køretøjsenheden er en generation 2-køretøjsenhed, der indeholder generation 2 af K_{M-VU}.

I dette tilfælde vil følgende ske i trin 2-5:

— Trin 2: Køretøjsenheden læser generation 2 og generation 3 af K_{M-WC} fra værkstedskortet og undersøger deres versionsnumre.

— Trin 3: Køretøjsenheden kombinerer generation 2-K_{M-WC} med dens K_{M-VU} for at beregne K_M og K_{ID}.

— Trin 4: Køretøjsenheden krypterer det serienummer, den modtager fra bevægelsessensoren med K_{ID}.

— Trin 5: Bevægelsessensoren sammenligner de modtagne data med $N_s[1]$ og finder ikke nogen, der passer. Herefter sammenligner den dataene med $N_s[2]$ og finder en værdi, der passer. Den konkluderer, at køretøjsenheden er en generation 2-køretøjsenhed og returnerer derfor $K_P[2]$.

([1]) Bemærk, at parringsnøgler af generation 1, generation 2 og generation 3 rent faktisk kan være den samme nøgle eller kan være tre forskellige nøgler med forskellig længde som forklaret i CSM_117.

▼B

12.3. **Parring af og kommunikation mellem køretøjsenhed og bevægelsessensor ved hjælp af AES**

CSM_218 Som anført i Tabel 3 i afsnit 9.2.1 skal alle nøgler, der anvendes til parring af en (andengenerations) køretøjsenhed og en bevægelsessensor og i den efterfølgende kommunikation være AES-nøgler frem for TDES-nøgler med dobbelt længde som specificeret i [ISO 16844-3]. Disse AES-nøgler kan have en længde på 128, 192 eller 256 bit. Eftersom blokstørrelsen i en AES er 16 byte, skal længden af en krypteret meddelelse være et multiplum af 16 byte sammenlignet med 8 byte for TDES. Desuden vil nogle af disse meddelelser blive brugt til at transportere AES-nøgler, hvis længde kan være 128, 192 eller 256 bit. Derfor skal antallet af databyte pr. instruktion i tabel 5 i [ISO 16844-3] ændres som vist i Tabel 6:

Tabel 6

Antal databyte i klartekst og krypteret form pr. instruktion defineret i [ISO 16844-3]

Instruktion	Anmodning/svar	Beskrivelse af data	Antal databyte i klartekst i henhold til [ISO 16844-3]	Antal databyte i klartekst ved brug af AES-nøgler	Antal krypterede databyte ved brug af AES-nøgler med en bitlængde på		
					128	192	256
10	anmodning	Ægthedskontroldata + filnummer	8	8	16	16	16
11	svar	Ægthedskontroldata + filindhold	16 eller 32, afhænger af filen	16 eller 32, afhænger af filen	16/32	16/32	16/32
41	anmodning	MoS-serienummer	8	8	16	16	16
41	svar	Parringsnøgle	16	16/24/32	16	32	32
42	anmodning	Sessionsnøgle	16	16/24/32	16	32	32
43	anmodning	Parringsoplysninger	24	24	32	32	32
50	svar	Parringsoplysninger	24	24	32	32	32
70	anmodning	Ægthedskontroldata	8	8	16	16	16
80	svar	MoS-tællerværdi + ægthedskontroldata	8	8	16	16	16

CSM_219 De parringsoplysninger, der fremsendes i instruktion 43 (VU-anmodning) og 50 (MoS-svar), samles som specificeret i afsnit 7.6.10 i [ISO 16844-3], bortset fra at AES-algoritmen skal benyttes i stedet for TDES-algoritmen i krypteringsordningen til parringsdataene, hvilket betyder to AES-krypteringer, og idet man anvender den udfyldning, der specificeres i CSM_220, så den passer med AES-blokstørrelsen. Nøglen K'_P, der benyttes til denne kryptering, genereres på følgende måde:

— Hvis parringsnøglen K_P er 16 byte lang: $K'_P = K_P$ XOR $(N_s||N_s)$

▼B

— Hvis parringsnøglen K_P er 24 byte lang: $K'_p = K_P$ XOR $(N_s||N_s||N_s)$

— Hvis parringsnøglen K_P er 32 byte lang: $K'_p = K_P$ XOR $(N_s||N_s||N_s||N_s)$

hvor N_s er bevægelsessensorens serienummer på 8 byte.

CSM_220 Hvis datalængden af klarteksten (ved brug af AES-nøgler) ikke er et multiplum af 16 byte, skal udfyldningsmetode 2, som defineres i [ISO 9797-1], benyttes.

Bemærk: I [ISO 16844-3] er antallet af klartekstdatabyte altid et multiplum af 8, og der er således ikke behov for udfyldning, når man bruger TDES. Definitionen af data og meddelelser i [ISO 16844-3] ændres ikke af denne del i dette tillæg, så der bliver behov for at bruge udfyldning.

CSM_221 Til instruktion 11, og hvis mere end en datablok skal krypteres, skal blokkædningsmetoden benyttes som defineret i [ISO 10116] med en indskudt parameter *m* = 1. Den anvendte IV skal være

— Til instruktion 11: ægthedskontrolblokken på 8 byte, som specificeres i afsnit 7.6.3.3 i [ISO 16844-3], udfyldt ved hjælp af udfyldningsmetode 2, som defineres i [ISO 9797-1]; se også afsnit 7.6.5 og 7.6.6 i [ISO 16844-3].

— Til alle andre instruktioner, hvor der overføres mere end 16 byte, som specificeret i Tabel 6: '00' {16}, dvs. 16 byte med den binære værdi 0.

Bemærk: Som vist i afsnit 7.6.5 og 7.6.6 i [ISO 16844-3] gælder det, at når MoS'en krypterer datafiler med henblik på medtagelse i instruktion 11, skal ægthedskontrolblokken både

— bruges som initialiseringsvektor for kryptering af datafilerne i CBC-tilstand

— krypteres og medtages som den første blok i dataene, der sendes til køretøjsenheden.

12.4. **Parring af køretøjsenhed og bevægelsessensor til forskellige udstyrsgenerationer**

CSM_222 Som forklaret i afsnit 9.2.1 kan en bevægelsessensor af anden generation indeholde TDES-baseret kryptering af parringsdataene (som defineret i del A i dette tillæg), hvilket betyder, at bevægelsessensoren kan parres med en køretøjsenhed af første generation. Hvis det forholder sig således, skal en køretøjsenhed af første generation og en bevægelsessensor af anden generation parres som beskrevet i del A i dette tillæg og i [ISO 16844-3]. Ved parringsprocessen kan man enten benytte et værkstedskort af første eller anden generation.

Bemærk:

— Det er ikke muligt at parre en køretøjsenhed af anden generation og en bevægelsessensor af første generation.

▼B

— Det er ikke muligt at anvende et værkstedskort af første generation til at sammenkoble en bevægelsessensor af anden generation med en bevægelsessensor.

13. SIKKERHED VED FJERNKOMMUNIKATION OVER DSRC

13.1. **Generelt**

Som det anføres i tillæg 14, genererer en bevægelsessensor regelmæssigt data til fjernovervågning af takograf (Remote Tachograph Monitoring — RTM) og sender dem til det interne eller eksterne fjernkommunikationsudstyr (Remote Communication Facility — RCF). Fjernkommunikationsudstyret har ansvaret for at sende disse data via DSRC-interfacet, som beskrives i tillæg 14, til fjerninterrogatoren. I tillæg 1 angives det, at RTM-dataene er en sammenføring af:

Krypteret takografindhold krypteringen af takografindholdet i klartekst

DSRC-sikkerhedsdata beskrives nedenfor

Formatet for takografindholdet i klartekst specificeres i tillæg 1 og beskrives nærmere i tillæg 14. I dette afsnit beskrives strukturen af DSRC-sikkerhedsdataene; den formelle specifikation findes i tillæg 1.

CSM_223 `tachographPayload`-dataene i klartekst, som en bevægelsessensor sender til fjernkommunikationsudstyr (hvis RCF'et er eksternt i forhold til køretøjsenheden) eller fra køretøjsenheden til fjerninterrogatoren via DSRC-interfacet (hvis RCF'et er indbygget i køretøjsenheden), skal beskyttes i »Krypter-derefter-autentificer«-tilstand, dvs. at takografindholdet krypteres først for at sikre meddelelsens fortrolighed, og derefter beregnes der en MAC for at sikre dataenes ægthed og integritet.

CSM_224 DSRC-sikkerhedsdataene består af sammenlægningen af følgende dataelementer i følgende rækkefølge; se også Figur 12:

Aktuel dato og klokkeslæt	køretøjsenhedens aktuelle dato og klokkeslæt (datatype `TimeReal`)
Tæller	en tæller på 3 byte, se CSM_225
køretøjsenhedens serienummer	køretøjsenhedens serienummer (datatype `VuSerialNumber`)
Versionsnummer for DSRC-hovednøgle	versionsnummeret for DSRC-hovednøglen på 1 bit, ud fra hvilken de køretøjsenhedsspecifikke DSRC-nøgler er afledt, se afsnit 9.2.2.
MAC	MAC'en beregnet ud fra alle de tidligere byte i RTM-dataene.

CSM_225 Tælleren på 3 byte i DSRC-sikkerhedsdataene skal være i MSB-first-format. Første gang en bevægelsessensor beregner et sæt RTM-data, efter at den er sat i produktion, sætter den tællerens værdi til 0. Køretøjsenheden øger værdien af tællerdataene med 1, hver gang den beregner det næste sæt RTM-data.

▼B

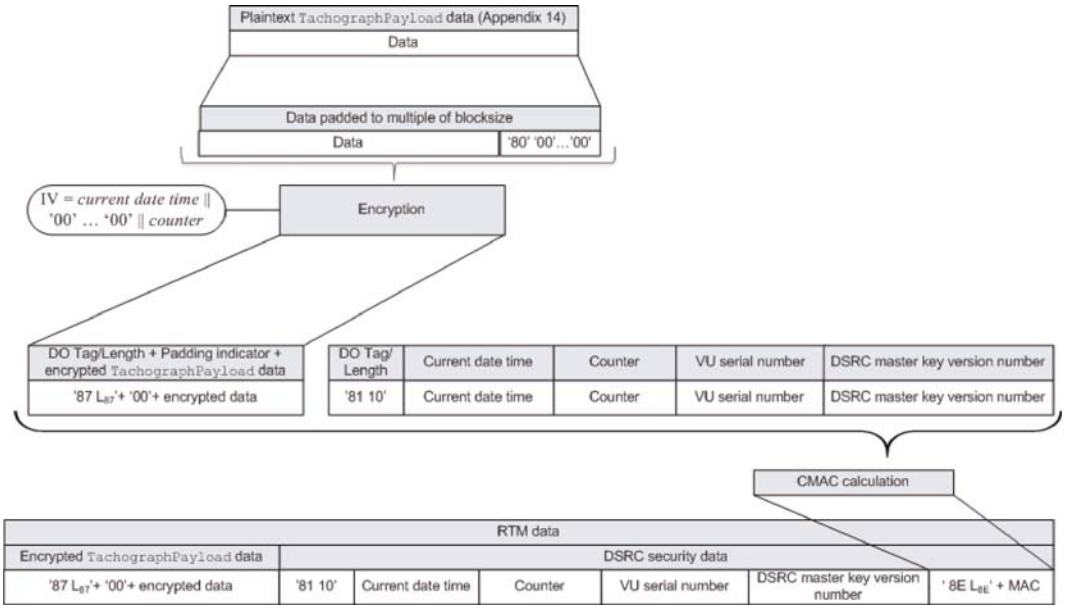
13.2. **Kryptering af takografindhold og MAC-generering**

CSM_226 Med et dataelement i klartekst med datatypen `TachographPayload` som beskrevet i tillæg 14 skal en bevægelsessensor kryptere disse data som vist i Figur 12: køretøjsenhedens DSRC-nøgle til kryptering af $K_VU_{DSRC}_ENC$ (se afsnit 9.2.2) skal anvendes med AES med blokkædningsmetoden (CBC) som defineret i [ISO 10116] med en indskudt parameter $m = 1$. Initialiseringsvektoren er lig med *IV = aktuel dato og klokkeslæt* || *'00 00 00 00 00 00 00 00'* || *tæller*, hvor *aktuel dato og klokkeslæt* og *tæller* specificeres i CSM_224. De data, der skal krypteres, udfyldes ved hjælp af metode 2, som defineres i [ISO 9797-1].

CSM_227 En køretøjsenhed beregner MAC'en i DSRC-sikkerhedsdataene som vist i Figur 12: MAC'en beregnes ud fra alle de foregående byte i RTM-dataene til og med versionsnummeret for DSRC-hovednøglen og inklusive dataobjekternes mærkater og længder. Køretøjsenheden bruger sin DSRC-nøgle til ægthed $K_VU_{DSRC}_MAC$ (se afsnit 9.2.2) med AES-algoritmen i CMAC-tilstand som specificeret i [SP 800-38B]. Længden af MAC'en sammenkædes med længden af de køretøjsenhedsspecifikke DSRC-nøgler som specificeret i CSM_50.

Figur 12

Kryptering af takografens dataindhold og MAC-generering



13.3. **Verifikation og dekryptering af takografindhold**

CSM_228 Når en fjerninterrogator modtager RTM-data fra en bevægelsessensor, sender den alle RTM-dataene til et kontrolkort i datafeltet for en PROCESS DSRC MESSAGE-kommando som beskrevet i tillæg 2. Herefter:

▼B

1. undersøger kontrolkortet versionsnummeret på DSRC-hovednøglen i DSRC-sikkerhedsdataene. Hvis kontrolkortet ikke kender den angivne DSRC-hovednøgle, returnerer den en fejl som specificeret i tillæg 2 og afbryder processen.

2. Kontrolkortet bruger den angivne DSRC-hovednøgle i kombination med køretøjsenhedens serienummer i DSRC-sikkerhedsdataene til at udlede de køretøjsenhedsspecifikke DSRC-nøgler $K_VU_{DSRC}_ENC$ og $K_VU_{DSRC}_MAC$ som specificeret i CSM_124.

3. Kontrolkortet bruger $K_VU_{DSRC}_MAC$ til at verificere MAC'en i DSRC-sikkerhedsdataene som specificeret i CSM_227. Hvis MAC'en er forkert, returnerer kontrolkortet en fejl som specificeret i tillæg 2 og afbryder processen.

4. Kontrolkortet bruger $K_VU_{DSRC}_ENC$ til at dekryptere det krypterede takografindhold som specificeret i CSM_226. Kontrolkortet fjerner udfyldningen og returnerer de dekrypterede data for takografindholdet til fjerninterrogatoren.

CSM_229 For at undgå replay-angreb verificerer fjerninterrogatoren, at der er tale om nye RTM-data, ved at verificere, at *aktuel dato og klokkeslæt* i DSRC-sikkerhedsdataene ikke afviger for meget fra det aktuelle klokkeslæt i fjerninterrogatoren.

Bemærk:

— Dette kræver, at fjerninterrogatoren har en nøjagtig og pålidelig kilde til klokkeslæt.

— Eftersom det i tillæg 14 kræves, at en bevægelsessensor skal beregne et nyt sæt RTM-data hver 60. sekund, og uret i køretøjsenheden må afvige med 1 minut fra det reelle tidspunkt, er den nedre grænse for RTM-dataene på 2 minutter. Den faktiske opdateringsfrekvens, der kræves, afhænger også af nøjagtigheden af fjerninterrogatorens ur.

CSM_230 Når et værksted verificerer, at DSRC-funktionen i en bevægelsessensor fungerer korrekt, sender den alle de RTM-data, som den har modtaget fra køretøjsenheden, til et værkstedskort i datafeltet for en PROCESS DSRC MESSAGE-kommando som beskrevet i tillæg 2. Værkstedskortet udfører alle kontroller og handlinger, som specificeres i CSM_228.

14. UNDERSKRIVELSE AF DATAOVERFØRSLER OG VERIFICERING AF UNDERSKRIFTER

14.1. **Generelt**

CSM_231 Det intelligente dedikerede udstyr (IDE) lagrer data, som er modtaget fra en bevægelsessensor eller et kort, i løbet af en overførselssession, i en fysisk datafil. Data kan lagres på et eksternt lagermedie. Denne fil indeholder digitale underskrifter over datablokke som specificeret i tillæg 7. Filen indeholder ligeledes følgende certifikater (se afsnit 9.1):

▼B

— Ved overførsel fra en køretøjsenhed:

— VU_Sign-certifikatet

— MSCA_VU-EGF-certifikatet, der indeholder den offentlige nøgle, som skal benyttes til verifikation af VU_Sign-certifikatet

— Ved overførsel fra et kort:

— Card_Sign-certifikatet

— MSCA_Card-certifikatet, der indeholder den offentlige nøgle, der skal benyttes til verifikation af Card_Sign-certifikatet

CSM_232 IDE-udstyret skal også have adgang til følgende:

— Hvis det anvender et kontrolkort til at verificere underskriften som vist i Figur 13: forbindelsescertifikatet, der knytter det seneste EUR-certifikat sammen med EUR-certifikatet, hvis gyldighedsperiode ligger umiddelbart forud for det, hvis dette findes.

— Hvis det selv verificerer underskriften: alle gyldige europæiske rodcertifikater.

Bemærk: Den metode, som IDE-udstyret bruger til at hente disse certifikater, specificeres ikke i dette tillæg.

14.2. **Generering af underskrifter**

CSM_233 Underskriftsalgoritmen, som anvendes til at oprette digitale underskrifter ud fra overførte data, er ECDSA som specificeret i [DSS] ved hjælp af hash-algoritmen, der er knyttet til køretøjsenhedens eller kortets nøglestørrelse som specificeret i CSM_50. Underskriftsformatet skal være klartekst som specificeret i [TR-03111].

14.3. **Verifikation af underskrift**

CSM_234 En IDE kan foretage verifikation af en underskrift ud fra selve de overførte data eller kan benytte et kontrolkort til dette. Hvis det anvender et kontrolkort, skal verifikationen foregå som vist i Figur 13: Hvis det selv foretager verifikationen af underskriften, skal IDE-udstyret verificere ægtheden og gyldigheden af alle certifikater i certifikatkæden i datafilen, og det skal verificere underskriften ud fra dataene i henhold til den underskriftsmetode, der defineres i [DSS].

Bemærkninger til Figur 13:

— Det udstyr, som har overført og underskrevet de data, der skal analyseres, benævnes EQT (udstyr).

— EQT-certifikaterne og de offentlige nøgler, der nævnes i figuren, er dem, der anvendes til underskrift, dvs. VU_Sign eller Card_Sign.

— EQT.CA-certifikaterne og de offentlige nøgler, der nævnes i figuren, er dem, der anvendes til underskrift af enten bevægelsessensor- eller kortcertifikater.

— EQT.CA.EUR-certifikatet, der nævnes i figuren, er det europæiske rodcertifikat, der angives i EQT.CA-certifikatets CAR.

▼B

— EQT.Link-certifikatet, der nævnes i figuren, er EQT'ens forbindelsescertifikat, hvis dette findes. Som beskrevet i afsnit 9.1.2 er dette et forbindelsescertifikat til et europæisk rodnøglepar, som er oprettet af ERCA'en og underskrevet af den tidligere europæiske private nøgle.

— EQT.Link.EUR-certifikatet er det europæiske rodcertifikat, der angives i EQT.Link-certifikatets CAR.

CSM_235 Ved beregning af hash-værdien M, som sendes til kontrolkortet i PSO:Hash-kommandoen, benytter IDT-udstyret den hash-algoritme, der er knyttet til nøglestørrelsen af køretøjsenheden eller kortet, hvorfra dataene er overført, som specificeret i CSM_50.

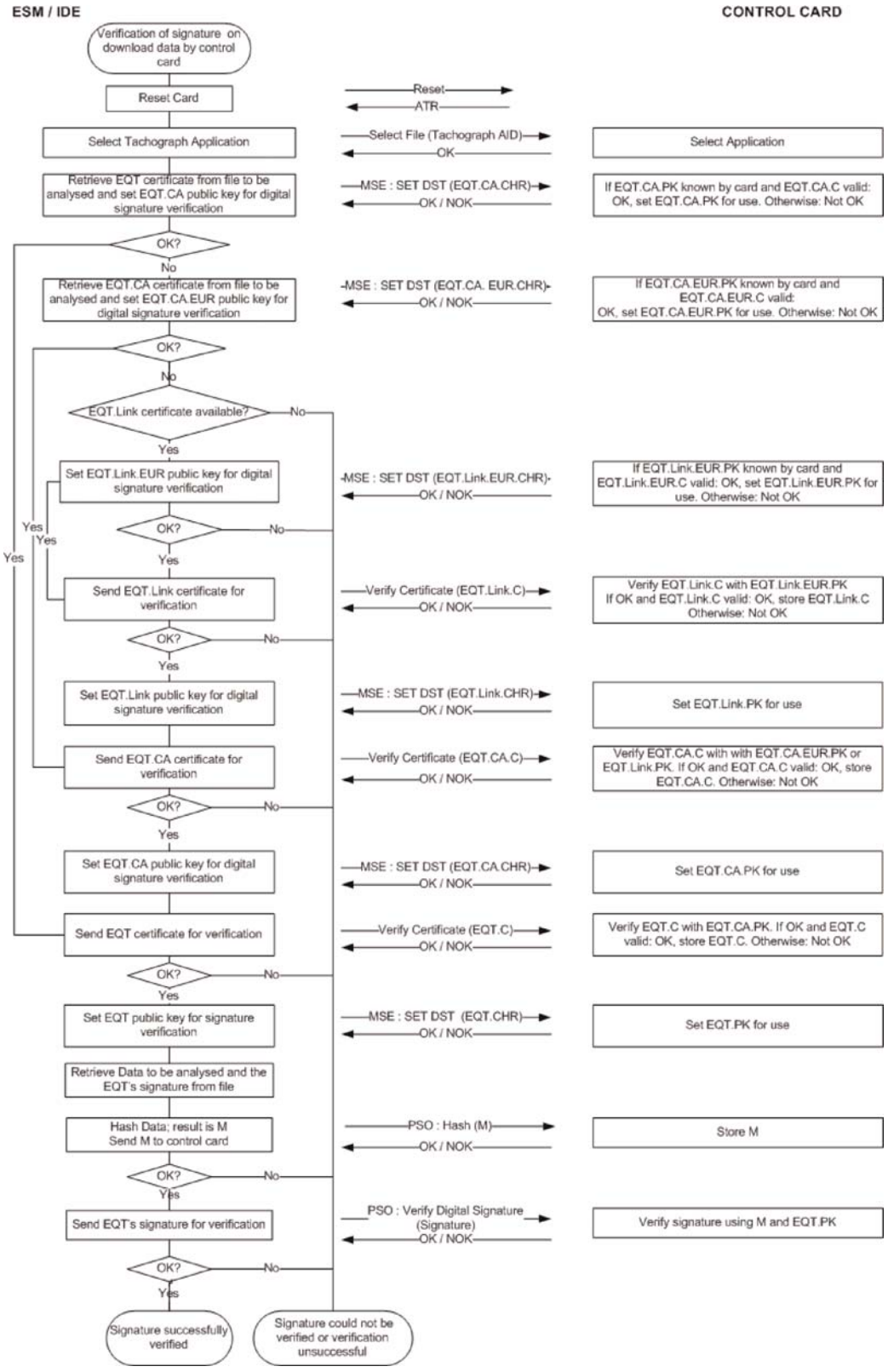
CSM_236 Til verifikation af EQT'ets underskrift skal kontrolkortet følge den underskriftsmetode, der defineres i [DSS].

Bemærk: I dette dokument angives det ikke, hvilke foranstaltninger der skal træffes, hvis en underskrift ud fra en overført datafil ikke kan verificeres, eller hvis verifikationen ikke lykkes.

▼B

Figur 13

Protokol til verifikation af underskriften ud fra en overført datafil



▼B

Tillæg 12

LOKALISERING BASERET PÅ ET GLOBALT SATELLITNAVIGATIONSSYSTEM (GNSS)

INDHOLDSFORTEGNELSE

1. INDLEDNING

1.1. Anvendelsesområde

1.2. Akronymer og notation

2. SPECIFIKATION AF GNSS-MODTAGEREN

3. NMEA-SÆTNINGER

4. KØRETØJSENHED MED EKSTERNT GNSS-UDSTYR

4.1. Konfiguration

4.1.1 Vigtigste komponenter og interfaces

4.1.2 Det eksterne GNSS-udstyrs tilstand ved afslutningen af produktionen

4.2. Kommunikation mellem det eksterne GNSS-udstyr og køretøjsenheden

4.2.1 Kommunikationsprotokol

4.2.2 Sikker overførsel af GNSS-data

4.2.3 Read Record-kommandoens struktur

4.3. Kobling, gensidig ægthedskontrol og kontrol af sessionsnøgleoverensstemmelse for det eksterne GNSS-udstyr med køretøjsenhed

4.4. Fejlhåndtering

4.4.1 Kommunikationsfejl med det eksterne GNSS-udstyr

4.4.2 Brud på det eksterne GNSS-udstyrs fysiske integritet

4.4.3 Manglende positionsoplysninger fra GNSS-modtager

4.4.4 Certifikatet for det eksterne GNSS-udstyr er udløbet

5. KØRETØJSENHED UDEN EKSTERNT GNSS-UDSTYR

5.1. Konfiguration

5.2. Fejlhåndtering

5.2.1 Manglende positionsoplysninger fra GNSS-modtager

6. GNSS-TIDSKONFLIKT

7. KØRETØJSBEVÆGELSESKONFLIKT

1. INDLEDNING

Dette tillæg indeholder de tekniske krav til GNSS-data, som benyttes af køretøjsenheden, inklusive de protokoller, der skal gennemføres for at garantere sikker og korrekt dataoverførsel af lokaliseringsoplysningerne.

De væsentligste artikler i forordning (EU) nr. 165/2014 bag disse krav er: »Artikel 8 Registrering af køretøjets position på visse punkter i løbet af den daglige arbejdsperiode«, »Artikel 10 Interface med intelligente transportsystemer« og »Artikel 11 Detaljerede bestemmelser for intelligente takografer«.

▼B

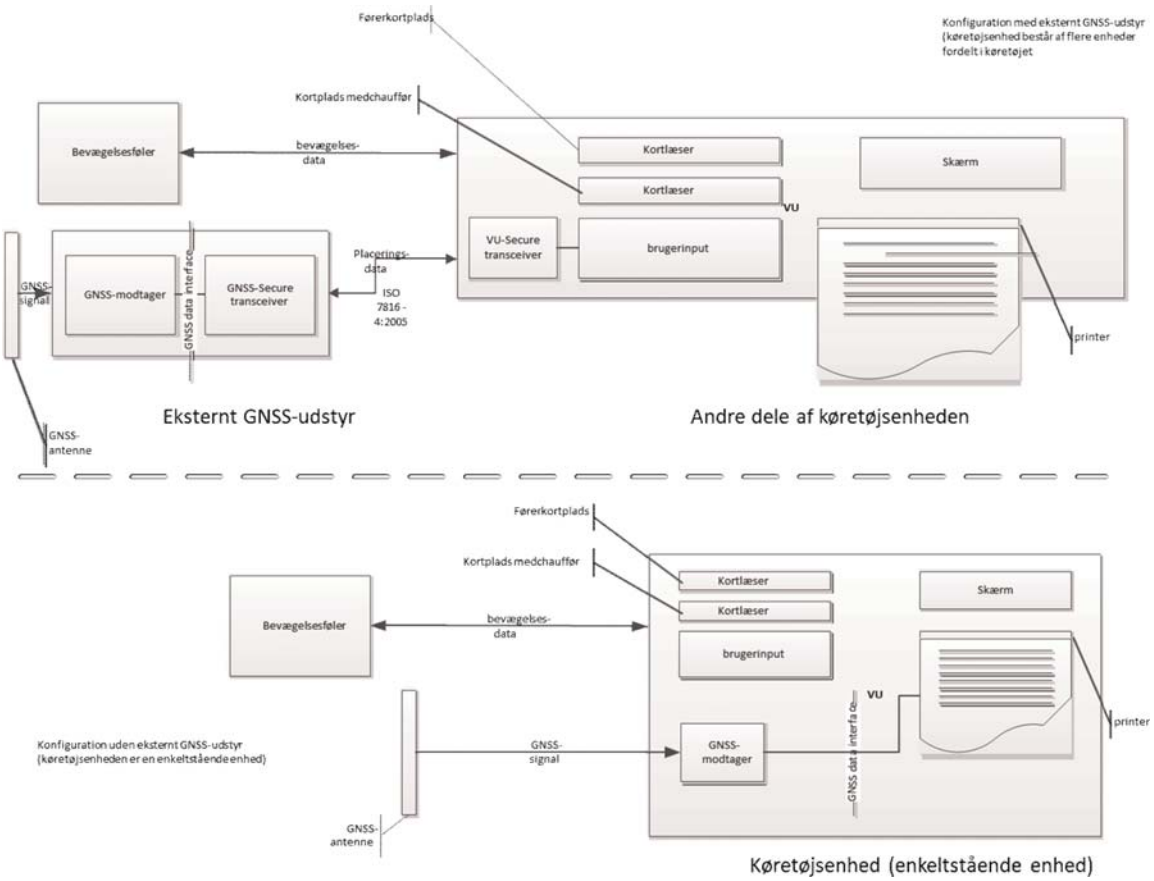
1.1. **Anvendelsesområde**

GNS_1 Køretøjsenheden indsamler positionsdata fra mindst ét GNSS med henblik på gennemførelsen af artikel 8.

Køretøjsenheden kan være forsynet med eksternt GNSS-udstyr, jf. Figur 1:

Figur 1

Forskellige konfigurationer af GNSS-modtageren.



1.2. **Akronymer og notation**

I dette tillæg anvendes følgende akronymer:

DOP	Præcisionsopløsning
EGF	GNSS-udstyrets elementærfil
EGNOS	European Geostationary Navigation Overlay Service
GNSS	Globalt satellitnavigationssystem
GSA	GPS DOP og aktive satellitter
HDOP	Horisontal præcisionsopløsning
ICD	Interfacekontroldokument
NMEA	National Marine Electronics Association

▼B

PDOP Positions præcisionsopløsning

RMC Anbefalet minimum specifik

SIS Signal i rummet

VDOP Vertikal præcisionsopløsning

VU Køretøjsenhed

2. SPECIFIKATION AF GNSS-MODTAGEREN

Uanset konfigurationen af den intelligente takograf med eller uden eksternt GNSS-udstyr er levering af nøjagtige og pålidelige lokaliseringsoplysninger et centralt element for en effektiv anvendelse af den intelligente takograf. Derfor er det hensigtsmæssigt at kræve, at den er forenelig med de serviceydelser, som leveres under programmerne Galileo og European Geostationary Navigation Overlay Service (Egnos) som fastsat i Europa-Parlamentets og Rådets forordning (EU) nr. 1285/2013 ([1]). Det system, der er oprettet under Galileoprogrammet, er et uafhængigt globalt satellitnavigationssystem, og det system, der er oprettet under Egnosprogrammet, er et regionalt satellitnavigationssystem, der forbedrer kvaliteten af GPS-signalet (det globale positioneringssystem).

GNS_2 Fabrikanterne sikrer, at GNSS-modtagerne i de intelligente takografer er kompatible med positioneringstjenesterne fra Galileo- og Egnossystemerne. Fabrikanterne kan derudover også vælge kompatibilitet med andre satellitnavigationssystemer.

GNS_3 GNSS-modtageren skal kunne understøtte Authentication on the Open Service of Galileo, når en sådan service leveres af Galileo-systemet og understøttes af fabrikanter af GNSS-modtagere. For intelligente takografer, der bringes på markedet inden de foranstående betingelser er opfyldt, og som ikke kan understøtte Authentication on the Open Service of Galileo, vil der dog ikke være noget krav om retrofitting.

3. NMEA-SÆTNINGER

I dette afsnit beskrives de NMEA-sætninger, der anvendes til driften af den intelligente takograf. Dette afsnit gælder både konfigurationen af den intelligente takograf med og uden eksternt GNSS-udstyr.

GNS_4 Lokaliseringsdataene er baseret på NMEA-sætningen Recommended Minimum Specific (RMC) GNSS-data, der indeholder positionsoplysninger (breddegrad, længdegrad), klokkeslæt i UTC-format (ttmmss.ss) og hastigheden over jorden i knob (Speed Over Ground in Knots) plus supplerende værdier.

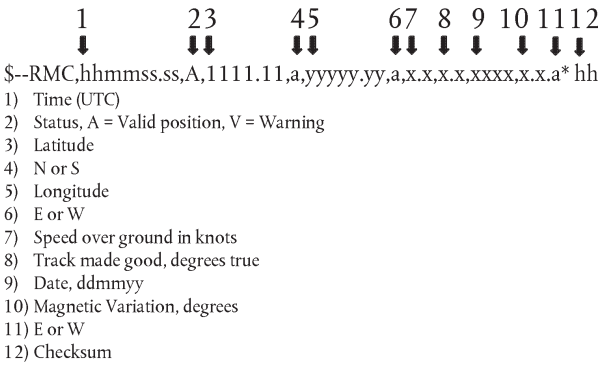
RMC-sætningen har følgende format (fra NMEA V4.1-standarden):

([1]) Europa-Parlamentets og Rådets forordning (EU) nr. 1285/2013 af 11. december 2013 om etablering og drift af de europæiske satellitbaserede navigationssystemer og om ophævelse af Rådets forordning (EF) nr. 876/2002 og Europa-Parlamentets og Rådets forordning (EF) nr. 683/2008 (EUT L 347 af 20.12.2013, s. 1).

▼B

Figur 2

RMC-sætningens struktur



Status viser, om der modtages et GNSS-signal. Indtil værdien for Status ikke er sat til A, kan de modtagne data (f.eks. om klokkeslæt eller breddegrad/længdegrad) ikke bruges til at registrere køretøjets position i køretøjsenheden.

Opløsningen af positionen er baseret på RMC-sætningens format som beskrevet ovenfor. Første del af felt 3) og 5) (de to første tal) bruges til at angive graderne. Resten bruges til at angive minutterne med tre decimaler. Så opløsningen er 1/1 000 minut eller 1/60 000 grad (fordi et minut er 1/60 grad).

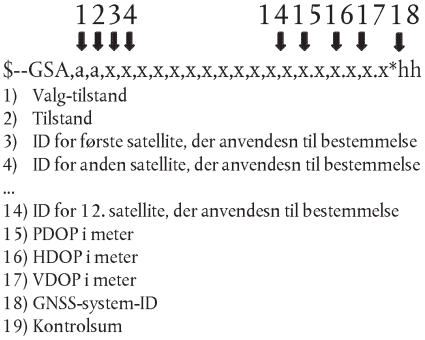
GNS_5 Køretøjsenheden gemmer positionsoplysninger for breddegrad og længdegrad i sin database med en opløsning på 1/10 minut eller 1/600 grad som beskrevet i tillæg 1 for typen GeoCo-ordinates.

Køretøjsenheden kan bruge kommandoen GPS DOP og aktive satellitter (GSA) til at afgøre og registrere signalets tilgængelighed og nøjagtighed. HDOP anvendes navnlig til at give en indikation af nøjagtigheden af de registrerede positionsdata (se 4.2.2). Køretøjsenheden gemmer værdien af den horisontale præcisionsopløsning (HDOP), der beregnes som den mindste af HDOP-værdierne, der er indsamlet på de tilgængelige GNSS-systemer.

GNSS-system-ID angiver GPS, Glonass, Galileo, Beidou eller Satellite-Based Augmentation System (SBAS).

Figur 3

GSA-sætningens struktur



▼B

Hvor Tilstand (2) giver en indikation, hvis der ikke er mulighed for bestemmelse (Tilstand=1), eller der er mulighed for bestemmelse for 2D (Tilstand=2) eller 3D (Tilstand=3).

GNS_6 *GSA*-sætningen gemmes med registreringsnummer '06'.

GNS_7 Den maksimale størrelse af NMEA-sætningerne (f.eks. RMC, GSA eller andre), som kan anvendes til at angive størrelsen af kommandoen Read record, er 85 byte (se Tabel 1).

4. KØRETØJSENHED MED EKSTERNT GNSS-UDSTYR

4.1. **Konfiguration**

4.1.1 *Vigtigste komponenter og interfaces*

I denne konfiguration er GNSS-modtageren en del af det eksterne GNSS-udstyr.

GNS_8 Det eksterne GNSS-udstyr skal have strøm fra en specifik køretøjsinterface.

GNS_9 Det eksterne GNSS-udstyr består af følgende komponenter (se Figur 4):

a) En kommerciel GNSS-modtager, der leverer positionsdata via GNSS-datainterfacet. GNSS-datainterfacet kan f.eks. være NMEA-standard V4.10, hvor GNSS-modtageren fungerer som transmitter og sender NMEA-sætninger til den sikre GNSS-sender/modtager med en frekvens på 1 Hz for det foruddefinerede sæt af NMEA-sætninger, der som minimum skal omfatte RMC- og GSA-sætningerne. Indførelsen af GNSS-datainterfacet vælges af fabrikanten af det eksterne GNSS-udstyr.

b) En sende-/modtageenhed (sikker GNSS-sender/modtager), der kan understøtte standard ISO/IEC 7816-4:2013 (se 4.2.1) til at kommunikere med køretøjsenheden og understøtte GNSS-datainterfacet til GNSS-modtageren. Enheden er udstyret med en hukommelse til lagring af GNSS-modtagerens og det eksterne GNSS-udstyrs identifikationsdata.

c) Et indkapslingssystem med en funktion til detektering af manipulation, som indkapsler både GNSS-modtageren og den sikre GNSS-sender/modtager. Funktionen til detektering af manipulation omfatter de sikkerheds- og beskyttelsesforanstaltninger, der kræves i beskyttelsesprofilen for den intelligente takograf.

d) En GNSS-antenne monteret på køretøjet og tilsluttet GNSS-modtageren gennem indkapslingssystemet.

GNS_10 Det eksterne GNSS-udstyr har som minimum følgende eksterne interfaces:

a) interfacet til GNSS-antennen, som er monteret på køretøjets trækker, hvis der benyttes en ekstern antenne

b) interfacet til køretøjsenheden.

GNS_11 I køretøjsenheden er køretøjsenhedens sikre sender-modtager den anden ende af den sikre kommunikation med den sikre GNSS-sender/modtager, og den skal understøtte ISO/IEC 7816-4:2013 for forbindelsen til det eksterne GNSS-udstyr.

▼B

GNS_12 Hvad angår det fysiske lag af forbindelsen til det eksterne GNSS-udstyr, skal køretøjsenheden understøtte ISO/IEC 7816-12:2005 eller en anden standard, som understøtter ISO/IEC 7816-4:2013 (se 4.2.1).

4.1.2 *Det eksterne GNSS-udstyrs tilstand ved afslutningen af produktionen*

GNS_13 Det eksterne GNSS-udstyr gemmer følgende værdier i det ikkeflygtige lager i den sikre GNSS-sender/modtager, når den forlader fabrikken:

— EGF_MA-nøgleparret og det tilhørende certifikat

— MSCA_VU-EGF-certifikatet, der indeholder den offentlige MSCA_VU-EGF.PK-nøgle, der skal anvendes til verifikation af EGF_MA-certifikatet

— EUR-certifikatet, der indeholder den offentlige EUR.PK-nøgle, der skal benyttes til verifikation af MSCA_VU-EGF-certifikatet

— EUR-certifikatet, hvis gyldighedsperiode ligger umiddelbart forud for EUR-certifikatets gyldighedsperiode, som skal anvendes til at verificere MSCA_VU-EGF-certifikatet, hvis dette findes

— forbindelsescertifikatet, der knytter disse to EUR-certifikater sammen, hvis dette findes

— det udvidede serienummer for det eksterne GNSS-udstyr

— identifikatoren for styresystemet i GNSS-udstyret

— typegodkendelsesnummeret på det eksterne GNSS-udstyr

— identifikatoren for sikkerhedskomponenten for det eksterne GNSS-modul.

4.2. **Kommunikation mellem det eksterne GNSS-udstyr og køretøjsenheden**

4.2.1 *Kommunikationsprotokol*

GNS_14 Kommunikationsprotokollen mellem det eksterne GNSS-udstyr og køretøjsenheden skal understøtte tre funktioner:

1. indsamling og distribution af GNSS-data (f.eks., position, tidspunkt, hastighed)

2. indsamling af konfigurationsdata for det eksterne GNSS-udstyr

3. administrationsprotokollen, der understøtter sammenkoblingen, gensidig ægthedskontrol og kontrol af sessionsnøgleoverensstemmelse mellem det eksterne GNSS-udstyr og køretøjsenheden.

GNS_15 Kommunikationsprotokollen er baseret på standard ISO/IEC 7816-4:2013, hvor køretøjsenhedens sikre sender/modtager er »master«, og den sikre GNSS-sender/modtager er »slave«. Den fysiske forbindelse mellem det eksterne GNSS-udstyr og køretøjsenheden er baseret på ISO/IEC 7816-12:2005 eller en anden standard, som understøtter ISO/IEC 7816-4:2013.

▼B

GNS_16 Kommunikationsprotokollen understøtter ikke felter med udvidet længde.

GNS_17 Kommunikationsprotokollen fra ISO 7816 (både *-4:2013 og *-12:2005) mellem det eksterne GNSS-udstyr og køretøjsenheden angives til T=1.

GNS_18 Hvad angår funktionerne 1) indsamling og distribution af GNSS-data, 2) indsamling af konfigurationsdata for det eksterne GNSS-udstyr og 3) administrationsprotokollen, skal den sikre GNSS-sender/modtager simulere et intelligent kort med en filsystemarkitektur bestående af en masterfil (MF), en registerfil (DF) med en applikations-ID som specificeret i tillæg 1, kapitel 6.2 (»FF 44 54 45 47 4D«) og med 3 elementærfiler, der indeholder certifikater og en enkelt elementærfil (EF.EGF) med en filidentifikator lig med '2F2F' som beskrevet i Tabel 1.

GNS_19 Den sikre GNSS-sender/modtager gemmer data, der kommer fra GNSS-modtageren og konfigurationen i EF.EGF. Dette er en lineær registerfil af variabel længde med en identifikator lig med '2F2F' i hexadecimalformat.

GNS_20 Den sikre GNSS-sender/modtager bruger en hukommelse til at gemme data, som kan udføre mindst 20 millioner skrive/læsecykler. Bortset fra dette aspekt overlades det interne design og implementeringen af den sikre GNSS-sender/modtager til fabrikanterne.

Kortlægningen af registernumre og data findes i Tabel 1. Bemærk, at der findes fire GSA-sætninger til de fire satellitsystemer og et Satellite-Based Augmentation System (SBAS).

GNS_21 Filstrukturen findes i Tabel 1. For så vidt angår adgangsbetingelser (ALW, NEV, SM-MAC) henvises til tillæg 2, kapitel 3.5.

▼C2

Tabel 1

Filstruktur

		Adgangsbetingelser		
Fil	Filidentifikator	Læs	Opdater	Krypteret
MF	3F00			
EF.ICC	0002	ALW	NEV (fra VU)	Nej
DF GNSS-udstyr	0501	ALW	NEV	Nej
EF EGF_MACertificate	C100	ALW	NEV	Nej
EF CA_Certificate	C108	ALW	NEV	Nej
EF Link_Certificate	C109	ALW	NEV	Nej
EF.EGF	2F2F	SM-MAC	NEV (fra VU)	Nej

▼C2

Fil/dataelement	Post nr.	Størrelse (byte)		Standardværdier
		Min.	Maks.	
MF		552	1031	
EF.ICC				
sensorGNSSSerialNumber		8	8	
DF GNSS-udstyr		612	1023	
EF EGF_MA_Certificate		204	341	
EGFCertificate		204	341	{00..00}
EG CA_Certificate		204	341	
MemberStateCertificate		204	341	{00..00}
EF Link_Certificate		204	341	
LinkCertificate		204	341	{00..00}
EF.EGF				
RMC NMEA-sætning	»01«	85	85	
1. GSA NMEA-sætning	»02«	85	85	
2. GSA NMEA-sætning	»03«	85	85	
3. GSA NMEA-sætning	»04«	85	85	
4. GSA NMEA-sætning	»05«	85	85	
5. GSA NMEA-sætning	»06«	85	85	
Udvidet serienummer for det eksterne GNSS-udstyr defineret i tillæg 1 som SensorGNSSSerialNumber.	»07«	8	8	
Identifikator for styresystemet for den sikre GNSS-sender/modtager defineret i tillæg 1 som SensorOSIdentifier.	»08«	2	2	
Typegodkendelsesnummer for det eksterne GNSS-udstyr defineret i tillæg 1 som SensorExternalGNSSApprovalNumber.	»09«	16	16	
Identifikator for sikkerhedskomponenten for det eksterne GNSS-udstyr defineret i tillæg 1 som SensorExternalGNSSSCIdentifier	»10«	8	8	
RFU — Forbeholdt fremtidig brug — (Reserved for future use)	Fra »11« til »FD«			

▼B

4.2.2 *Sikker overførsel af GNSS-data*

GNS_22 Den sikre overførsel af GNSS-positionsdata er kun tilladt på følgende betingelser:

1. Koblingsprocessen er gennemført som beskrevet i tillæg 11. Fælles sikkerhedsmekanismer.

▼B

2. Den periodiske gensidige ægthedskontrol og kontrol af sessionsnøgleoverensstemmelse mellem køretøjsenheden og det eksterne GNSS-udstyr beskrives ligeledes i tillæg 11. Fælles sikkerhedsmekanismer er blevet gennemført med den angivne frekvens.

GNS_23 Hver T sekunder, hvor T er lavere end eller lig med 10, medmindre kobling eller gensidig ægthedskontrol og kontrol af sessionsnøgleoverensstemmelse finder sted, anmoder køretøjsenheden det eksterne GNSS-udstyr om positionsoplysninger på grundlag af følgende flow:

1. Køretøjsenheden anmoder om positionsdata fra det eksterne GNSS-udstyr sammen med data om præcisionsopløsning (fra GSA NMEA-sætningen). Køretøjsenhedens sikre sender/modtager anvender ISO/IEC 7816-4:2013 SELECT- og READ RECORD(S)- kommandoen i tilstanden »Kun ægthedskontrol« for den sikre meddelelsesfunktion som beskrevet i tillæg 11 afsnit 11.5 med filidentifikatoren »2F2F« og RECORD-tallet lig med »01« til RMC NMEA-sætningen og ‘02’,‘03’,‘04’,‘05’,‘06’ for GSA NMEA-sætningen.

2. De senest modtagne positionsdata gemmes i elementærfilen med identifikatoren ‘2F2F’ og posterne, der beskrives i Tabel 1 i den sikre GNSS-sender/modtager, mens den sikre GNSS-sender/modtager modtager NMEA-data med en frekvens på mindst 1 Hz fra GNSS-modtageren via GNSS-datainterfacet.

3. Den sikre GNSS-sender/modtager sender svaret til køretøjsenhedens sikre sender/modtager ved hjælp af APDU-svarmeddelelsen i tilstanden »Kun ægthedskontrol« i den sikre meddelelsesoverførsel som beskrevet i tillæg 11, afsnit 11.5.

4. Køretøjsenhedens sikre sender/modtager kontrollerer ægtheden og integriteten af det modtagne svar. Ved et positivt resultat overføres positionsdataene til køretøjsenhedens processor via GNSS-datainterfacet.

5. Køretøjsenhedens processor kontrollerer de modtagne data ved at udtrække oplysningerne (f.eks. breddegrad, længdegrad, tidspunkt) af RMC NMEA-sætningen. RMC NMEA-sætningen medtager oplysningerne, hvis positionen er gyldig. Hvis positionen ikke er gyldig, er positionsdataene endnu ikke tilgængelige, og de kan ikke anvendes til at registrere køretøjets position. Hvis positionen er gyldig, udtrækker køretøjsenhedens processor ligeledes værdierne HDOP af GSA NMEA-sætningerne og beregner den gennemsnitlige værdi af de tilgængelige satellitsystemer (dvs. når den modtager et signal).

6. Køretøjsenhedens processor gemmer de modtagne og behandlede oplysninger som breddegrad, længdegrad, tidspunkt og hastighed i køretøjsenheden i det format, der defineres i tillæg 1, Dataordliste, som GeoCoordinates sammen med værdien af HDOP beregnet som et minimum af de HDOP-værdier, der er indsamlet på de tilgængelige GNSS-systemer.

▼B

4.2.3 *Read Record-kommandoens struktur*

Dette afsnit indeholder en detaljeret beskrivelse af Read Record-kommandoens struktur. Sikre meddelelser (tilstanden »Kun ægthedskontrol«) tilføjes som beskrevet i tillæg 11, Fælles sikkerhedsmekanismer.

GNS_24 Kommandoen understøtter sikker meddelelsesoverførsel i tilstanden »Kun ægthedskontrol«, se tillæg 11.

GNS_25 Kommandomeddelelse

Byte	Længde	Værdi	Beskrivelse
CLA	1	'0Ch'	Der er anmodet om sikker meddelelsesoverførsel
INS	1	'B2h'	Read Record
P1	1	'XXh'	Post nr. ('00' henviser til den aktuelle post)
P2	1	'04h'	Læst posten med det postnummer, der angives i P1
Le	1	'XXh'	Forventet datalængde. Antal byte, som skal læses

GNS_26 Posten, der henvises til i P1, bliver den aktuelle post.

Byte	Længde	Værdi	Beskrivelse
#1-#X	X	'XX..XXh'	Data læst
SW	2	'XXXXh'	Statusord (SW1,SW2)

— Giver kommandoen resultat, tilbagemelder den sikre GNSS-sender/modtager '**9000**'.

— Hvis den aktuelle fil ikke er postorienteret, tilbagemelder den sikre GNSS-sender/modtager **»6981«**.

— Hvis kommandoen bruges med P1 = »00«, men der ikke findes nogen aktuel elementærfil, tilbagemelder den sikre GNSS-sender/modtager **»6986«** (kommando ikke tilladt).

— Hvis posten ikke findes, tilbagemelder den sikre GNSS-sender/modtager **»6A 83«**.

— Hvis det eksterne GNSS-udstyr har konstateret manipulation, tilbagemelder den statusordene '**66 90**'.

GNS_27 Den sikre GNSS-sender/modtager understøtter følgende kommandoer fra takografer af anden generation, som specificeres i tillæg 2:

Kommando	Reference
Select	Tillæg 2, kapitel 3.5.1
Read Binary	Tillæg 2, kapitel 3.5.2
Get Challenge	Tillæg 2, kapitel 3.5.4
PSO: Verify Certificate	Tillæg 2, kapitel 3.5.7
External Authenticate	Tillæg 2, kapitel 3.5.9
General Authenticate	Tillæg 2, kapitel 3.5.10
MSE:SET	Tillæg 2, kapitel 3.5.11.

▼B

4.3. **Kobling, gensidig ægthedskontrol og kontrol af sessionsnøgleoverensstemmelse for det eksterne GNSS-udstyr med køretøjsenhed**

Kobling, gensidig ægthedskontrol og kontrol af sessionsnøglesoverensstemmelse for det eksterne GNSS-udstyr med køretøjsenhed beskrives i tillæg 11. Fælles sikkerhedsmekanismer, kapitel 11.

4.4. **Fejlhåndtering**

I dette afsnit beskrives det, hvordan potentielle fejltilstande hos det eksterne GNSS-udstyr behandles og registreres i køretøjsenheden.

4.4.1 *Kommunikationsfejl med det eksterne GNSS-udstyr*

GNS_28 Hvis det ikke lykkes køretøjsenheden at kommunikere med det sammenkoblede eksterne GNSS-udstyr i mere end 20 på hinanden følgende minutter, genererer køretøjsenheden en hændelse af typen EventFaultType og registrerer den i køretøjsenheden med værdien enum '53'H *Kommunikationsfejl på ekstern GNSS* og med tidsstemplet indstillet til det aktuelle klokkeslæt. Hændelsen genereres kun, hvis følgende to betingelser er opfyldt: a) den intelligente takograf er ikke i kalibreringstilstand og b) køretøjet bevæger sig. I den forbindelse opstår der en kommunikationsfejl, når køretøjsenhedens sikre sender/modtager ikke modtager en svarmeddelelse efter en anmodningsmeddelelse som beskrevet i 4.2.

4.4.2 *Brud på det eksterne GNSS-udstyrs fysiske integritet*

GNS_29 Hvis det eksterne GNSS-udstyr er blevet brudt, skal den sikre GNSS-sender/modtager slette hele sin hukommelse, inklusive kryptografisk materiale. Som beskrevet i GNS_25 og GNS_26 detekterer køretøjsenheden manipulation, hvis Svar har status '6690'. Køretøjsenheden genererer herefter en begivenhed af typen EventFaultType enum *'55'H Detektering af manipulering af GNSS*.

4.4.3 *Manglende positionsoplysninger fra GNSS-modtager*

GNS_30 Hvis den sikre GNSS-sender/modtager ikke modtager data fra GNSS-modtageren i mere end tre på hinanden følgende timer, genererer den sikre GNSS-sender/modtager en svarmeddelelse på READ RECORD-kommandoen med et RECORD-nummer lig med '01' med et datafelt på 12 byte, som alle er sat til 0xFF. Efter modtagelsen af svarmeddelelsen med denne værdi i datafeltet, genererer og registrerer køretøjsenheden kun en begivenhed af typen EventFaultType enum '52'H *Fejl på ekstern GNSS-modtager* med et tidsstempel lig med det aktuelle klokkeslæt, hvis følgende to betingelser er opfyldt: a) den intelligente takograf er ikke i kalibreringstilstand og b) køretøjet bevæger sig.

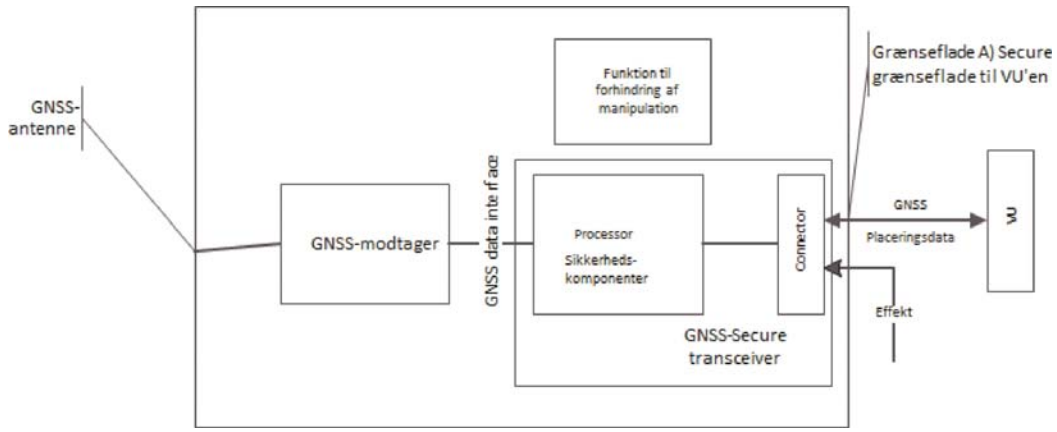
4.4.4 *Certifikatet for det eksterne GNSS-udstyr er udløbet*

GNS_31 Hvis køretøjsenheden detekterer, at EGF'ens certifikat, som anvendes til gensidig ægthedskontrol, ikke længere er gyldigt, genererer og registrerer køretøjsenheden en fejl på kontrolapparatet af typen EventFaultType enum *'56'H Eksternt GNSS-udstyrs certifikat udløbet* med et tidsstempel lig med det aktuelle klokkeslæt. Køretøjsenheden anvender stadig de modtagne GNSS-positionsdata.

▼B

Figur 4

Skema over det eksterne GNSS-udstyr



5. KØRETØJSENHED UDEN EKSTERNT GNSS-UDSTYR

5.1. **Konfiguration**

I denne konfiguration befinder GNSS-modtageren sig inde i køretøjsenheden som beskrevet i Figur 1.

GNS_32 GNSS-modtageren fungerer som transmitter og sender NMEA-sætninger til køretøjsenhedens processor, der fungerer som modtager med en frekvens på 1/10 Hz eller hurtigere for et forud defineret sæt af NMEA-sætninger, der som minimum skal omfatte RMC- og GSA-sætningerne.

GNS_33 En ekstern GNSS-antenne monteret på køretøjet eller en intern GNSS-antenne skal være tilsluttet køretøjsenheden.

5.2. **Fejlhåndtering**

5.2.1 *Manglende positionsoplysninger fra GNSS-modtager*

GNS_34 Hvis køretøjsenheden ikke modtager data fra GNSS-modtageren i mere end tre på hinanden følgende timer, genererer og registrerer køretøjsenheden kun en begivenhed af typen EventFaultType enum '51'H *Fejl på intern GNSS-modtager* med et tidsstempel lig med det aktuelle klokkeslæt, hvis følgende to betingelser er opfyldt: a) den intelligente takograf er ikke i kalibreringstilstand og b) køretøjet bevæger sig.

6. GNSS-TIDSKONFLIKT

Hvis køretøjsenheden detekterer en diskrepans på mere end 1 minut mellem tidspunktet i køretøjsenhedens tidsmålerfunktion og klokkeslættet fra GNSS-modtageren, registrerer køretøjsenheden en hændelse af typen EventFaultType enum *'0B'H Tidskonflikt (GNSS i forhold til køretøjsenhedens interne ur)*. Denne hændelse registreres sammen med det interne klokkeslæt for køretøjsenheden og følger med en automatisk indstilling af klokkeslæt. Efter at en tidskonfliktbegivenhed er blevet udløst, vil køretøjsenheden ikke kontrollere diskrepanser i klokkeslæt i de næste 12 timer. Denne begivenhed vil ikke blive udløst, hvis GNSS-modtageren ikke har detekteret noget gyldigt GNSS-signal inden for de seneste 30 dage. Men når positionsoplysningerne fra GNSS-modtageren er tilgængelige igen, udføres den automatiske indstilling af klokkeslæt.

▼B

7. KØRETØJSBEVÆGELSESKONFLIKT

GNS_35 Køretøjsenheden udløser og registrerer begivenheden køretøjsbevægelseskonflikt (se krav 84 i dette bilag) med et tidsstempel lig med det aktuelle klokkeslæt, hvis de bevægelsesoplysninger, der beregnes ud fra bevægelsesføleren, modsiges af bevægelsesoplysninger beregnet ud fra den interne GNSS-modtager eller det eksterne GNSS-udstyr. Med henblik på at opdage sådanne modsigelser anvendes middelværdien af hastighedsdifferencen mellem kilderne, jf. nedenstående:

— mindst hver 10 sekunder beregnes den absolutte værdi af forskellen mellem køretøjets hastighed skønnet ud fra GNSS og hastigheden skønnet ud fra bevægelsesføleren.

— alle beregnede værdier inden for en tidsramme, som omfatter mindst fem minutters bevægelse, anvendes til at beregne middelværdien

— middelværdien beregnes som gennemsnittet af 80 % af de resterende værdier, når de højeste værdier i absolutte tal er elimineret.

Begivenheden køretøjsbevægelseskonflikt udløses, hvis middelværdien er over 10 km/h i fem uafbrudte minutter, hvor køretøjet er i bevægelse. Der kan anvendes andre uafhængige kilder til bevægelsesoplysninger, så der tilvejebringes en mere pålidelig detektering af takografmanipulationer. (Bemærk: brugen af middelværdien for de seneste 5 minutter anvendes for at mindske risikoen for afvigende måleværdier og øjebliksværdier). Denne begivenhed udløses ikke under følgende omstændigheder: a) under færgeoverfart/transport med tog, b) når positionsoplysningerne fra GNSS-modtageren ikke er tilgængelige, og c) når enheden er i kalibreringstilstand.

▼B

Tillæg 13

ITS-INTERFACE

INDHOLDSFORTEGNELSE

1. INDLEDNING

2. ANVENDELSESOMRÅDE

2.1. Akronymer, definitioner og notation

3. HENVISNINGER TIL FORORDNINGER OG STANDARDER

4. FUNKTIONSPRINCIPPER FOR INTERFACE

4.1. Forudsætninger for dataoverførsel via ITS-interfacet

4.1.1 Data overført via ITS-interfacet

4.1.2 Indholdet af dataene

4.1.3 ITS-applikationer

4.2. Kommunikationsteknologi

4.3. PIN-godkendelse

4.4. Meddelelsesformat

4.5. Førerens samtykke

4.6. Hentning af standarddata

4.7. Hentning af personoplysninger

4.8. Hentning af data om hændelser og fejl

1. INDLEDNING

I dette tillæg specificeres den udformning og de procedurer, der skal følges for at implementere interfacet med intelligente transportsystemer (ITS) i henhold til kravet i artikel 10 i forordning (EU) nr. 165/2014 (*forordningen*).

I forordningen angives det, at takografer på køretøjer kan udstyres med standardiserede interfaces, der gør det muligt at anvende de data, der registreres eller frembringes af takografen, i en ekstern enhed, under forudsætning af at følgende betingelser er opfyldt:

a) Interfacet påvirker ikke ægtheden og integriteten af takografens data.

b) Interfacet overholder de detaljerede bestemmelser i artikel 11 i forordningen.

c) Den eksterne anordning, der er forbundet med interfacet, har først adgang til personoplysninger, herunder geolokaliseringsdata, efter bevisligt samtykke fra den fører, som dataene vedrører.

2. ANVENDELSESOMRÅDE

Formålet med dette tillæg er at specificere, hvordan applikationer på eksterne anordninger kan hente (*dataene*) fra en takograf via en Bluetooth®-forbindelse.

Dataene, der er tilgængelige via dette interface, beskrives i bilag 1 i dette dokument. Dette interface tillader ikke implementering af andre interfaces (f.eks. via CAN-bussen) til at overføre dataene fra køretøjsenheden til andre køretøjsprocessorer.

▼B

I dette tillæg specificeres:

— *dataene*, der er tilgængelige via ITS-interfacet

— Bluetooth®-profilen, der anvendes til overførsel af dataene

— anmodnings- og overførselsprocedurer samt transaktionernes rækkefølge

— parringsmekanismen mellem takografen og den eksterne anordning

— samtykkemekanismen, som er til rådighed for føreren.

Det skal præciseres, at følgende ikke specificeres i dette bilag:

— indsamling af *dataene* og håndtering af disse i køretøjsenheden (som specificeres andetsteds i *forordningen* eller på anden måde er en funktion af produktdesignet)

— formatet for præsentationen af de indsamlede data til applikationen på den eksterne anordning

— ovenstående datasikkerhedsbestemmelser vedrørende Bluetooth® (såsom kryptering) for så vidt angår indholdet af *dataene* (som angives andetsteds i *forordningen* [tillæg 10, Fælles sikkerhedsmekanismer])

— Bluetooth®-protokollerne, som ITS-interfacet benytter.

2.1. **Akronymer, definitioner og notation**

Følgende akronymer og definitioner anvendes i dette tillæg:

Kommunikation	Udveksling af information/data mellem en masterenhed (dvs. takograferne) og en ekstern enhed via ITS-interfacet over Bluetooth®.
Dataene	Datasæt som fastlagt i bilag 1.
Forordningen	Europa-Parlamentets og Rådets forordning (EU) nr. 165/2014 af 4. februar 2014 om takografer inden for vejtransport, om ophævelse af Rådets forordning (EØF) nr. 3821/85 om kontrolapparatet inden for vejtransport og om ændring af Europa-Parlamentets og Rådets forordning (EF) nr. 561/2006 om harmonisering af visse sociale bestemmelser inden for vejtransport.
BR	Basishastighed
EDR	Forøget datahastighed
GNSS	Globalt satellitnavigationssystem
IRK	Identitetsudvekslingnøgle
ITS	Intelligent transportsystem
LE	Lavt energiindhold
PIN	Personnummer
PUK	Personlig frigivelseskode
SID	Tjenesteidentifikator
SPP	Profil for seriel port

▼B

SSP	Sikker simpel parring
TRTP	Parameter for anmodning om overførsel
TREP	Parameter for svar på overførsel
VU	Køretøjsenhed

3. HENVISNINGER TIL FORORDNINGER OG STANDARDER

Specifikationen, som fastlægges i dette tillæg, henviser til og er baseret på følgende forordninger og standarder, enten helt eller delvist. I bestemmelserne i dette tillæg angives de relevante standarder eller de relevante bestemmelser i standarderne. Hvis der er modstrid mellem kravene, har bestemmelserne i dette tillæg forrang.

I dette tillæg henvises der til følgende forordninger og standarder:

— Europa-Parlamentets og Rådets forordning (EU) nr. 165/2014 af 4. februar 2014 om takografer inden for vejtransport, om ophævelse af Rådets forordning (EØF) nr. 3821/85 om kontrolapparatet inden for vejtransport og om ændring af Europa-Parlamentets og Rådets forordning (EF) nr. 561/2006 om harmonisering af visse sociale bestemmelser inden for vejtransport.

— Europa-Parlamentets og Rådets forordning (EF) nr. 561/2006 af 15. marts 2006 om harmonisering af visse sociale bestemmelser inden for vejtransport og om ændring af Rådets forordning (EØF) nr. 3821/85 og (EF) nr. 2135/98 samt ophævelse af Rådets forordning (EØF) nr. 3820/85

— ISO 16844 — 4: Road vehicles — Tachograph systems — Part 4: Can-interface

— ISO 16844 — 7: Road vehicles — Tachograph systems — Part 7: Parametre

— Bluetooth® — Serial Port Profile — V1.2

— Bluetooth® — Core Version 4.2

— NMEA 0183 V4.1 protokol

4. FUNKTIONSPRINCIPPER FOR INTERFACE

4.1. **Forudsætninger for dataoverførsel via ITS-interfacet**

Køretøjsenheden er ansvarlig for at have ajourførte data gemt i køretøjsenheden, uden at ITS-interfacet involveres. Metoderne til sikring af dette ligger internt i køretøjsenheden og angives andetsteds i forordningen og angives derfor ikke i dette tillæg.

4.1.1 *Data overført via ITS-interfacet*

Køretøjsenheden er ansvarlig for at ajourføre de data, der vil være tilgængelige via ITS-interfacet med en hyppighed, der fastsættes i procedurerne for køretøjsenheden, uden at ITS-interfacet involveres. Dataene fra køretøjsenheden bruges som input og til at ajourføre *dataene*, og metoderne til dette angives andetsteds i *forordningen*, eller hvor der ikke findes en sådan angivelse, er det en del af produktdesignet og angives ikke i dette tillæg.

▼B

4.1.2 *Indholdet af dataene*

Indholdet af *dataene* er som angivet i bilag 1 til dette tillæg.

4.1.3 *ITS-applikationer*

ITS-applikationer vil anvende de data, der stilles til rådighed via ITS-interfacet, til f.eks. at optimere forvaltningen af førerens aktiviteter under hensyntagen til forordningen, til at detektere mulige fejl ved takografen eller til at bruge GNSS-dataene. Specifikationen af applikationerne ligger ikke inden for dette tillægs område.

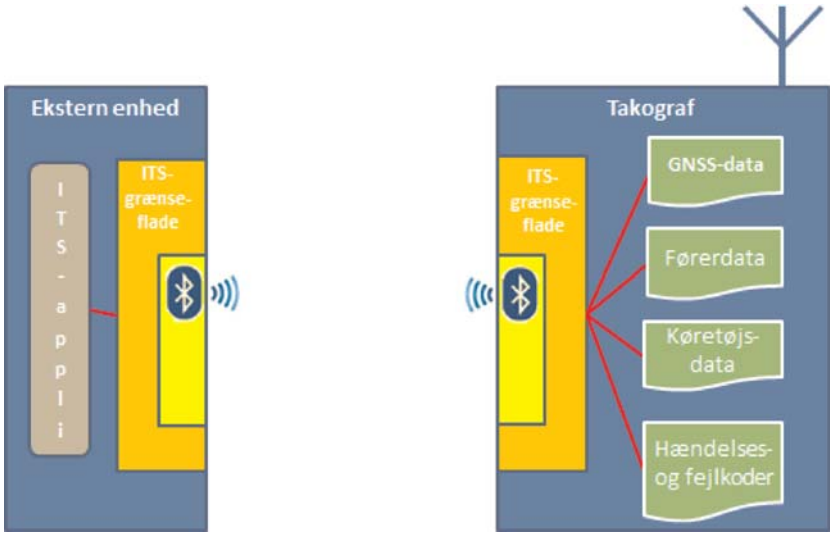
4.2. **Kommunikationsteknologi**

Udveksling af *data* via ITS-interfacet foregår via et Bluetooth®-interface, der er kompatibelt med version 4.2 eller senere. Bluetooth® fungerer i det industrielle, videnskabelige og medicinske (ISM) bånd fra 2,4 til 2,485 GHz, hvor der ikke kræves tilladelser. Bluetooth® 4.2 tilbyder forbedret beskyttelse af personoplysninger og sikkerhedsmekanismer samt bedre hastighed og pålidelighed ved dataoverførslerne. I forbindelse med denne specifikation er Bluetooth® klasse 2-radio, der anvendes med en rækkevidde på op til 10 meter. Der findes flere oplysninger om Bluetooth® 4.2 på www.bluetooth.com (https://www.bluetooth.org/en-us/specification/adopted-specifikations?_ga=1.215147412.2083380574.1435305676).

Kommunikationen etableres med kommunikationsudstyret, efter at en parringsproces er gennemført af en godkendt anordning. Eftersom Bluetooth® benytter master/slave-modellen til at kontrollere, hvornår og hvor anordninger kan sende data, spiller takografen rollen som master, mens den eksterne anordning er slave.

Når en ekstern anordning kommer inden for køretøjsenhedens rækkevidde første gang, kan Bluetooth®-parringsprocessen indledes (se også bilag 2). Anordningerne udveksler adresser, navne og profiler og den fælles hemmelige nøgle, som giver dem mulighed for at koble sig sammen, hver gang de er sammen fremover. Når dette trin er afsluttet, er den eksterne anordning godkendt og i stand til at indlede anmodninger om dataoverførsel fra takografen. Der er ikke planer om at tilføje krypteringsmekanismer ud over dem, som Bluetooth® tilbyder. Men hvis der er behov for yderligere sikkerhedsmekanismer, vil dette ske i overensstemmelse med tillæg 10, Fælles sikkerhedsmekanismer.

Det overordnede kommunikationsprincip beskrives i følgende figur.



▼B

SPP (Serial Port Profile) i Bluetooth® anvendes til at overføre data fra køretøjsenheden til den eksterne anordning.

4.3. **PIN-godkendelse**

Af sikkerhedshensyn kræver køretøjsenheden et godkendelsessystem med PIN-kode, som er separat fra Bluetooth-parringen. Hver køretøjsenhed skal kunne generere PIN-koder bestående af mindst fire cifre med henblik på ægthedskontrol. Hver gang en ekstern anordning parres med køretøjsenheden, skal den opgive den korrekte PIN-kode, før den modtager data.

Hvis PIN-koden angives korrekt, sættes anordningen på positivlisten. Positivlisten gemmer mindst 64 anordninger, der er parret med den pågældende køretøjsenhed.

Hvis der angives en forkert PIN-kode tre gange i træk, anbringes anordningen midlertidigt på negativlisten. Mens en anordning er på negativlisten, afvises alle nye forsøg på parring fra anordningen. Hvis der herefter igen angives en forkert PIN-kode tre gange i træk, anbringes anordningen på negativlisten i stadig længere perioder. Angivelse af den korrekte PIN-kode betyder, at blokeringen og antallet af forsøg nulstilles. Figur 1 i bilag 2 viser sekvensdiagrammet for forsøg på PIN-validering.

Tabel 1

Blokeringens varighed afhængigt af antallet af på hinanden mislykkede forsøg på at angive den korrekte PIN-kode

Antal på hinanden følgende mislykkede forsøg	Blokeringens varighed
3	30 sekunder
6	5 minutter
9	1 time
12	24 timer
15	Permanent

Hvis der angives en forkert PIN-kode 15 gange (5 × 3) i træk, anbringes ITS-enheden permanent på negativlisten. Denne permanente blokering kan kun ophæves ved angivelse af den korrekte PUK-kode.

PUK-koden består af 8 cifre og leveres af fabrikanten af køretøjsenheden. Hvis der angives en forkert PUK-kode 10 gange i træk, vil ITS-enheden blive permanent anbragt på negativlisten.

Selv om fabrikanten kan tilbyde en mulighed for at ændre PIN-koden direkte gennem køretøjsenheden, kan PUK-koden ikke ændres. Hvis det er muligt at ændre PIN-koden, kræver det, at den aktuelle PIN-kode kan indtastes direkte i køretøjsenheden.

Derudover skal anordninger, der gemmes på positivlisten, bevares, indtil de fjernes manuelt af brugeren (f.eks. via brugerinterfacet på køretøjsenheden eller med andre metoder). Dette betyder, at forsvundne eller stjålne ITS-enheder kan fjernes fra positivlisten. Enhver ITS-enhed, der forlader Bluetooth-forbindelsens rækkevidde i mere end 24 timer, skal ligeledes fjernes fra køretøjsenhedens positivliste og skal angive den korrekte PIN-kode igen, når forbindelsen skal genoprettes.

▼B

Formatet af meddelelser mellem køretøjsenhedens interface og køretøjsenheden fastlægges ikke, men overlades til fabrikanten. Den pågældende fabrikant skal imidlertid sikre, at meddelelsesformatet mellem ITS-enheden og køretøjsenhedens interface overholdes (se ASN.1-specifikationer).

Enhver dataanmodning skal derfor mødes med en vellykket verifikation af afsenderens oplysninger, inden der sker nogen form for databehandling. Figur 2 i bilag 2 viser sekvensdiagrammet for denne procedure. Enhver anordning på negativlisten modtager en automatisk afvisning, enhver anordning, der hverken befinder sig på negativlisten eller positivlisten, modtager en anmodning om PIN-kode, som den skal imødekomme, inden den sender sin dataanmodning på ny.

4.4. **Meddelelsesformat**

Alle meddelelser, som udveksles mellem ITS-enheden og køretøjsenhedens interface, er formateret med en tredelt struktur: En header bestående af en destinationsbyte (TGT), en kildebyte (SRC) og en længdebyte (LEN),

Datafeltet bestående af en serviceidentifikatorbyte (SID) og et variabelt antal databyte (højst 255).

Kontrolsumbyten er 1 bit-sumserie modulo 256 for alle meddelelsens byte bortset fra selve kontrolsummen.

Meddelelsen af Big Endian.

Tabel 2

Overordnet meddelelsesformat

Header			Datafelt					Kontrolsum
TGT	SRC	LEN	SID	TRTP	CC	CM	DATA	CS
3 byte			Maks. 255 byte					1 byte

Header

TGT og SRC: ID for mål- (TGT) og kilde- (SRC) anordninger for meddelelsen. Køretøjsenhedens interface har standard-ID'en ”EE”. Denne ID kan ikke ændres. ITS-enheden benytter standard-ID'en ”A0” til sin første meddelelse i kommunikationssessionen. Køretøjsenhedens interface tildeler herefter ITS-enheden en entydig ID og underretter den om denne ID til brug for kommende meddelelser i løbet af sessionen.

LEN-byten tager kun hensyn til ”DATA”-delen af datafeltet (se tabel 2), de 4 første byte er underforståede.

Køretøjsenhedens interface bekræfter ægtheden af meddelelsens afsender ved at krydskontrollere sin egen ID-liste med Bluetooth-dataene ved at kontrollere ITS-enheden, der står opført med den opgivne ID inden for Bluetooth-forbindelsens rækkevidde.

Datafelt

Ud over SID'en skal datafeltet ligeledes indeholde andre parametre: en parameter for overførselsanmodning (TRTP) og tællerbyte.

▼B

Hvis de data, der skal overføres, er for lange til at kunne rummes i en meddelelse, opdeles de i flere delmeddelelser. Hver delmeddelelse skal have samme header og SID, men indeholder en tæller på 2 byte, Counter Current (CC) og Counter Max (CM), som angiver nummeret på delmeddelelsen. For at der skal kunne foretages fejlkontrol og afbrydelse, kvitterer den modtagende enhed for hver delmeddelelse. Den modtagende enhed kan acceptere delmeddelelsen, anmode om, at den overføres på ny, anmode den afsendende enhed om at starte forfra eller afbryde dataoverførslen.

Hvis CC og CM ikke anvendes, tildeles de værdien 0xFF.

F.eks. sendes følgende meddelelse

HEADER	SID	TRTP	CC	CM	DATA	CS
3 byte	Længere end 255 byte					1 byte

således:

HEADER	SID	TRTP	01	n	DATA	CS
3 byte	255 byte					1 byte

HEADER	SID	TRTP	02	n	DATA	CS
3 byte	255 byte					1 byte

…

HEADER	SID	TRTP	N	N	DATA	CS
3 byte	Maks. 255 byte					1 byte

Tabel 3 indeholder de meddelelser, som køretøjsenheden og ITS-enheden skal kunne udveksle. Indholdet af de enkelte parametre angives i hexadecimalformat. Tabellen indeholder ikke CC og CM af tydelighedshensyn; det fuldstændige format vises ovenfor.

Tabel 3

Detaljeret meddelelsesindhold

Meddelelse	Header			DATA			Kontrol-sum
	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

Meddelelse	Header			DATA			Kontrol-sum
	TGT	SRC	LEN	SID	TRTP	DATA	
BanLiftingResult	*ITSID*	EE	01	06	FF	BOOLEAN (T/F)	
RequestRejected	*ITSID*	EE	08	07	FF	Klokkeslæt	
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							
Ingen tilgængelige data	*ITSID*	EE	02	0A	TREP	10	
Personoplysninger ikke delt	*ITSID*	EE	02	0A	TREP	11	
NegativeAnswer							
Generel afvisning	*ITSID*	EE	02	0B	SID Req	10	
Tjeneste understøttes ikke	*ITSID*	EE	02	0B	SID Req	11	
Delfunktion understøttes ikke	*ITSID*	EE	02	0B	SID Req	12	
Ukorrekt meddelelseslængde	*ITSID*	EE	02	0B	SID Req	13	
Betingelser ikke korrekte eller fejl i anmodningssekvens	*ITSID*	EE	02	0B	SID Req	22	
Anmodning uden for gyldighedsområde	*ITSID*	EE	02	0B	SID Req	31	
Afventer svar	*ITSID*	EE	02	0B	SID Req	78	
Uoverensstemmelse for ITSID	*ITSID*	EE	02	0B	SID Req	FC	
ITSID ikke fundet	*ITSID*	EE	02	0B	SID Req	FB	

RequestPIN (SID 01)

Denne meddelelse udstedes af køretøjsenhedens interface, hvis en ITS, der ikke er på negativlisten, men heller ikke på positivlisten, sender en dataanmodning.

▼B

SendITSID (SID 02)

Denne meddelelse udstedes af køretøjsenhedens interface, når en ny anordning sender en anmodning. Denne anordning benytter standard-ID'en ”A0”, før den tildeles en entydig ID til kommunikationssessionen.

SendPIN (SID 03)

Denne meddelelse udstedes af ITS-enheden, som skal påføres positivlisten fra køretøjsenhedens interface. Indholdet af denne meddelelse er en kode på 4 HELTAL mellem 0 og 9.

PairingResult (SID 04)

Denne meddelelse udstedes af køretøjsenhedens interface for at informere ITS-enheden om, hvorvidt den fremsendte PIN-kode er korrekt. Indholdet af denne meddelelse er BOOLEAN med værdien ”True”, hvis PIN-koden var korrekt, og ”False”, hvis den ikke var.

SendPUC (SID 05)

Denne meddelelse udstedes af ITS-enheden for at ophæve en opførelse på negativlisten fra køretøjsenhedens interface. Indholdet af denne meddelelse er en kode på 8 HELTAL mellem 0 og 9.

BanLiftingResult (SID 06)

Denne meddelelse udstedes af køretøjsenhedens interface for at informere ITS-enheden om, hvorvidt den sendte PUK-kode var korrekt. Indholdet af denne meddelelse er BOOLEAN med værdien ”True”, hvis PUK-koden var korrekt, og ”False”, hvis den ikke var.

RequestRejected (SID 07)

Denne meddelelse udstedes af køretøjsenhedens interface som svar på en meddelelse fra en ITS-enhed på negativlisten, undtagen ”SendPUC”. Meddelelsen indeholder den resterende tid, som ITS-enheden står på negativlisten, efterfulgt af ”Time”-sekvensformatet som defineret i bilag 3.

RequestData (SID 08)

Denne meddelelse til dataadgang udstedes af ITS-enheden. Datatypen angives af en parameter for anmodning om dataoverførsel (TRTP) på en byte. Der findes flere datatyper:

— standardTachData (TRTP 01): Data fra takografen, der er klassificeret som ikke-personoplysninger.

— personalTachData (TRTP 02): Data fra takografen, der er klassificeret som personoplysninger.

— gnssData (TRTP 03): GNSS-data, altid personoplysninger.

— standardEventData (TRTP 04): Registrerede hændelsesdata, der er klassificeret som ikke-personoplysninger.

— personalEventData (TRTP 05): Registrerede hændelsesdata, der er klassificeret som personoplysninger.

— standardFaultData (TRTP 06): Registrerede fejl, der er klassificeret som ikke-personoplysninger.

— manufacturerData (TRTP 07): Data, der stilles til rådighed af fabrikanten.

▼B

Se bilag 3 i dette tillæg for flere oplysninger om indholdet af de enkelte datatyper.

Se tillæg 12 for flere oplysninger om GNSS-datas format og indhold.

Se bilag IB og IC for flere oplysninger om koden for hændelsesdata og fejl.

ResquestAccepted (SID 09)

Denne meddelelse udstedes af køretøjsenhedens interface, hvis en ITS-enheds "RequestData"-meddelelse er accepteret. Denne meddelelse indeholder en TREP på 1 byte, som er TRTP-byten for den tilhørende RequestData-meddelelse, samt alle data af den ønskede type.

DataUnavailable (SID 0A)

Denne meddelelse udstedes af køretøjsenhedens interface, hvis de ønskede data af en bestemt grund ikke er til rådighed for fremsendelse til en ITS-enhed på positivlisten. Meddelelsen indeholder en TREP på 1 byte, som er TRTP'en for de ønskede data, og en fejlkode på 1 byte, som specificeres i tabel 3. Følgende koder er til rådighed:

— Ingen tilgængelige data (10): Køretøjsenhedens interface kan ikke få adgang til dataene på køretøjsenheden af ikke nærmere angivne årsager.

— Personoplysninger ikke delt (11): ITS-enheden forsøger at hente personoplysninger, når de ikke er delt.

NegativeAnswer (SID 0B)

Disse meddelelser udstedes af køretøjsenhedens interface, hvis en anmodning ikke kan gennemføres af en anden grund, end at dataene ikke er tilgængelige. Disse meddelelser er typisk resultatet af et forkert anmodningsformat (længde, SID, ITSID osv.), men kan også have andre årsager. TRTP i datafeltet indeholder forespørgslens SID. Datafeltet indeholder en kode, der angiver årsagen til det negative svar. Følgende koder er til rådighed:

— Generel afvisning (kode: 10)

— Handlingen kan ikke gennemføres af en årsag, der ikke nævnes nedenfor eller i afsnit (indsæt afsnitsnummer for *DataUnavailable*).

— Tjeneste understøttes ikke (kode: 11)

— Forespørgslens SID kan ikke forstås.

— Delfunktion understøttes ikke (kode: 12)

— Forespørgslens TRTP kan ikke forstås. Det kan f.eks. skyldes manglende værdier eller værdier uden for gyldighedsområdet.

— Forkert meddelelseslængde (kode: 13)

— Længden af den modtagne meddelelse er forkert (uoverensstemmelse mellem LEN-byten og meddelelsens faktiske længde).

— Betingelser ikke korrekte eller fejl i anmodningssekvens (kode: 22)

— Tjenesten, der anmodes om, er ikke aktiv, eller sekvensen af anmodningsmeddelelser er ukorrekt.

— Anmodning uden for gyldighedsområde (kode: 33)

▼B

— Posten med anmodningens parametre (datafelt) ugyldig.

— Afventer svar (kode: 78)

— Operationen, der anmodes om, kan ikke gennemføres i tide, og køretøjsenheden er ikke klar til at modtage endnu en anmodning.

— Uoverensstemmelse med *ITSID* (kode: FB)

— SRC'ens *ITSID* stemmer ikke overens med den tilhørende anordning efter sammenligning med Bluetooth-oplysningerne.

— *ITSID* ikke fundet (kode: FC)

— SRC'ens *ITSID* er ikke tilknyttet nogen anordning.

Linje 1 til og med 72 (**FormatMessageModule**) i ASN.1-koden i bilag 3 angiver meddelelsesformatet som beskrevet i tabel 3. Der findes nærmere oplysninger om meddelelsesindholdet nedenfor.

4.5. **Førerens samtykke**

Alle tilgængelige data klassificeres som enten standard eller personlige. Personoplysninger er kun tilgængelige, hvis føreren har givet sit samtykke og accepteret, at vedkommendes personlige takografoplysninger kan forlade køretøjets netværk til tredjepartsanvendelser.

Førerens samtykke gives, når kortindehaveren, første gang et givet førerkort eller værkstedskort, der i øjeblikket er ukendt af køretøjsenheden, isættes, og kortindehaveren opfordres til at give sit samtykke til, at takografrelaterede personoplysninger kan sendes via det valgfri ITS-interface. (se også bilag I C punkt 3.6.2).

Samtykkestatus (givet/ikke givet) registreres i takografens hukommelse.

Hvis der er tale om flere førere, vil kun personoplysninger om førere, der har givet deres samtykke, blive delt med ITS-interfacet. Hvis der f.eks. er to førere på køretøjet, og kun den første har indvilget i at dele sine personoplysninger, vil personoplysningerne for den anden fører ikke blive delt.

4.6. **Hentning af standarddata**

Figur 3 i bilag 2 viser sekvensdiagrammerne for gyldige anmodninger fra ITS-enheden om adgang til standarddata. Hvis ITS-enheden står på positivlisten og ikke anmoder om personoplysninger, kræves der ikke nogen yderligere verifikation. I diagrammerne forudsættes det, at den korrekte procedure, som fremgår af figur 2 i bilag 2, er blevet fulgt. De kan sammenlignes med det grå felt *REQUEST TREATMENT* i figur 2.

Følgende data blandt de tilgængelige data betragtes som standard:

— standardTachData (TRTP 01)

— StandardEventData (TRTP 04)

— standardFaultData (TRTP 06)

4.7. **Hentning af personoplysninger**

Figur 4 i bilag 2 viser sekvensdiagrammet for behandling af anmodninger om personoplysninger. Som anført tidligere sender køretøjsenhedens interface kun personoplysninger, hvis føreren har givet sit udtrykkelige samtykke (se også 4.5). Ellers skal anmodningen automatisk afvises.

▼B

Følgende data blandt de tilgængelige data betragtes som personoplysninger:

— personalTachData (TRTP 02)

— gnssData (TRTP 03)

— personalEventData (TRTP 05)

— manufacturerData (TRTP 07)

4.8. **Hentning af data om hændelser og fejl**

ITS-enheder skal kunne anmode om hændelsesdata, der indeholder en liste over alle uforudsete hændelser. Disse data betragtes som standarddata eller personoplysninger, se bilag 3. Indholdet af de enkelte hændelser er i overensstemmelse med dokumentationsmaterialet i bilag 1 i dette tillæg.

▼B

BILAG 1

LISTE OVER TILGÆNGELIGE DATA VIA ITS-INTERFACET

Data	Kilde	►C2 Dataklassificering (personlig/ikke personlig) ◄
VehicleIdentificationNumber	Køretøjsenhed	**ikke personlig**
CalibrationDate	Køretøjsenhed	**ikke personlig**
TachographVehicleSpeed speed instant t	Køretøjsenhed	personlig
Driver1WorkingState Selector driver	Køretøjsenhed	personlig
Driver2WorkingState	Køretøjsenhed	personlig
DriveRecognize Speed Threshold detected	Køretøjsenhed	**ikke personlig**
Driver1TimeRelatedStates Weekly day time	Førerkort	personlig
Driver2TimeRelatedStates	Førerkort	personlig
DriverCardDriver1	Køretøjsenhed	**ikke personlig**
DriverCardDriver2	Køretøjsenhed	**ikke personlig**
OverSpeed	Køretøjsenhed	personlig
TimeDate	Køretøjsenhed	**ikke personlig**
HighResolutionTotalVehicleDistance	Køretøjsenhed	**ikke personlig**
ServiceComponentIdentification	Køretøjsenhed	**ikke personlig**
ServiceDelayCalendarTimeBased	Køretøjsenhed	**ikke personlig**
Driver1Identification	Førerkort	personlig
Driver2Identification	Førerkort	personlig
NextCalibrationDate	Køretøjsenhed	**ikke personlig**
Driver1ContinuousDrivingTime	Førerkort	personlig
Driver2ContinuousDrivingTime	Førerkort	personlig
Driver1CumulativeBreakTime	Førerkort	personlig
Driver2CumulativeBreakTime	Førerkort	personlig
Driver1CurrentDurationOfSelectedActivity	Førerkort	personlig
Driver2CurrentDurationOfSelectedActivity	Førerkort	personlig
SpeedAuthorised	Køretøjsenhed	**ikke personlig**
TachographCardSlot1	Førerkort	**ikke personlig**
TachographCardSlot2	Førerkort	**ikke personlig**
Driver1Name	Førerkort	personlig
Driver2Name	Førerkort	personlig

▼B

Data	Kilde	►C2 Dataklassificering (personlig/ikke personlig) ◄
OutOfScopeCondition	Køretøjsenhed	**ikke personlig**
ModeOfOperation	Køretøjsenhed	**ikke personlig**
Driver1CumulatedDrivingTimePreviousAndCurrentWeek	Førerkort	personlig
Driver2CumulatedDrivingTimePreviousAndCurrentWeek	Førerkort	personlig
EngineSpeed	Køretøjsenhed	personlig
RegisteringMemberState	Køretøjsenhed	**ikke personlig**
VehicleRegistrationNumber	Køretøjsenhed	**ikke personlig**
Driver1EndOfLastDailyRestPeriod	Førerkort	personlig
Driver2EndOfLastDailyRestPeriod	Førerkort	personlig
Driver1EndOfLastWeeklyRestPeriod	Førerkort	personlig
Driver2EndOfLastWeeklyRestPeriod	Førerkort	personlig
Driver1EndOfSecondLastWeeklyRestPeriod	Førerkort	personlig
Driver2EndOfSecondLastWeeklyRestPeriod	Førerkort	personlig
Driver1CurrentDailyDrivingTime	Førerkort	personlig
Driver2CurrentDailyDrivingTime	Førerkort	personlig
Driver1CurrentWeeklyDrivingTime	Førerkort	personlig
Driver2CurrentWeeklyDrivingTime	Førerkort	personlig
Driver1TimeLeftUntilNewDailyRestPeriod	Førerkort	personlig
Driver2TimeLeftUntilNewDailyRestPeriod	Førerkort	personlig
Driver1CardExpiryDate	Førerkort	personlig
Driver2CardExpiryDate	Førerkort	personlig
Driver1CardNextMandatoryDownloadDate	Førerkort	personlig
Driver2CardNextMandatoryDownloadDate	Førerkort	personlig
TachographNextMandatoryDownloadDate	Køretøjsenhed	**ikke personlig**
Driver1TimeLeftUntilNewWeeklyRestPeriod	Førerkort	personlig
Driver2TimeLeftUntilNewWeeklyRestPeriod	Førerkort	personlig
Driver1NumberOfTimes9hDailyDrivingTimesExceeded	Førerkort	personlig
Driver2NumberOfTimes9hDailyDrivingTimesExceeced	Førerkort	personlig

▼B

Data	Kilde	►C2 Dataklassificering (personlig/ikke personlig) ◄
Driver1CumulativeUninterruptedRestTime	Førerkort	personlig
Driver2CumulativeUninterruptedRestTime	Førerkort	personlig
Driver1MinimumDailyRest	Førerkort	personlig
Driver2MinimumDailyRest	Førerkort	personlig
Driver1MinimumWeeklyRest	Førerkort	personlig
Driver2MinimumWeeklyRest	Førerkort	personlig
Driver1MaximumDailyPeriod	Førerkort	personlig
Driver2MaximumDailyPeriod	Førerkort	personlig
Driver1MaximumDailyDrivingTime	Førerkort	personlig
Driver2MaximumDailyDrivingTime	Førerkort	personlig
Driver1NumberOfUsedReducedDailyRestPeriods	Førerkort	personlig
Driver2NumberOfUsedReducedDailyRestPeriods	Førerkort	personlig
Driver1RemainingCurrentDrivingTime	Førerkort	personlig
Driver2RemainingCurrentDrivingTime	Førerkort	personlig
GNSS position	Køretøjsenhed	personlig

2) GNSS-DATA LØBENDE TILGÆNGELIGE MED FØRERS SAMTYKKE

Se tillæg 12 — GNSS.

3) HÆNDELSESKODER TILGÆNGELIGE UDEN FØRERS SAMTYKKE

Begivenhed	Lagringsbestemmelse	Data, som skal lagres for hver hændelse
Isætning af ugyldigt kort	— de 10 seneste hændelser	— dato og klokkeslæt for hændelsen — korttype, nummer, udstedende medlemsstat og generation for kortet, der oprettede hændelsen — antal tilsvarende hændelser den pågældende dag
Kortkonflikt	— de 10 seneste hændelser	— hændelsens startdato og -klokkeslæt — hændelsens slutdato og -klokkeslæt — korttype, nummer, udstedende medlemsstat og generation for de to kort, der skabte konflikten
Seneste kortsession ikke korrekt afsluttet	— de 10 seneste hændelser	— dato og klokkeslæt for isætning af kortet — korttype, kortnummer, udstedende medlemsstat og generation — de seneste sessionsdata, aflæst fra kortet: — dato og klokkeslæt for isætning af kortet — køretøjets indregistreringsnummer, indregistreringsmedlemsstat og køretøjsenhedens generation

▼B

Begivenhed	Lagringsbestemmelse	Data, som skal lagres for hver hændelse
Afbrydelse af strømforsyning (2)	— den længstvarige hændelse for hver af de 10 seneste dages forekomst — en af de 5 længstvarende hændelser inden for de sidste 365 dage	— hændelsens startdato og -klokkeslæt — hændelsens slutdato og -klokkeslæt — korttype, kortnummer og udstedende medlemsstat for ethvert kort, som er isat ved hændelsens start og/eller slutning — antal tilsvarende hændelser den pågældende dag
Kommunikationsfejl med fjernkommunikations-udstyret	— den længstvarende hændelse for hver af de 10 seneste dages forekomst — de 5 længstvarende hændelser inden for de sidste 365 dage	— hændelsens startdato og -klokkeslæt — hændelsens slutdato og -klokkeslæt — korttype, kortnummer og udstedende medlemsstat for ethvert kort, som er isat ved hændelsens start og/eller slutning — antal tilsvarende hændelser den pågældende dag
Manglende positionsoplysninger fra GNSS-modtager	— den længstvarende hændelse for hver af de 10 seneste dages forekomst — de 5 længstvarende hændelser inden for de sidste 365 dage	— hændelsens startdato og -klokkeslæt, — hændelsens slutdato og -klokkeslæt — korttype, kortnummer og udstedende medlemsstat for ethvert kort, som er isat ved hændelsens start og/eller slutning — antal tilsvarende hændelser den pågældende dag
Fejl i bevægelsesdata	— den længstvarende hændelse for hver af de 10 seneste dages forekomst — de 5 længstvarende hændelser inden for de sidste 365 dage	— hændelsens startdato og -klokkeslæt — hændelsens slutdato og -klokkeslæt — korttype, kortnummer og udstedende medlemsstat for ethvert kort, som er isat ved hændelsens start og/eller slutning — antal tilsvarende hændelser den pågældende dag
Køretøjsbevægelses-konflikt	— den længstvarende hændelse for hver af de 10 seneste dages forekomst — de 5 længstvarende hændelser inden for de sidste 365 dage	— hændelsens startdato og -klokkeslæt — hændelsens slutdato og -klokkeslæt — korttype, kortnummer og udstedende medlemsstat for ethvert kort, som er isat ved hændelsens start og/eller slutning — antal tilsvarende hændelser den pågældende dag
Forsøg på krænkelse af sikkerheden	de 10 seneste hændelser for hver type hændelse	— hændelsens startdato og -klokkeslæt — hændelsens slutdato og -klokkeslæt (hvis relevant) — korttype, kortnummer og udstedende medlemsstat for ethvert kort, som er isat ved hændelsens start og/eller slutning — hændelsens type

▼B

Begivenhed	Lagringsbestemmelse	Data, som skal lagres for hver hændelse
Tidskonflikt	— den længstvarende hændelse for hver af de 10 seneste dages forekomst — de 5 længstvarende hændelser inden for de sidste 365 dage	— kontrolapparat for dato og klokkeslæt — GNSS-dato og -klokkeslæt — korttype, kortnummer og udstedende medlemsstat for ethvert kort, som er isat ved hændelsens start og/eller slutning — antal tilsvarende hændelser den pågældende dag

4) TILGÆNGELIGE HÆNDELSESKODER MED FØRERS SAMTYKKE

Begivenhed	Lagringsbestemmelse	Data, som skal lagres for hver hændelse
Kørsel uden behørigt kort	— den længstvarende hændelse for hver af de 10 seneste dages forekomst — de 5 længstvarende hændelser inden for de sidste 365 dage	— hændelsens startdato og -klokkeslæt — hændelsens slutdato og -klokkeslæt — korttype, kortnummer og udstedende medlemsstat for ethvert kort, som er isat ved hændelsens start og/eller slutning — antal tilsvarende hændelser den pågældende dag
Isætning af kort under kørslen	— den seneste hændelse for hver af de 10 seneste dages forekomst	— dato og klokkeslæt for hændelsen — korttype, kortnummer, udstedende medlemsstat og generation — antal tilsvarende hændelser den pågældende dag
Overskridelse af tilladt hastighed (1)	— den alvorligste hændelse for hver af de seneste 10 dages forekomst (dvs. den, hvor gennemsnitshastigheden har været størst) — de 5 alvorligste hændelser inden for de sidste 365 dage — den første hændelse, som har fundet sted efter sidste kalibrering	— hændelsens startdato og -klokkeslæt — hændelsens slutdato og -klokkeslæt — den højeste hastighed målt under hændelsen — den aritmetiske gennemsnitshastighed målt under hændelsen — korttype, kortnummer, udstedende medlemsstat og generation for førerkortet (hvis relevant) — antal tilsvarende hændelser den pågældende dag

5) TILGÆNGELIGE FEJLDATAKODER UDEN FØRERS SAMTYKKE

Fejl	Lagringsbestemmelse	Data, som skal gemmes for hver hændelse
Kortfejl	— de 10 seneste kortfejl for førerkortet	— fejlens startdato og -klokkeslæt — fejlens slutdato og -klokkeslæt — korttype, kortnummer, udstedende medlemsstat og generation
Fejl ved kontrolapparatet	— de 10 seneste fejl af hver fejltype — den første fejl efter seneste kalibrering	— fejlens startdato og -klokkeslæt — fejlens slutdato og -klokkeslæt — fejltype — korttype, kortnummer og udstedende medlemsstat og generation for ethvert kort, som er isat ved fejlens start og/eller slutning

▼B

Denne fejl skal udløses, når et af nedenstående svigt forekommer, uden at apparatet er i kalibreringstilstand:

— Intern fejl i køretøjsenhed

— Printerfejl

— Displayfejl

— Dataoverførselsfejl

— Følerfejl

— Fejl på GNSS-modtager eller eksternt GNSS-udstyr

— Fejl på fjernkommunikationsudstyr.

6) FABRIKANTSPECIFIKKE HÆNDELSER OG FEJL UDEN FØRERS SAMTYKKE

Hændelse eller fejl	Lagringsbestemmelse	Data, som skal lagres for hver hændelse
Fastsættes af fabrikanten	Fastsættes af fabrikanten	Fastsættes af fabrikanten

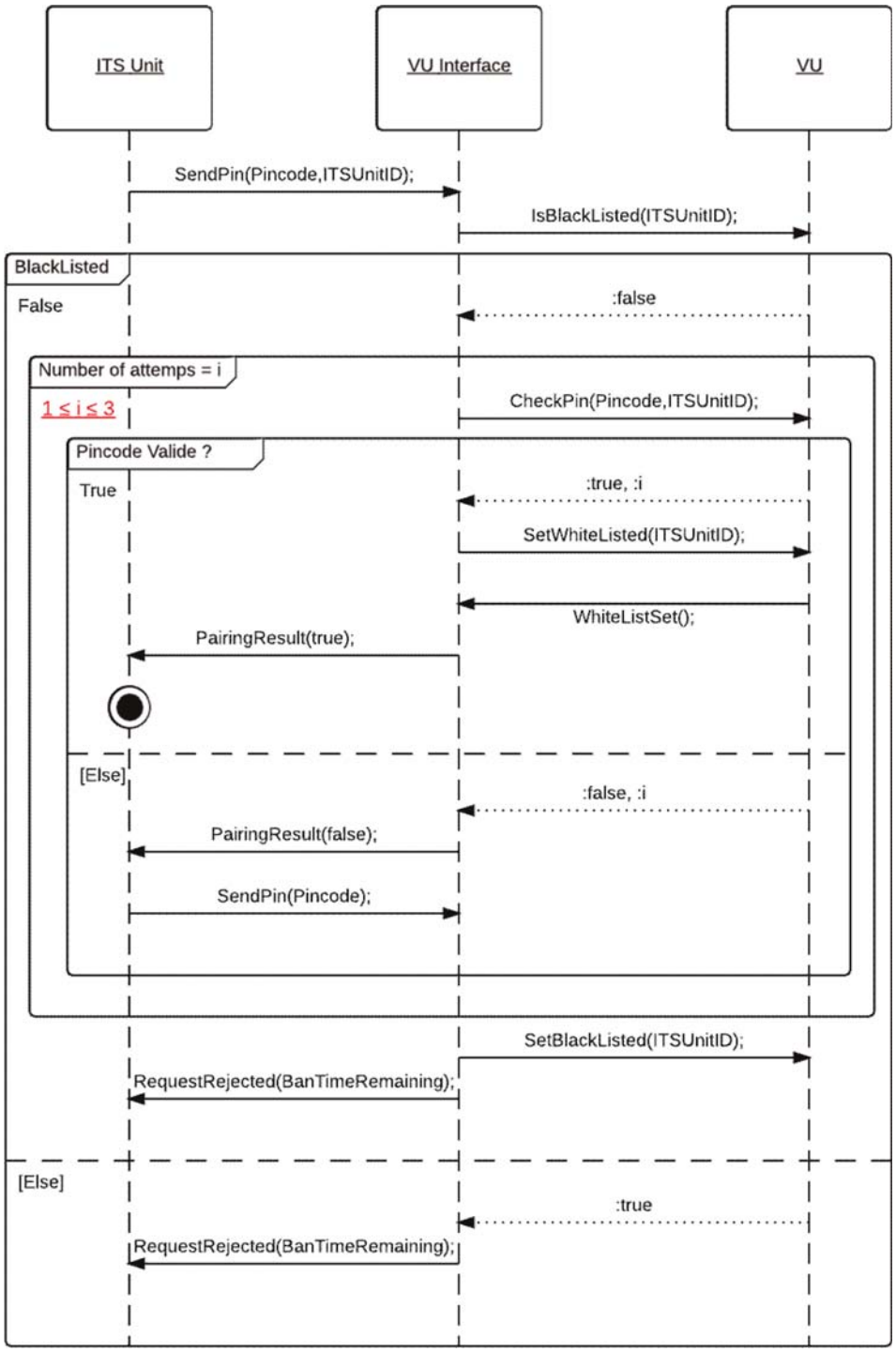
▼B

BILAG 2

SEKVENSDIAGRAMMER FOR MEDDELELSESUDVEKSLINGER MED ITS-ENHEDEN.

Figur 1.

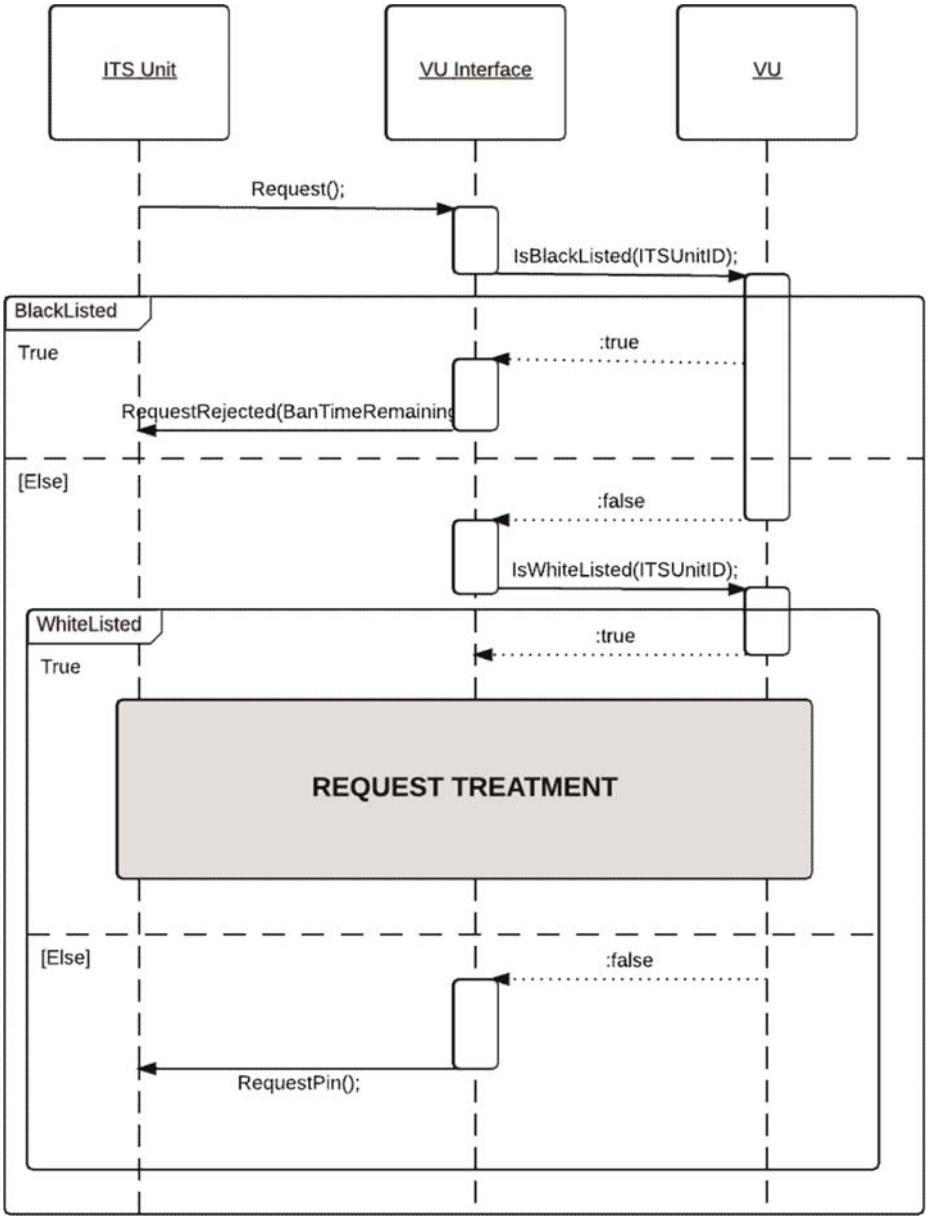
Sekvensdiagram for PIN-valideringsforsøg



▼B

Figur 2.

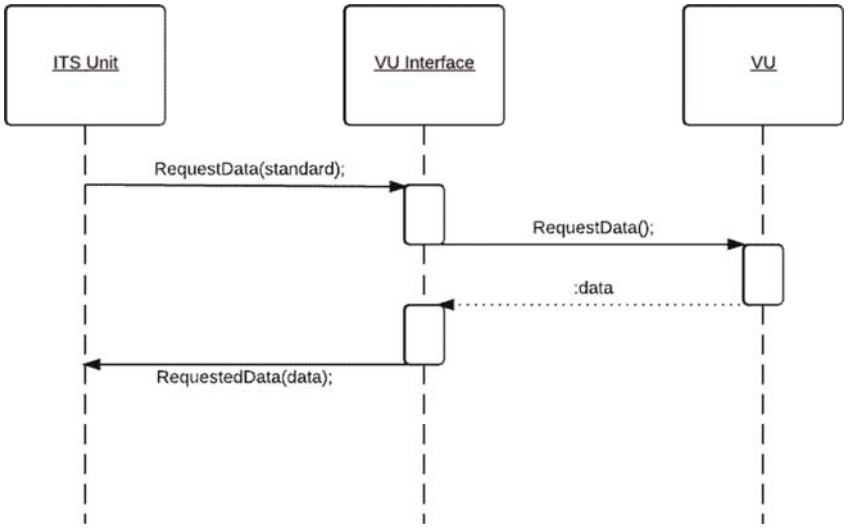
Sekvensdiagram for ITS-enhedens godkendelsesverifikation



▼B

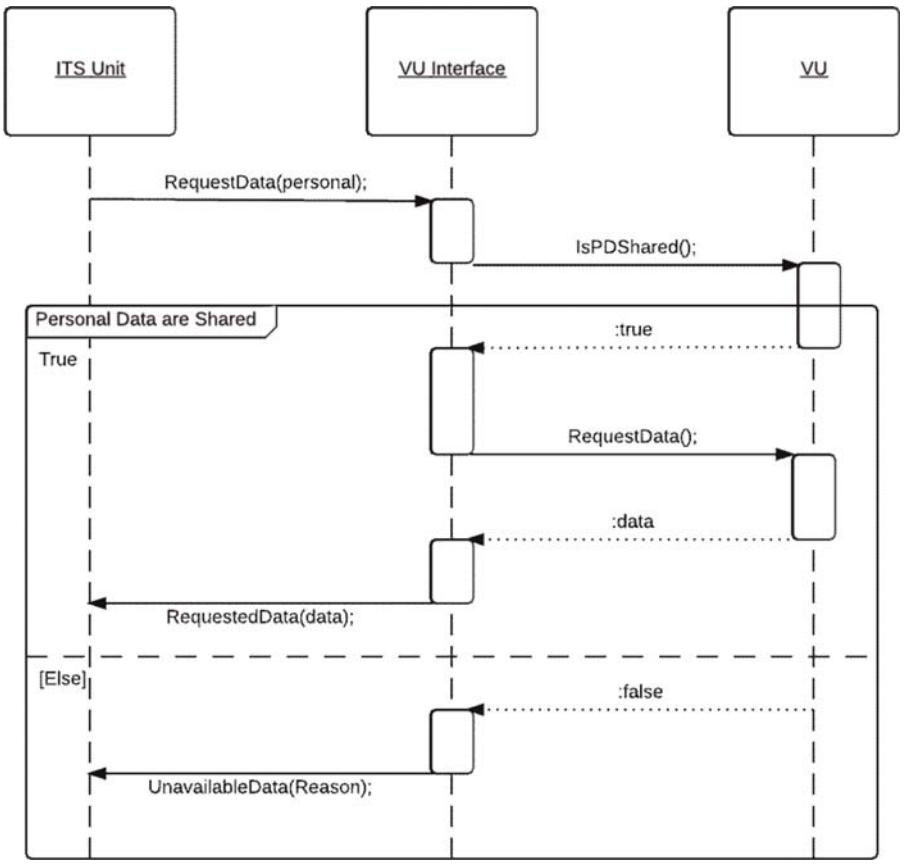
Figur 3.

Sekvensdiagram til behandling af anmodning om data, der er klassificeret som ikke-personoplysninger (efter korrekt PIN-adgang)



Figur 4.

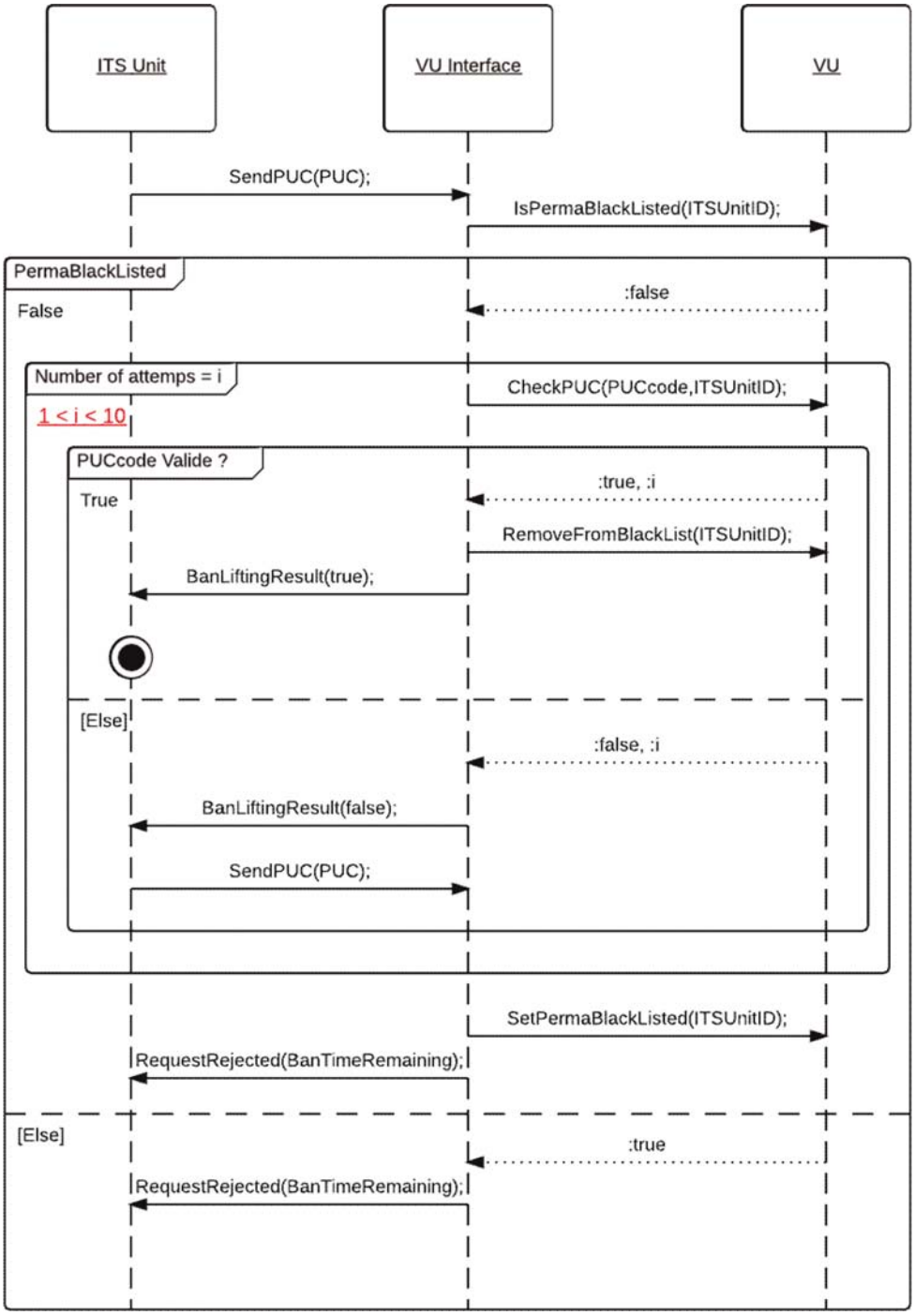
Sekvensdiagram til behandling af anmodning om data, der er klassificeret som personoplysninger (efter korrekt PIN-adgang)



▼B

Figur 5.

Sekvensdiagram for PUK-valideringsforsøg



▼B

BILAG 3

ASN.1 SPECIFICATIONS

```
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

```
                    beginDate GeneralizedTime,
                    endDate GeneralizedTime,
                    carsdType SEQUENCE OF UTF8String,
                    cardsNumber SEQUENCE OF INTEGER,
                    issuingMemberState SEQUENCE OF NationAlpha,
                    cardsGeneration SEQUENCE OF INTEGER,
             }

             RecordingEquipmentFault ::= SEQUENCE{
                    beginDate GeneralizedTime,
                    endDate GeneralizedTime,
                    faultType RecordingEquipmentFaultType,
                    carsdType SEQUENCE OF UTF8String,
                    cardsNumber SEQUENCE OF INTEGER,
                    issuingMemberState SEQUENCE OF NationAlpha,
                    cardsGeneration SEQUENCE OF INTEGER,
             }
END
```

▼B

Tillæg 14.

FJERNKOMMUNIKATIONSFUNKTION

INDHOLDSFORTEGNELSE

1 INDLEDNING

2 ANVENDELSESOMRÅDE

3 AKRONYMER, DEFINITIONER OG NOTATION

4 DRIFTSSCENARIER

4.1 Oversigt

4.1.1 Forudsætninger for dataoverførsel via 5,8 GHz DSRC-interface

4.1.2 Profil 1a: via en håndholdt eller midlertidig vejsidemonteret læser i udstyr til tidlig fjernafsløring

4.1.3 Profil 1b: via en køretøjsmonteret og dirigeret læser i udstyr til tidlig fjernafsløring.

4.2 Sikkerhed/integritet

5 DESIGN OG PROTOKOLLER TIL FJERNKOMMUNIKATION

5.1 Design

5.2 Arbejdsgang

5.2.1 Drift

5.2.2 Fortolkning af data modtaget via DSRC-kommunikationen

5.3 Fysiske DSRC-interfaceparametre til fjernkommunikation

5.3.1 Lokaliseringsbegrænsninger

5.3.2 Downlink- og uplink-parametre

5.3.3 Antennedesign

5.4 DSRC-protokolkrav til RTM

5.4.1 Oversigt

5.4.2 Kommandoer

5.4.3 Kommandosekvens ved anmodning

5.4.4 Datastrukturer

5.4.5 Elementer af RtmData, udførte handlinger og definitioner

5.4.6 Dataoverførselsmekanisme

5.4.7 Detaljeret DSRC-transaktionsbeskrivelse

5.4.8 Beskrivelse af DSRC-afprøvningstransaktion

5.5 Understøttelse af direktiv 2015/71/EF

5.5.1 Oversigt

5.5.2 Kommandoer

▼B

5.5.3 Kommandosekvens ved anmodning

5.5.4 Datastrukturer

5.5.5 ASN.1-modul til OWS DSRC-transaktionen

5.5.6 Elementer i OwsData, udførte handlinger og definitioner

5.5.7 Dataoverførselsmekanismer

5.6 Dataoverførsel mellem DSRC-køretøjsenheden og køretøjsenheden

5.6.1 Fysisk forbindelse og interfaces

5.6.2 Applikationsprotokol

5.7 Fejlhåndtering

5.7.1 Registrering og kommunikation af data i DSRC-køretøjsenheden

5.7.2 Fejl i trådløs kommunikation

6 IDRIFTSÆTTELSE OG PERIODISKE INSPEKTIONSAFPRØVNINGER FOR FJERNKOMMUNIKATIONSFUNKTIONEN

6.1 Generelt

6.2 ECHO

6.3 Afprøvning til validering af sikkert dataindhold

1 INDLEDNING

I dette tillæg specificeres den udformning og de procedurer, der skal følges for at gennemføre fjernkommunikationsfunktionen (kommunikationen) i henhold til kravet i artikel 9 i forordning (EU) nr. 165/2014 (forordningen).

DSC_1 I forordning (EU) nr. 165/2014 bestemmes det, at takografen skal være udstyret med en fjernkommunikationsfunktion, der giver repræsentanter for de kompetente kontrolmyndigheder mulighed for at aflæse takografoplysninger fra forbipasserende køretøjer ved hjælp fjernaflæsningsudstyr (læser i udstyr til tidlig fjernafsløring [REDCR]), navnlig anmodningsudstyr, der tilsluttes trådløst med CEN 5,8 GHz Dedicated Short Range Communication-interfaces (DSRC-interfaces).

Det er vigtigt at forstå, at formålet med denne funktion udelukkende er, at den skal fungere som et foreløbigt filter til udvælgelse af køretøjer til nærmere inspektion, og at den ikke træder i stedet for den formelle inspektionsproces som fastlagt i bestemmelserne i forordning (EU) 165/2014. Se betragtning 9 i præamblen til denne forordning, hvori det hedder, at fjernkommunikation mellem takografen og kontrolmyndighederne med henblik på vejkontrol letter målrettede vejkontroller.

DSC_2 *Dataene* udveksles ved hjælp af *kommunikationen*, som skal være en trådløs forbindelse, der benytter 5,8 GHz DSRC trådløs kommunikation, der er i overensstemmelse med dette tillæg og er afprøvet i forhold til de relevante parametre i EN 300 674-1, {Electromagnetic compatibility and Radio spectrum Matters (ERM); Road Transport and Traffic Telematics (RTTT); Dedicated Short Range Communication (DSRC)

▼B

transmission equipment (500 kbit/s / 250 kbit/s) operating in the 5,8 GHz Industrial, Scientific and Medical (ISM) band; Part 1: General characteristics and test methods for Road Side Units (RSU) and On -Board Units (OBU)}.

DSC_3 *Kommunikationen* etableres kun med kommunikationsudstyret, når der kommer en anmodning fra den kompetente kontrolmyndigheds udstyr ved hjælp af godkendte radiokommunikationsmetoder (*læseren i udstyr til tidlig fjernafsløring (REDCR)*).

DSC_4 *Dataene* skal sikres for at garantere deres integritet.

DSC_5 Adgang til de kommunikerede *data* begrænses til kontrolmyndigheder, der er bemyndiget til at kontrollere overtrædelser af forordning (EF) nr. 561/2006 og af forordning (EU) nr. 165/2014 og til værksteder, for så vidt det er nødvendigt at kontrollere takografens korrekte funktion.

DSC_6 *Data*, som udveksles i forbindelse med *kommunikationen*, begrænses til de data, der er nødvendige af hensyn til de målrettede vejkontroller af køretøjer med en potentielt manipuleret eller misbrugt takograf.

DSC_7 Dataintegritet og -sikkerhed opnås ved at sikre *dataene* inde i køretøjsenheden (VU) og ved kun at overføre de sikrede indholds*data* og sikkerhedsrelaterede data (se 5.4.4) over det trådløse 5,8 GHz DSRC-fjernkommunikationsmedium, hvilket betyder, at kun godkendte personer fra de kompetente kontrolmyndigheder har mulighed for at forstå de data, der overføres via *kommunikationen*, og for at verificere deres ægthed. Se tillæg 11, Fælles sikkerhedsmekanismer.

DSC_8 *Dataene* indeholder et tidsstempel med tidspunktet for deres seneste ajourføring.

DSC_9 Indholdet af sikkerhedsdataene skal udelukkende være kendt af de kompetente kontrolmyndigheder og være inden for deres kontrol samt de parter, som de deler disse oplysninger med, og ligger uden for bestemmelserne for *kommunikationen*, der er genstand for dette tillæg, bortset fra, at *kommunikationen* giver mulighed for at overføre en pakke med sikkerhedsdata med hver pakke indholdsdata.

DSC_10 Den samme arkitektur og det samme udstyr skal være i stand til at hente andre datakoncepter (såsom weigh-on-board) ved hjælp af den heri angivne arkitektur.

DSC_11 Det skal præciseres, at i overensstemmelse med bestemmelserne of forordning (EU) nr. 165/2014 (artikel 7) må data vedrørende førerens identitet ikke transmitteres over *kommunikationen*.

2 ANVENDELSESOMRÅDE

Formålet med dette tillæg er at angive, hvordan repræsentanter for de kompetente kontrolmyndigheder anvender en bestemt 5,8 GHz DSRC trådløs kommunikation til at opnå fjernadgang til data (*dataene*) fra et bestemt køretøj, der angiver, at det pågældende køretøj har overtrådt

▼B

forordning (EU) 165/2014 og bør tages i betragtning med henblik på standsning for en nærmere undersøgelse.

I forordning (EU) nr. 165/2014 kræves det, at de indsamlede data kun må være data eller vedrøre data, der angiver en mulig overtrædelse begået af en af de registrerede, der er omfattet af forordning (EU) nr. 165/2014.

I dette scenario er der kun begrænset tid til rådighed til kommunikation, fordi *kommunikationen* er målrettet og har kort rækkevidde. Desuden kan de kompetente kontrolmyndigheder anvende de samme kommunikationsmidler til fjernovervågning af takografer (RTM) til andre formål (såsom de største tilladte dimensioner og den største tilladte vægt for tunge varekøretøjer, som defineret i direktiv 2015/719/EF), og sådanne operationer kan være separate eller sekventielle alt efter de kompetente kontrolmyndigheders valg.

I dette tillæg specificeres:

— Kommunikationsudstyr, -procedurer og -protokoller, der skal benyttes til *kommunikationen*

— Standarder og forordninger, som radioudstyret skal overholde

— Præsentationen af *dataene* for *kommunikations*udstyret

— Anmodnings- og dataoverførselsprocedurer og operationernes rækkefølge

— *Dataene*, der skal overføres

— Potentiel fortolkning af *dataene*, der overføres via *kommunikationen*

— Bestemmelserne for sikkerhedsdata vedrørende *kommunikationen*

— De kompetente kontrolmyndigheders adgang til *dataene*

— Hvordan *læseren i udstyr til tidlig fjernafsløring* kan anmode om forskellige koncepter for last- og flådedata

Det skal præciseres, at følgende ikke specificeres i dette tillæg:

— Indsamling af dataene og håndtering af disse i køretøjsenheden (som er en funktion af produktdesignet, medmindre det specificeres andetsteds i forordning (EU) nr. 165/2014)

— Formen af præsentationen af de indsamlede data for repræsentanten for de kompetente kontrolmyndigheder eller de kriterier, som de kompetente kontrolmyndigheder skal anvende til at beslutte, hvilke køretøjer de vil standse (dette skal være en funktion af produktdesignet, medmindre det angives andetsteds i forordning (EU) 165/2014, eller en politisk beslutning truffet af de kompetente kontrolmyndigheder). Det præciseres, at: *Kommunikationen* kun gør *dataene* tilgængelige for de kompetente kontrolmyndigheder, således at de kan træffe beslutninger på et velinformeret grundlag

▼B

— Datasikkerhedsbestemmelser (såsom kryptering) for så vidt angår indholdet af *dataene* (som angives i tillæg 11, Fælles sikkerhedsmekanismer).

— Nærmere oplysninger og andre datakoncepter end RTM, som kan opnås ved hjælp af den samme arkitektur og det samme udstyr

— Nærmere oplysninger om adfærden og administrationen mellem køretøjsenheder og DSRC-køretøjsenheden og ej heller adfærden inden for DSRC-køretøjsenheden (ud over at stille *dataene* til rådighed, når en REDCR anmoder om dette).

3 AKRONYMER, DEFINITIONER OG NOTATION

Følgende akronymer og definitioner, der er specifikke for dette tillæg, anvendes i tillægget:

Antennen	elektrisk enhed, der omdanner elektrisk strøm til radiobølger og omvendt, når den bruges sammen med en radiosender eller radiomodtager. Under drift leverer en radiosender elektrisk strøm, der svinger i radiofrekvens, til antennens terminaler, og antennen udstråler energi fra strømmen i form af elektromagnetiske bølger (radiobølger). Ved modtagelsen fanger antennen noget af effekten i en elektromagnetisk bølge og frembringer en svag spænding ved sine terminaler, som sendes videre til en modtager for at blive forstærket
Kommunikationen	udveksling af information/data mellem en *DSRC-REDCR* og en DSRC-køretøjsenhed i henhold til afsnit 5 i et master-slave-forhold for at modtage *dataene*.
Dataene	sikre data i et defineret format (se 5.4.4), som *DSRC-REDCR'en* anmoder om, og som leveres til *DSRC-REDCR'en* af *DSRC-køretøjsenheden* via en 5,8 GHz DSRC-forbindelse som defineret i 5 nedenfor
Forordning (EF) nr. 165/2014	Europa-Parlamentets og Rådets forordning (EU) nr.165/2014 af 4. februar 2014 om takografer inden for vejtransport, som ophævede Rådets forordning (EØF) nr. 3821/85 om kontrolapparatet inden

▼B

	for vejtransport og ændrede Europa-Parlamentets og Rådets forordning (EF) nr. 561/2006 om harmonisering af visse bestemmelser på det sociale område inden for vejtransport
AID	Applikationsnavn
BLE	Bluetooth Low Energy
BST	Beacon Service Table
CIWD	Isætning af kort under kørsel
CRC	Cyklisk redundanskontrol
DSC (n)	Identifikator for et krav om et specifikt DSRC-tillæg
DSRC	Dedicated Short Range Communication
DSRC-REDCR	DSRC-læser i udstyr til tidlig fjernafsløring.
DSRC-VU	DSRC-køretøjsenhed. Dette er "udstyret til tidlig fjernafsløring", som defineres i bilag 1C.
DWVC	Kørsel uden gyldigt kort
EID	Elementidentifikator
LLC	Logical Link Control
LPDU	LLC-dataenhedsprotokol
OWS	Vejesystem om bord
PDU	Protokoldataenhed
REDCR	Læser i udstyr til tidlig fjernafsløring, som defineret i bilag 1C.
RTM	Fjernovervågning af takograf
SM-REDCR	Sikkerhedsmodul i læser i udstyr til tidlig fjernafsløring
TARV	Telematics Applications for Regulated Vehicles (ISO 15638-standardserien)

▼B

VU	Køretøjsenhed
VUPM	Indholdshukommelse i køretøjsenhed
VUSM	Sikkerhedsmodul i køretøjsenhed
VST	Servicetabel for køretøj
WIM	Weigh in motion
WOB	Weigh on board

Den specifikation, som fastlægges i dette tillæg, henviser til og er baseret på følgende forordninger og standarder, enten helt eller delvist. I bestemmelserne i dette tillæg angives de relevante standarder eller de relevante bestemmelser i standarderne. Hvis der er modstrid mellem kravene, har bestemmelserne i dette tillæg forrang. Hvis der er tale om modstridende bestemmelser, når der ikke entydigt er fastlagt nogen specifikation i dette tillæg, skal drift i henhold til ERC 70-03 (efter afprøvning i forhold til de relevante parametre i EN 300 674-1) have forrang efterfulgt af EN 12795, EN 12253 EN 12834 og EN 13372, 6.2, 6.3, 6.4 og 7.1 i faldende betydningsrækkefølge.

I dette tillæg henvises der til følgende forordninger og standarder:

[1] I forordning (EU) nr. Rådets forordning (EU) nr.165/2014 af 4. februar 2014 om takografer inden for vejtransport, som ophævede Rådets forordning (EØF) nr. 3821/85 om kontrolapparatet inden for vejtransport og ændrede Europa-Parlamentets og Rådets forordning (EF) nr. 561/2006 om harmonisering af visse bestemmelser på det sociale område inden for vejtransport

[2] Europa-Parlamentets og Rådets forordning (EF) nr. 561/2006 af 15. marts 2006 om harmonisering af visse bestemmelser på det sociale område inden for vejtransport og om ændring af Rådets forordning (EØF) nr. 3821/85 og (EF) nr. 2135/98 og om ophævelse af Rådets forordning (EØF) nr. 3820/85 (EØS-relevant tekst).

[3] ERC 70-03 CEPT: ECC Recommendation 70-03: Relating to the Use of Short Range Devices (SRD)

[4] ISO 15638-9 Intelligent transport systems — Framework for cooperative telematics applications for regulated commercial freight vehicles (TARV).

[5] EN 300 674-1 Electromagnetic compatibility and Radio spectrum Matters (ERM); Road Transport and Traffic Telematics (RTTT); Dedicated Short Range Communication (DSRC) transmission equipment (500 kbit/s / 250 kbit/s) operating in the 5,8 GHz Industrial, Scientific and Medical (ISM) band; Part 1: General characteristics and test methods for Road Side Units (RSU) and On-Board Units (OBU).

[6] EN 12253 Road transport and traffic telematics — Dedicated short-range communication — Physical layer using microwave at 5.8 GHz.

▼B

[7] EN 12795 Road transport and traffic telematics — Dedicated short-range communication — Data link layer: medium access and logical link control.

[8] EN 12834 Road transport and traffic telematics — Dedicated short-range communication — Application layer.

[9] EN 13372 Road transport and traffic telematics — Dedicated short-range communication — Profiles for RTTT applications

[10] ISO 14906 Electronic fee collection — Application interface definition for dedicated short-range communication

4 DRIFTSSCENARIER

4.1 **Oversigt**

Forordning (EU) nr. 165/2014 indeholder specifikke og kontrollerede scenarier, inden for hvilke *kommunikationen* skal anvendes.

Følgende scenarier er understøttet:

"Communication Profile 1: Roadside inspection using a short range wireless communication Remote Early Detection Communication Reader instigating a physical roadside inspection (master-:-slave)

Reader Profile 1a: via a hand aimed or temporary roadside mounted and aimed Remote Early Detection Communication

Reader Profile 1b: via a vehicle mounted and directed Remote Early Detection Communication Reader".

4.1.1 *Forudsætninger for dataoverførsel via 5,8 GHz DSRC-interface*

BEMÆRK: For at forstå indholdet af forudsætningerne henvises læseren til figur 14.3 herunder.

4.1.1.1 Data lagret i køretøjsenheden

DSC_12 Køretøjsenheden er ansvarlig for at ajourføre data, der skal gemmes i køretøjsenheden, hvert 60. sekund og vedligeholde dem, uden at DSRC-kommunikationsfunktionen involveres. Metoderne, som skal anvendes til dette, er indbygget i køretøjsenheden som specificeret i forordning (EU) nr. 165/2014, bilag 1 C, afsnit 3.19 "*Fjernkommunikation til målrettede vejkontroller*" og specificeres ikke i dette tillæg.

4.1.1.2 Data leveret til DSRC-køretøjsenheden

DSC_13 Køretøjsenheden er ansvarlig for at ajourføre DSRC-takografdataene (*dataene*), når de data, der er lagret i køretøjsenheden, ajourføres med det i 4.1.1.1 (DSC_12) fastsatte interval uden at inddrage DSRC-kommunikationsfunktionen.

DSC_14 Dataene fra køretøjsenheden bruges som input og til at ajourføre *dataene*, og metoderne til dette angives i bilag 1C, afsnit 3.19 "*Fjernkommunikation til målrettede vejkontroller*". Alternativt, hvis der ikke findes en sådan angivelse, er det en del af produktdesignet og angives ikke i dette tillæg. For så vidt angår udformningen af forbindelsen mellem DSRC-køretøjsenheden og køretøjsenheden henvises til afsnit 5.6.

▼B

4.1.1.3 Dataenes indhold

DSC_15 *Dataenes* indhold og format betyder, at de, når de er dekrypterede, skal være strukturerede og tilgængelige i den form og det format, der specificeres i 5.4.4 i dette tillæg (Datastrukturer).

4.1.1.4 Præsentation af data

DSC_16 *Dataene* er blevet ajourført hyppigt i overensstemmelse med procedurerne i 4.1.1.1 og skal sikres forud for præsentationen for DSRC-køretøjsenheden og skal præsenteres som en sikret datakonceptværdi til midlertidig lagring i DSRC-køretøjsenheden som den aktuelle version af *dataene*. Disse data overføres fra *VUSM* til DSRC-funktionen *VUPM*. *VUSM* og *VUPM* er funktioner og ikke nødvendigvis fysiske enheder. Den fysiske enhed, der anvendes til at udføre disse funktioner, fastlægges i henhold til produktdesign, medmindre den specificeres andetsteds i forordning (EU) nr. 165/2014.

4.1.1.5 Sikkerhedsdata

DSC_17 Sikkerhedsdata (*securityData*), der omfatter de data, som *REDCR'en* behøver for at kunne dekryptere *dataene*, leveres som defineret i tillæg 11, Fælles sikkerhedsmekanismer, og præsenteres som en datakonceptværdi til midlertidig lagring i *DSRC-køretøjsenheden* som den aktuelle version af *securityData* i den form, der defineres i dette tillægs afsnit 5.4.4.

4.1.1.6 VUPM-data, der er tilgængelige for overførsel via DSRC-interfacet

DSC_18 Datakonceptet, som altid skal være tilgængeligt i DSRC-funktionen VUPM til umiddelbar overførsel efter anmodning fra REDCR'en, er som defineret i afsnit 5.4.4 med de fuldstændige specifikationer for ASN.1-modulet.

Generel oversigt over kommunikationsprofil 1

Denne profil omfatter brugssituationen, hvor repræsentanten for de kompetente kontrolmyndigheder benytter en fjernkommunikationsenhed med kort rækkevidde som læser i udstyr til tidlig fjernafsløring (5,8 GHz DSRC-interfaces, der fungerer inden for ERC 70-03, og som er afprøvet i forhold til de relevante parametre i EN 300 674-1 som beskrevet i afsnit 5) (*REDCR'en*) med henblik på fjernidentifikation af et køretøj, der muligvis overtræder forordning (EU) nr. 165/2014. Når køretøjet er identificeret, beslutter repræsentanten for de kompetente kontrolmyndigheder, som kontrollerer anmodningen, hvorvidt køretøjet skal standses.

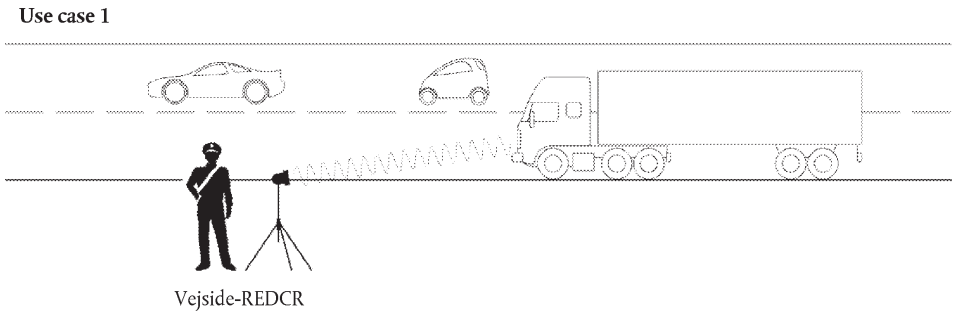
4.1.2 *Profil 1a: via en håndholdt eller midlertidig vejsidemonteret læser i udstyr til tidlig fjernafsløring*

I denne brugssituation befinder repræsentanten for de kompetente kontrolmyndigheder sig ved vejsiden og retter en *REDCR*, der er håndholdt, monteret på en trefod eller en tilsvarende type, fra vejsiden mod midten af det udvalgte køretøjs forrude. Anmodningen gennemføres ved hjælp af 5,8 GHz DSRC-interfaces, der opererer inden for ERC 70-03, og som er afprøvet i forhold til de relevante parametre i 300 674-1 som beskrevet i afsnit 5. Se figur 14.1 (Brugssituation 1).

▼B

Figur 14.1

Vejsideanmodning ved hjælp af 5,8 GHz DSRC

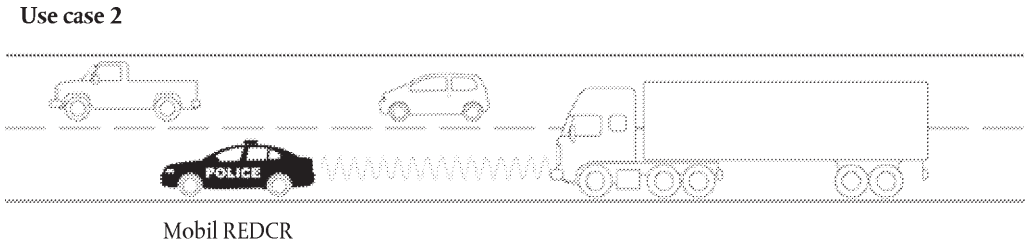


4.1.3 *Profil 1b: via en køretøjsmonteret og dirigeret læser i udstyr til tidlig fjernafsløring.*

I denne brugssituation befinder repræsentanten for de kompetente kontrolmyndigheder sig i et køretøj i bevægelse og retter enten en håndholdt, bærbar *REDCR* fra køretøjet imod midten af det udvalgte køretøjs forrude, eller også er *REDCR'en* monteret i eller på køretøjet, så den peger mod midten af forruden på det kontrollerede køretøj, når køretøjet med læseren i udstyr til tidlig fjernafsløring befinder sig i en bestemt position i forhold til det udvalgte køretøj (f.eks. direkte foran i en trafikstrøm). Anmodningen gennemføres ved hjælp af 5,8 GHz DSRC-interfaces, der opererer inden for ERC 70-03, og som er afprøvet i forhold til de relevante parametre i 300 674-1 som beskrevet i afsnit 5. Se figur 14.2. (Brugssituation 2).

Figur 14.2

Køretøjsbaseret anmodning ved hjælp af 5,8 GHz DSRC



4.2 **Sikkerhed/integritet**

For at man skal kunne fastslå ægtheden og integriteten af data, der er overført via fjernkommunikation, verificeres og dekrypteres de sikrede *data* i overensstemmelse med tillæg 11, Fælles sikkerhedsmekanismer.

5 DESIGN OG PROTOKOLLER TIL FJERNKOMMUNIKATION

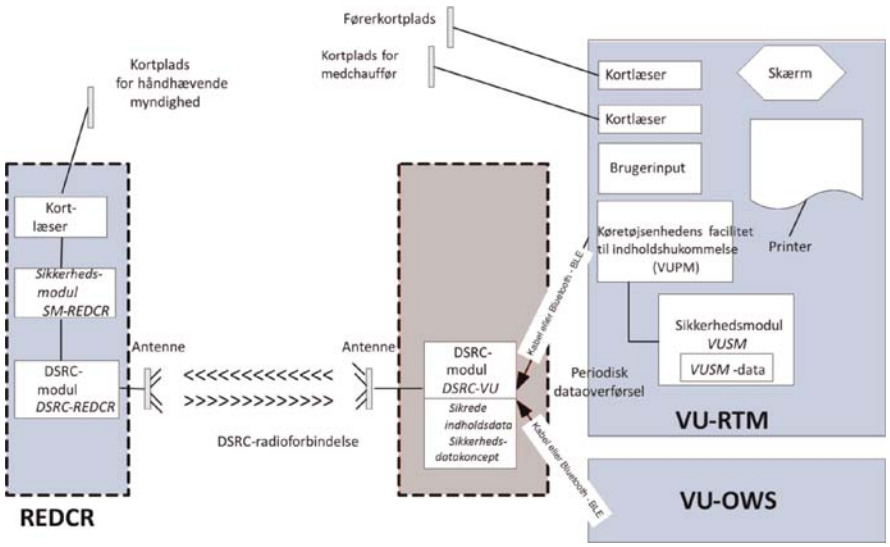
5.1 **Design**

Designet af fjernkommunikationsfunktionen i den intelligente takograf beskrives i figur 14.3.

▼B

Figur 14.3

Design af fjernkommunikationsfunktionen



DSC_19 Følgende funktioner er placeret i køretøjsenheden:

— Sikkerhedsmodulet (*VUSM*). Denne funktion i køretøjsenheden er ansvarlig for at sikre *de data*, som skal overføres fra DSRC-køretøjsenheden til repræsentanten for de kompetente kontrolmyndigheder via fjernkommunikation.

— De sikrede data gemmes i VUSM-hukommelsen. Med de intervaller, der fastlægges i 4.1.1.1 (DSC_12), krypterer køretøjsenheden dataene og leverer input til RTM-datakonceptet (som omfatter datakonceptværdier for indholdsdata og sikkerhedsdata som fastlagt nedenfor i dette tillæg), som ligger i DSRC-køretøjsenhedens hukommelse. Sikkerhedsmodulets funktion fastlægges i tillæg 11, Fælles sikkerhedsmekanismer, og ligger uden for dette tillægs dækningsområde, bortset fra at det skal levere ajourføringer til køretøjsenhedens kommunikationsenhed, hver gang VUSM-dataene ændrer sig.

— Kommunikationen mellem køretøjsenheden og DSRC-køretøjsenheden kan foregå via et kabel eller Bluetooth Low Energy-kommunikation (BLE-kommunikation), og DSRC-køretøjsenhedens fysiske placering kan være bygget sammen med antennen ved køretøjets forrude, være indbygget i køretøjsenheden eller være placeret et sted imellem disse.

— DSRC-køretøjsenheden skal til enhver tid have en pålidelig strømforsyning. Strømforsyningsmetoden fastlægges i designfasen.

— DSRC-køretøjsenhedens hukommelse skal være ikke-flygtig for at kunne gemme dataene i DSRC-køretøjsenheden, selv når køretøjets tænding er slået fra.

— Hvis kommunikationen mellem køretøjsenheden og DSRC-køretøjsenheden foregår via BLE, og strømforsyningen er et ikkegenopladeligt batteri, skal DSRC-køretøjsenhedens strømforsyning udskiftes ved hver periodisk inspektion,

▼B

og fabrikanten af udstyret til DSRC-køretøjsenheden er ansvarlig for at sikre, at strømforsyningen er tilstrækkelig til at holde fra den ene periodiske inspektion til den næste, idet en REDCR skal have normal adgang til dataene igennem hele perioden uden fejl eller afbrydelser.

— Køretøjsenhedens RTM-funktion "indholdshukommelse" (*VUPM*). Denne funktion i køretøjsenheden er ansvarlig for at levere og ajourføre *dataene*. Indholdet af *dataene*. ("TachographPayload") defineres i 5.4.4/5.4.5 nedenfor og ajourføres med det interval, der fastlægges i 4.1.1.1 (DSC_12).

— DSRC-køretøjsenhed. Dette er den funktion, der er indbygget i eller tilsluttet antennen og er i kommunikation med køretøjsenheden via en kablet eller trådløs (BLE) forbindelse, og som indeholder de aktuelle data (*VUPM-data*) og forvalter svaret på en anmodning via 5,8 GHz DSRC-mediet. Afbrydelse af DSRC-enheden eller interferens med DSRC-enhedens funktion under køretøjets normale drift betragtes som en overtrædelse af forordning (EU) 165/2014.

— Sikkerhedsmodulet (REDCR) (*SM-REDCR*) er den funktion, der anvendes til at dekryptere og kontrollere integriteten af dataene, der kommer fra køretøjsenheden. Metoderne til at opnå dette fastlægges i tillæg 11, Fælles sikkerhedsmekanismer, og defineres ikke i dette tillæg.

— DSRC-enhedens (REDCR) (*DSRC-REDCR*) funktion omfatter en 5,8 GHz sender/modtager og tilhørende firmware og software, der administrerer *kommunikationen DSRC-køretøjsenheden* i overensstemmelse med dette tillæg.

— *DSRC-REDCR* forespørger DSRC-køretøjsenheden i det udvalgte køretøj og modtager *dataene* (det udvalgte køretøjs aktuelle *VUPM-data*) via DSRC-forbindelsen og behandler og gemmer de modtagne data i sin *SM-REDCR*.

— *DSRC-køretøjsenhedens* antenne skal være anbragt i en position, hvor den optimerer DSRC-kommuniktionen mellem køretøjet og antennen i vejsiden (normalt i eller tæt på midten af køretøjets frontrude). For lette køretøjer er montering svarende til den øverste del af frontruden hensigtsmæssig.

  — Der må ikke forefindes metalgenstande (f.eks. navneskilte, mærkater, refleksdæmpende folie (toning), solskærme, vinduesviskere, som ikke er i brug) foran eller tæt på antennen, som kan forstyrre kommunikationen.

  — Antennen skal monteres, så dens boresigte er omtrent 900 i forhold til vejoverfladen (dvs. vertikal retning).

▼B

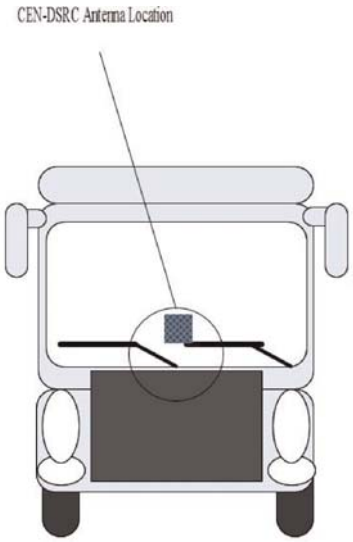
DSC_20 Antennen og kommunikationen opererer inden for ERC 70-03 og er afprøvet i forhold til de relevante parametre i 300 674-1 som beskrevet i afsnit 5. Antennen og kommunikationen kan anvende teknikker til at afhjælpe risikoen for interferens af det trådløse signal som beskrevet i ECC-rapport 228, f.eks. ved brug af filtre i CEN DSRC 5,8 GHz-kommunikationen.

DSC_21 DSRC-antennen tilsluttes DSRC-køretøjsenheden enten direkte inde i modulet, der er monteret på eller i nærheden af forruden, eller via et dedikeret kabel, der er konstrueret på en sådan måde, at en ulovlig afbrydelse er vanskelig. Afbrydelse af eller interferens med antennens funktion betragtes som en overtrædelse af forordning (EU) nr. 165/2014. Bevidst maskering af eller andre former for forstyrrelse af antennens drift betragtes som en overtrædelse af forordning (EU) nr. 165/2014.

DSC_22 Antennens formfaktor defineres ikke og er genstand for en kommerciel beslutning, når blot den monterede DSRC-køretøjsenhed opfylder overensstemmelseskravene som defineret i afsnit 5 nedenfor. Antennen skal monteres som fastsat i DSC_19 og som vist i figur 14.4 (oval linje), og den understøtter effektivt de anvendelsessituationer, der beskrives i 4.1.2 og 4.1.3.

Figur 14.4

Eksempel på placering af 5,8 GHz DSRC-antennen i forruden af regulerede køretøjer



REDCR'ens og dens antennes formfaktor kan variere i henhold til omstændighederne for læseren (monteret på trefod, håndholdt, køretøjsmonteret osv.) og den metode, som anvendes af repræsentanten for de kompetente kontrolmyndigheder.

Et display og/eller en meddelelsesfunktion benyttes til at præsentere resultaterne af fjernkommunikationsfunktionen for repræsentanten for de kompetente kontrolmyndigheder. Et display kan have form af en skærm, en udskrift, et lydsignal eller en kombination af sådanne meddelelser. Formen af et sådant display og/eller meddelelser fastlægges i henhold til kravene fra repræsentanterne for de kompetente kontrolmyndigheder og udstyrsdesignet og angives ikke i dette tillæg.

▼B

DSC_23 REDCR'ens design og formfaktor fastlægges af det kommercielle design, driftskravene i ERC 70-03 samt design- og præstationsspecifikationerne i dette tillæg (afsnit 5.3.2), således at markedet gives maksimal fleksibilitet til at designe og levere udstyr, der kan opfylde de specifikke behov for anmodninger hos en given kompetent kontrolmyndighed.

DSC_24 *DSRC-køretøjsenheden* og dens placering inde i eller uden for køretøjsenheden afhænger af det kommercielle design, driftskravene i ERC 70-03 samt de design- og præstationsspecifikationer, der defineres i dette tillæg (afsnit 5.3.2) og i denne bestemmelse (5.1).

DSC_25 *DSRC-køretøjsenheden* skal imidlertid inden for rimelige grænser være i stand til at modtage datakonceptværdier fra andet intelligent køretøjsudstyr ved hjælp af en open industry-standardforbindelse og protokoller (f.eks. fra weigh on board-udstyr), så længe disse datakoncepter identificeres med entydige og kendte applikationsidentifikatorer/filnavne, og instruktionen om at anvende sådanne protokoller skal stilles til rådighed for Kommissionen og uden beregning for fabrikanter af relevant udstyr.

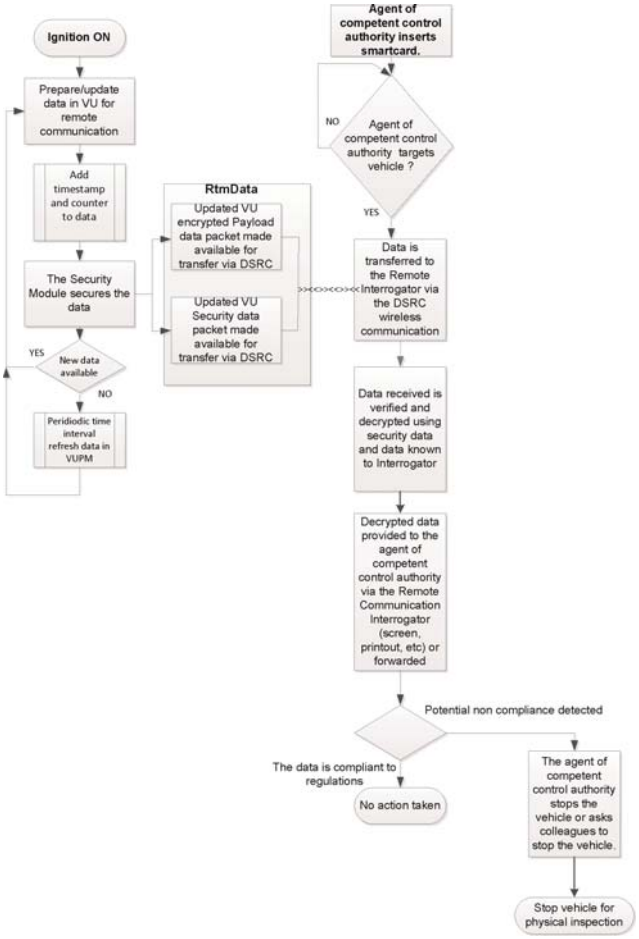
5.2 **Arbejdsgang**

5.2.1 *Drift*

Arbejdsgangen for driften fremgår af figur 14.5.

Figur 14.5

Arbejdsgang for fjernkommunikationsfunktionen



▼B

Trinnene beskrives i det følgende:

a. Så snart køretøjet er i drift (tænding TIL), leverer takografen data til køretøjsenhedsfunktionen. Køretøjsenhedsfunktionen forbereder *dataene* til fjernkommunikationsfunktionen (krypteret) og ajourfører *VUPM*, der ligger i DSRC-køretøjsenhedens hukommelse (som defineret i 4.1.1.1-4.1.1.2). De indsamlede *Data* formateres som angivet i 5.4.4-5.4.5 nedenfor.

b. Hver gang *dataene* ajourføres, skal tidsstemplet, som defineres i sikkerhedsdatakonceptet, ajourføres.

c. *VUSM*-funktionen sikrer dataene i overensstemmelse med procedurerne i tillæg 11.

d. Hver gang *dataene* ajourføres (se 4.1.1.1-4.1.1.2), overføres *dataene* til DSRC-køretøjsenheden, hvor de erstatter eventuelle tidligere data, således at de ajourførte aktuelle data (*dataene*) altid vil være tilgængelige, hvis der indkommer en anmodning fra en *REDCR*. Når køretøjsenheden leverer *dataene* til DSRC-køretøjsenheden, skal de kunne identificeres med filnavnet *RTMData* eller med identifikatorerne ApplicationID og Attribute.

e. Hvis en repræsentant for de kompetente kontrolmyndigheder ønsker at kontrollere et køretøj og indsamle *dataene* fra det udvalgte køretøj, skal repræsentanten for de kompetente kontrolmyndigheder først isætte sit smartcard i *REDCR'en* for at give mulighed for *kommunikationen* og give *SM-REDCR'en* mulighed for at verificere dets ægthed og kryptere dataene.

f. Repræsentanten for den kompetente kontrolmyndighed udvælger herefter et køretøj og anmoder om dataene via fjernkommunikation. *REDCR'en* indleder en 5,8 GHz DSRC-interfacesession med *DSRC-køretøjsenheden* for det udvalgte køretøj og anmoder om *dataene*. *Dataene* overføres til *REDCR'en* via det trådløse kommunikationssystem som en DSRC-attribut ved hjælp af applikationstjenesten GET som defineret i 5.4. Attributten indeholder de krypterede indholdsdataværdier og DSRC-sikkerhedsdataene.

g. Dataene analyseres af *REDCR*-udstyret og leveres til repræsentanten for den kompetente kontrolmyndighed.

h. Repræsentanten for den kompetente kontrolmyndighed anvender dataene som en del af beslutningen om, hvorvidt køretøjet skal standses med henblik på en detaljeret inspektion, eller om en anden repræsentant for den kompetente kontrolmyndighed skal anmodes om at standse køretøjet.

5.2.2 *Fortolkning af data modtaget via DSRC-kommunikationen*

DSC_26 Data, der modtages over 5.8 GHz-interfacet har alene den betydning og vægt, der defineres i 5.4.4 og 5.4.5 nedenfor og skal forstås inden for de deri definerede formål. I overensstemmelse med bestemmelserne of forordning (EU) nr. 165/2014 må *dataene* udelukkende bruges til at stille relevante oplysninger til rådighed for en kompetent kontrolmyndighed med henblik på at hjælpe disse med at afgøre, hvilke

▼B

køretøjer der skal standses med henblik på fysisk inspektion, og skal efterfølgende destrueres i overensstemmelse med artikel 9 i forordning (EU) nr. 165/2014.

5.3 **Fysiske DSRC-interfaceparametre til fjernkommunikation**

5.3.1 *Lokaliseringsbegrænsninger*

DSC_27 Fjernanmodninger til køretøjer ved hjælp af et 5,8 GHz DSRC-interface bør ikke anvendes nærmere end 200 meter fra en operationel 5,8 GHz DSRC-bro.

5.3.2 *Downlink- og uplink-parametre*

DSC_28 Udstyret til fjernaflæsning af takografer skal være i overensstemmelse med og fungere inden for ERC70-03 samt de parametre, der defineres i tabel 14.1 og 14.2 nedenfor.

DSC_29 Med henblik på at sikre kompatibilitet med driftsparametrene for andre standardiserede 5,8 GHz DSRC-systemer gælder det endvidere, at det udstyr, der benyttes til fjernaflæsning af takografer, skal være i overensstemmelse med parametrene i EN 12253 og EN 13372.

Det gælder navnlig:

Tabel 14.1

Downlinkparametre

Punkt nr.	Parameter	Værdi(er)	Bemærkning
D1	Downlink-bærefrekvenser	Der findes fire alternativer, som en REDCR kan benytte: 5,7975 GHz 5,8025 GHz 5,8075 GHz 5,8125 GHz	Inden for ERC 70-03. Bærefrekvenser vælges af montøren af systemet ved vejsiden og behøver ikke være kendt af DSRC-køretøjsenheden (Overholder EN 12253, EN 13372)
D1a (*)	Bærefrekvensernes tolerance:	inden for ± 5 ppm	(Overholder EN 12253)
D2 (*)	RSU (REDCR) Spektralmaske for transmitter	Inden for ERC 70-03. REDCR'en skal være i overensstemmelse med Class B,C som defineret i EN 12253. Ingen andre specifikke krav i dette bilag	Parameter, der benyttes til at kontrollere interferens mellem interrogatorer i nærheden (som defineret i EN 12253 og EN 13372).
D3	OBU(DSRC-VU) Minimum frekvensinterval	5,795-5,815 GHz	(Overholder EN 12253)
D4 (*)	Maksimum E.I.R.P.	Inden for ERC 70-03 (uden tilladelse) og inden for de nationale bestemmelser Maksimum +33 dBm	(Overholder EN 12253)

▼B

Punkt nr.	Parameter	Værdi(er)	Bemærkning
D4a	Vinklet E.I.R.P.-maske	I henhold til den indberettede og offentliggjorte specifikation fra designeren af interrogatoren	(Overholder EN 12253)
D5	Polarisering	Venstre, cirkulær	(I overensstemmelse med EN 12253)
D5a	Krydspolarisering	XPD: I boresigte: (REDCR) RSU t ≥15 dB (DSRC-VU) OBU r≥ 10 dB I -3 dB-området: (REDCR) RSU t ≥ 10 dB (DSRC-VU) OBU r ≥ 6 dB	(Overholder EN 12253)
D6 (*)	Modulation	Amplitudemodulation i to niveauer.	(Overholder EN 12253)
D6a (*)	Modulationsindeks	0,5 … 0,9	(Overholder EN 12253)
D6b	Øjenmønster	≥ 90 % (tid) / ≥ 85 % (amplitude)	
D7 (*)	Datakodning	FM0 ‘1’-bit'en har kun transitioner ved begyndelsen og slutningen af bitintervallet. ‘0’-bit'en har en yderligere transition i midten af bitintervallet sammenlignet med ‘1’-bit'en.	(Overholder EN 12253)
D8 (*)	Bithastighed	500 kBit/s	(Overholder EN 12253)
D8a	Bit-klokkens tolerance	bedre end ± 100 ppm	(Overholder EN 12253)
D9 (*)	Bitfejlrate (B.E.R.) for kommunikation	$\leq 10^{-6}$, når den indfaldende effekt ved OBU (DSRC-VU) ligger i det interval, der er givet ved [D11a til D11b].	(Overholder EN 12253)
D10	Start-trigger til OBU (DSRC-køretøjsenhed)	OBU (DSRC-køretøjsenheden) skal starte op ved modtagelse af en hvilken som helst ramme med 11 oktetter eller derover (inklusive præambel)	Der kræves intet særligt startmønster. DSRC-køretøjsenheden kan starte op ved modtagelse af en ramme med mindre end 11 oktetter (Overholder EN 12253)
D10a	Maksimal opstartstid	≤ 5 ms	(Overholder EN 12253)
D11	Kommunikationszone	Region, inden for hvilken der opnås en B.E.R. i henhold til D9a	(Overholder EN 12253)
D11a (*)	Effektgrænse for kommunikation (øvre).	-24dBm	(Overholder EN 12253)

▼B

Punkt nr.	Parameter	Værdi(er)	Bemærkning
D11b (*)	Effektgrænse for kommunikation (nedre).	Indfaldende effekt: – 43 dBm (boresigte) – 41 dBm (inden for – 45 ° — + 45 ° svarende til det plan, der er parallelt med vejoverfladen, når DSRC-køretøjsenheden senere installeres i køretøjet (azimut))	(Overholder EN 12253) Udvidede krav til horisontale vinkler op til ± 45 ° som følge af de anvendelsessituationer, der defineres i dette bilag.
D12 (*)	Afbrydelsesniveau for (DSRC-køretøjsenhed)	– 60 dBm	(Overholder EN 12253)
D13	Præambel	Præambel er obligatorisk.	(Overholder EN 12253)
D13a	Længde og mønster for præambel	16 bit ± 1 bit FM0-kodede '1' bits	(Overholder EN 12253)
D13b	Bølgeform for præambel	En skiftende sekvens af lavt og højt niveau med en impulsvarighed på 2 μs. Tolerancen angives i D8a	(Overholder EN 12253)
D13c	Efterstillede bit	RSU'en (REDCR) må højst transmittere 8 bit efter afslutningsmarkøren. Der er ikke behov for en OBU (DSRC-køretøjsenhed) for at tage hensyn til disse supplerende bit.	(Overholder EN 12253)

(*) — Downlink-parametre er underlagt overensstemmelsesafprøvning i overensstemmelse med den relevante parameterafprøvning fra EN 300 674-1

Tabel 14.2

Uplink-parametre

Punkt nr.	Parameter	Værdi(er)	Bemærkning
U1 (*)	Frekvenser for sub-bærebølge	En OBU (DSRC-køretøjsenhed) skal understøtte 1,5 MHz og 2,0 MHz En RSU (REDCR) skal understøtte 1,5 MHz eller 2,0 MHz eller begge. U1-0: 1,5 MHz U1-1: 2,0 MHz	Frekvensvalg for sub-bærebølge (1,5 MHz eller 2,0 MHz) afhængigt af den valgte EN 13372-profil.
U1a (*)	Tolerance for sub-bærebølgefrekvenser	inden for ± 0,1 %	(Overholder EN 12253)
U1b	Brug af sidebånd	Samme data på begge sider	(Overholder EN 12253)
U2 (*)	OBU (DSRC-køretøjsenhed) Spektralmaske for transmitter	Overholder EN12253 1) Effekt, udadgående bånd: se ETSI EN 300 674-1	(Overholder EN 12253)

▼B

Punkt nr.	Parameter	Værdi(er)	Bemærkning
		2) Effekt, indadgående bånd: [U4a] dBm i 500 kHz 3) Emission på en hvilken som helst anden uplink-kanal: U2(3)-1 = -35 dBm i 500 kHz	
U4a (*)	Maksimalt enkelt sidebånd E.I.R.P. (boresigte)	To muligheder: U4a-0: -14 dBm U4a-1: -21 dBm	I henhold til den indberettede og offentliggjorte specifikation fra designeren af udstyret
U4b (*)	Maksimalt enkelt sidebånd E.I.R.P. (35 °)	To muligheder: — Ikke relevant — – 17dBm	I henhold til den indberettede og offentliggjorte specifikation fra designeren af udstyret
U5	Polarisering	Venstre, cirkulær	(I overensstemmelse med EN 12253)
U5a	Krydspolarisering	XPD: I boresigte: (REDCR) RSU r ≥ 15 dB (DSRC-VU) OBU t ≥ 10 dB Ved -3 dB: (REDCR) RSU r ≥ 10 dB (DSRC-VU) OBU t ≥ 6 dB	(Overholder EN 12253)
U6	Modulation af sub-bærebølge	2-PSK Kodede data synkroniseret med sub-bærebølge: Transitionerne for kodede data er sammenfaldende med transitionerne for sub-bærebølgen.	(Overholder EN 12253)
U6b	Driftsperiode	Driftsperiode: 50 % ± α, α ≤ 5 %	(Overholder EN 12253)
U6c	Modulation på bærebølge	Multiplikation af moduleret sub-bærebølge med bærebølge.	(Overholder EN 12253)
U7 (*)	Datakodning	NRZI (Ingen transition ved begyndelsen af '1'-bit'en, transition ved begyndelsen af '0'-bit'en, ingen transition inden for bit'en)	(Overholder EN 12253)
U8 (*)	Bithastighed	250 kbit/s	(Overholder EN 12253)
U8a	Tolerance for bit-takt	Inden for ± 1 000 ppm	(Overholder EN 12253)
U9	Bitfejlrate (B.E.R.) ved kommunikation	$\leq 10^{-6}$	(Overholder EN 12253)

▼B

Punkt nr.	Parameter	Værdi(er)	Bemærkning
U11	Kommunikationszone	Den fysiske region, inden for hvilken DSRC-køretøjsenheden befinder sig, således at dens transmissioner modtages af REDCR'en med en B.E.R. på mindre end det, der angives i U9a.	(Overholder EN 12253)
U12a (*)	Konverteringsforstærkning (nedre grænse)	1 dB for hvert sidebånd Vinkelinterval: Cirkulært symmetrisk mellem boresigte og ± 35 ° og	
		inden for – 45 ° — + 45 ° svarende til det plan, der er parallelt med vejoverfladen, når DSRC-køretøjsenheden senere installeres i køretøjet (azimut)	Større end det angivne interval for horisontale vinkler op til ± 45° som følge af de anvendelsessituationer, der defineres i dette bilag.
U12b (*)	Konverteringsforstærkning (øvre grænse)	10 dB for hvert sidebånd	Mindre end det angivne værdiinterval for hvert sidebånd inden for en cirkelformet kegle omkring boresigtet med en ± 45 ° åbningsvinkel.
U13	Præambel	Præambel er obligatorisk.	(Overholder EN 12253)
U13a	Præambel Længde og mønster	32 til 36 µs udelukkende moduleret med sub-bærebølge, herefter 8 bit NRZI-kodede '0'-bit.	(Overholder EN 12253)
U13b	Efterstillede bit	DSRC-køretøjsenheden må højst transmittere 8 bit efter afslutningsmarkøren. En RSU (REDCR) skal ikke tage hensyn til disse supplerende bit.	(Overholder EN 12253)

(*) Uplink-parametre er underlagt overensstemmelsesafprøvning i overensstemmelse med den relevante parameterafprøvning fra EN 300 674-1

5.3.3 *Antennedesign*

5.3.3.1 REDCR-antenne

DSC_30 Udformningen af *REDCR*-antennen bestemmes af det kommercielle design, og den skal operere inden for de grænser, der er fastsat i 5.3.2, som har til formål at optimere *DSRC-REDCR*'ens læseevne med det specifikke formål og på de læsevilkår, som *REDCR'en* er udformet til at operere under.

5.3.3.2 Køretøjsenhedens antenne

DSC_31 Udformningen af antennen på *DSRC-køretøjsenheden* bestemmes af det kommercielle design, og den skal operere inden for de grænser, der er fastsat i 5.3.2, som har til formål at optimere *DSRC-REDCR'ens* læseevne med det specifikke formål og på de læsevilkår, som *REDCR'en* er udformet til at operere under.

▼B

DSC_32 Køretøjsenhedens antenne fastgøres til eller tæt ved køretøjets forrude som specificeret i ovenstående 5.1.

DSC_33 I testmiljøet i et værksted (se afsnit 6.3) skal antennen på en DSRC-køretøjsenhed, der er monteret i henhold til 5.1 ovenfor, oprette forbindelse til standardtestkommunikationsudstyr og gennemføre en RTM-transaktion som defineret i dette tillæg i en afstand på 2 og 10 m mere end 99 % af tiden med et gennemsnit på over 1 000 læste anmodninger.

5.4 **DSRC-protokolkrav til RTM**

5.4.1 *Oversigt*

DSC_34 Transaktionsprotokollen til download af *dataene* via 5,8 GHz DSRC-interfaceforbindelsen skal være i overensstemmelse med følgende beskrivelse. I dette afsnit beskrives en transaktionsstrøm under ideelle betingelser uden genfremsendelser eller kommunikationsafbrydelser.

Bemærk: Formålet med initialiseringsfasen (trin 1) er at etablere kommunikationen mellem *REDCR'en* og DSRC-køretøjsenheder, der er kommet ind i 5,8 GHz DSRC- (master-slave) transaktionsområdet, men endnu ikke har etableret kommunikation med *REDCR'en*, og at anmelde applikationsprocesser.

— **Trin 1** Initialisering. *REDCR'en* sender en ramme med en ”Beacon Service Table” (BST), der indeholder applikationsidentifikatorerne (AIDs) i den serviceliste, den understøtter. I RTM-applikationen bliver dette ganske enkelt tjenesten med AID-værdien = 2 (Freight&Fleet). *DSRC-køretøjsenheden* evaluerer den modtagne BST og reagerer (se nedenfor) med listen over de understøttede applikationer i Freight&Fleet-området eller reagerer ikke, hvis ingen applikationer understøttes. Hvis *REDCR'en* ikke tilbyder AID = 2, afslutter svarer DSRC-køretøjsenheden ikke REDCR'en.

— **Trin 2** *DSRC-køretøjsenheden* sender en ramme med en anmodning om tildeling af et privat vindue.

— **Trin 3** *REDCR'en* sender en ramme med tildeling af et privat vindue.

— **Trin 4** *DSRC-køretøjsenheden* bruger det tildelte private vindue til at sende en ramme med dets servicetabel for køretøjet (VST). Denne VST indeholder en liste med alle de forskellige applikationsforekomster, som denne *DSRC-køretøjsenhed* understøtter i AID = 2-rammen. De forskellige forekomster identificeres ved hjælp af entydigt genererede EID'er, hver tilhørende en parameterværdi for applikationsindholdsmarkør, der angiver applikationen og den understøttede standard.

— **Trin 5** Derefter analyserer *REDCR'en* den tilbudte VST og afslutter enten forbindelsen (RELEASE), da den ikke er interesseret i noget af det, VST'en kan tilbyde (dvs. at den modtager en VST fra en *DSRC-køretøjsenhed*, der ikke understøtter RTM-transaktionen), eller den starter en app-forekomst.

▼B

— **Trin 6** For at igangsætte dette sender REDCR'en en ramme med en kommando om at hente RTM-data, som identificerer forekomsten af RTM-applikationen ved at specificere den identifikator, der svarer til forekomsten af RTM-applikationen (som specificeret af DSRC-køretøjsenheden i VST'en), og tildeler et privat vindue.

— **Trin 7** *DSRC-køretøjsenheden* bruger det nyligt tildelte private vindue til at sende en ramme med den behandlede identifikator svarende til RTM-applikationsforekomsten som tilvejebragt i VST'en, efterfulgt af egenskaben *RtmData* (dataindholdselement + sikkerhedselement).

— **Trin 8** Hvis der er anmodet om flere services, ændres værdien 'n' til det næste servicereferencenummer, og processen gentages.

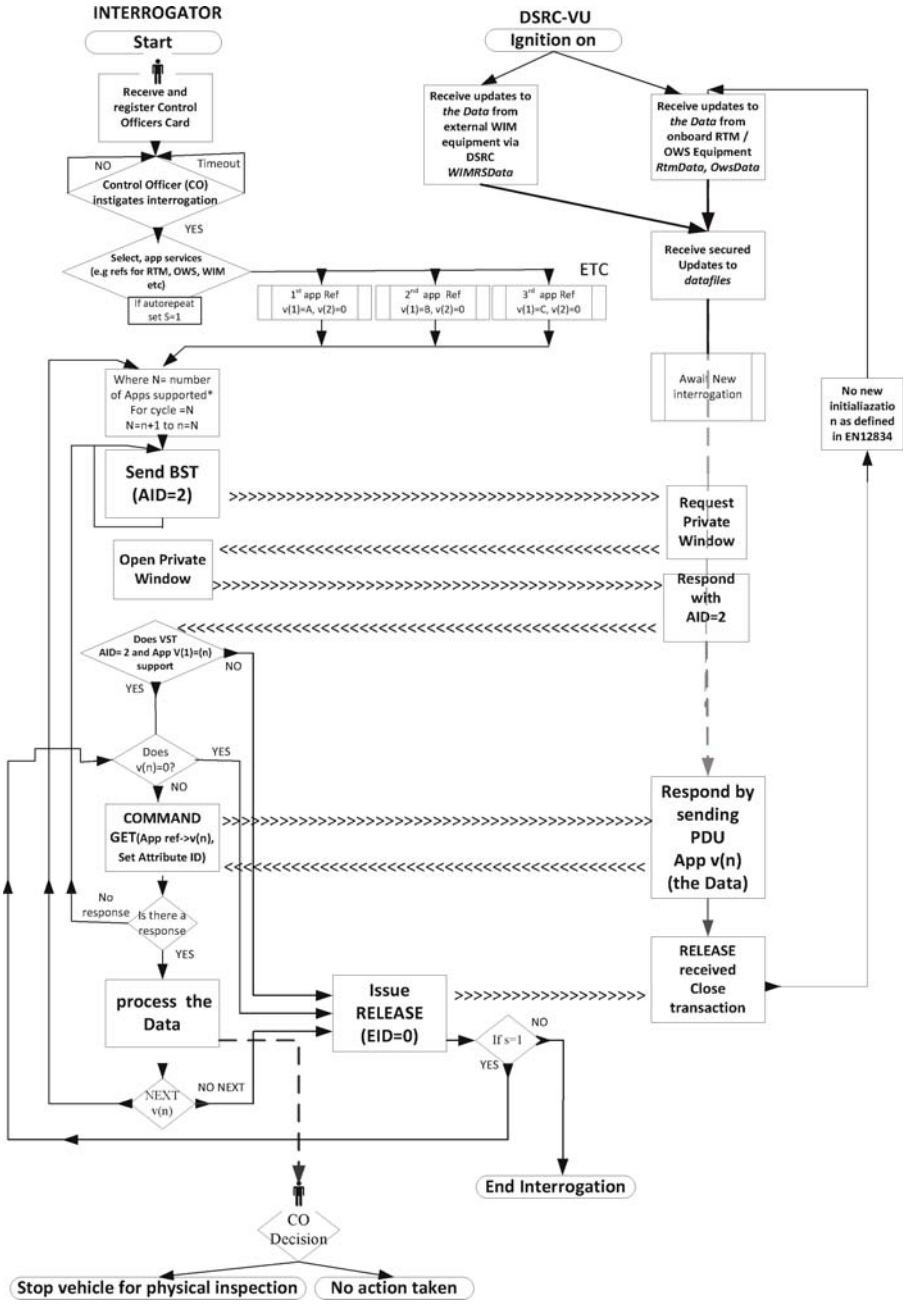
— **Trin 9** *REDCR'en* bekræfter modtagelsen af data ved at sende en ramme med en RELEASE-kommando til *DSRC-køretøjsenheden* for at afslutte sessionen ELLER går tilbage til trin 6, hvis den ikke har valideret en vellykket modtagelse af LDPU'en.

Se figur 14.6 for en grafisk beskrivelse af transaktionsprotokollen.

▼B

Figur 14.6

RTM 5,8 GHz DSRC-procesflow



5.4.2 *Kommandoer*

DSC_35 Følgende kommandoer bruges kun i en RTM-transaktionsfase

— **INITIALISATION.request**: En kommando, der afgives af REDCR'en i form af en transmission med definition af applikationer, som REDCR'en understøtter.

— **INITIALISATION.response**: Et svar fra DSRC-køretøjsenheden, der bekræfter forbindelsen og indeholder en liste over understøttede applikationsforekomster med kendetegn og information om, hvordan de skal håndteres (EID).

▼B

— **GET.request**: En kommando afgivet af *REDCR'en* til *DSRC-køretøjsenheden*, der angiver den applikationsforekomst, der skal håndteres ved hjælp af en defineret EID, som denne modtages i VST'en, som instruerer *DSRC-køretøjsenheden* i at sende de(n) valgte attribut(ter) sammen med *dataene*. Formålet med GET-kommandoen er, at *REDCR'en* skal hente *dataene* fra *DSRC-køretøjsenheden*.

— **GET.response**: Et svar fra DSRC-køretøjsenheden, der indeholder *dataene* fra forespørgslen.

— **ACTION.request ECHO**: En kommando, der instruerer *DSRC-køretøjsenheden* i at sende data tilbage fra *DSRC-køretøjsenheden* til *REDCR'en*. Formålet med ECHO-kommandoen er at give værksteder eller prøveanlæg til typegodkendelse mulighed for at efterprøve, at DSRC-forbindelsen fungerer uden at kræve adgang til sikkerhedsoplysninger.

— **ACTION**.response (ECHO): Svar fra DSRC-køretøjsenheden på ECHO-kommandoen.

— **EVENT_REPORT.request** RELEASE: En kommando til *DSRC-køretøjsenheden* om, at transaktionen er afsluttet. Formålet med RELEASE-kommandoen er at afslutte sessionen med *DSRC-køretøjsenheden*. Ved modtagelsen af RELEASE reagerer *DSRC-køretøjsenheden* ikke på yderligere anmodninger under den nuværende forbindelse. Bemærk, at en DSRC-køretøjsenhed i henhold til EN 12834 ikke forbindes to gange til samme interrogator, medmindre den har været ude af kommunikationsområdet i 255 sekunder, eller hvis interrogatorens Beacon-ID er blevet ændret.

5.4.3 *Kommandosekvens ved anmodning*

DSC_36 Set ud fra kommando- og responssekvensen beskrives transaktionen som følger:

Rækkefølge	Sender		Modtager	Beskrivelse	Handling
1	REDCR	>	DSRC-VU	Initialisering af kommunikationen forbindelse — Anmodning	REDCR udsender BST
2	*DSRC-køretøjsenhed*	>	*REDCR*	*Initialisering af kommunikationen forbindelse — Svar*	*Hvis BST understøtter AID=2, anmoder DSRC-køretøjs-enheden om et privat vindue*
3	REDCR	>	DSRC-køretøjsenhed	Tildeler et privat vindue	Sender ramme med tildeling af privat vindue
4	*DSRC-køretøjsenhed*	>	*REDCR*	*Sender VST*	*Sender ramme indeholdende VST*
5	REDCR	>	DSRC-køretøjsenhed	Sender GET.request om data i Attribut for specifik EID	
6	*DSRC-VU*	>	*REDCR*	*Sender GET.response med ønsket Attribut til specifik EID*	*Sender attribut (RTMData, OWSData….) med data til specifik EID*

▼B

Rækkefølge	Sender		Modtager	Beskrivelse	Handling
7	REDCR	>	DSRC-køretøjsenhed	Sender GET.request om data anden Attribut (hvis relevant)	
8	*DSRC-køretøjsenhed*	>	*REDCR*	*Sender GET.response med ønsket Attribut*	*Sender Attribut med data til specifik EID*
9	REDCR	>	DSRC-køretøjsenhed	Bekræfter vellykket modtagelse af data	Sender RELEASE-kommando, der afslutter transaktionen
10	*DSRC-køretøjsenhed*			*Afslutter transaktionen*	

Et eksempel på transaktionssekvensen og indholdet af de udvekslede rammer defineres i punkt 5.4.7 og 5.4.8.

5.4.4 *Datastrukturer*

DSC_37 Når *dataene* sendes via 5,8 GHz DSRC-interfacet, skal deres semantiske struktur være i overensstemmelse med beskrivelsen i dette tillæg. Den måde, disse data er struktureret på, specificeres i denne artikel.

DSC_38 Indholdsdataene (RTM-data) består af en sammenkædning af

1. EncryptedtachographPayload-data, som er krypteringen af TachographPayload som defineret i ASN.1 i afsnit 5.4.5. Krypteringsmetoden er beskrevet i tillæg 11

2. DSRCSecurityData, specificeres i tillæg 11.

DSC_39 RTM-data behandles som RTM-attribut = 1 og overføres i RTM-container = 10.

DSC_40 RTM-indholdsmarkøren identificerer den understøttede standarddel i TARV-serien af standarder (RTM svarer til del 9)

ASN.1-moduldefinition for DSRC-dataene inden for RTM-applikationen defineres som følger:

▼B

```
TarvRtm {iso(1) standard(0) 15638 part9(9) version1(1)}
DEFINITIONER AUTOMATISKE ETIKETTER
::= BEGIN
IMPORTS
-- Importerer dataattributter og -elementer fra EFC, der anvendes til RTM
LPN
FROM EfcDsrcApplication {iso(1) standard(0) 14906 application(0) version5(5)}

-- Importerer funktionsparametre fra EFC-applikationsinterfacedefinitionen
SetMMIRq
FROM EfcDsrcApplication {iso(1) standard(0) 14906 application(0) version5(5)}

-- Importerer L7 DSRCData-moduldata fra EFC-applikationsinterfacedefinitionen
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)};


-- Definitioner af RTM-funktionerne:
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})

-- Definitioner af RTM-attributterne:
RtmData ::= SEQUENCE {
      encryptedTachographPayload OCTET STRING (SIZE(67)) (BEGRÆNSET AF { -- beregnet ved kryptering af
TachographPayload i henhold til tillæg 11 --}),
      DSRCSecurityData OCTET STRING
      }
TachographPayload ::= SEQUENCE {
             tp15638VehicleRegistrationPlate LPN -- Køretøjets nummerplade i henhold til EN 15509.
             tp15638SpeedingEvent            BOOLEAN, -- 1= Uregelmæssigheder i hastighed (se bilag 1C)
             tp15638DrivingWithoutValidCard  BOOLEAN,     -- 1= Brug af ulovligt kort (se bilag 1C)
             tp15638DriverCard               BOOLEAN,-- 0= Angiver et gyldigt førerkort   (se bilag 1C)
             tp15638CardInsertion            BOOLEAN, -- 1= Isættelse af kort under kørsel  (se bilag 1C)
             tp15638MotionDataError          BOOLEAN, -- 1= Fejl ved køredata (se bilag 1C)
             tp15638VehicleMotionConflict    BOOLEAN, -- 1= Konflikt ved køredata (se bilag 1C)
             tp156382ndDriverCard            BOOLEAN, -- 1= Et andet førerkort er isat (se bilag 1C)
             tp15638CurrentActivityDriving   BOOLEAN, -- 1= anden aktivitet valgt;
                                                      -- 0= kørsel valgt
             tp15638LastSessionClosed        BOOLEAN, -- 1= ukorrekt, 0= korrekt, lukket
             tp15638PowerSupplyInterruption  INTEGER (0..127), -- Dataafbrydelser i de seneste 10 dage
             tp15638SensorFault              INTEGER (0..255),-- eventFaultType i henhold til dataordliste
-- Alle efterfølgende tidsrelaterede typer som defineret i bilag 1C.
             tp15638TimeAdjustment           INTEGER(0..4294967295), -- Tidspunkt for seneste
tidsindstilling
             tp15638LatestBreachAttempt      INTEGER(0..4294967295), -- Tidspunkt for seneste forsøg på
sikkerhedsbrud
             tp15638LastCalibrationData      INTEGER(0..4294967295), -- Tidspunkt for seneste
kalibreringsdata
             tp15638PrevCalibrationData      INTEGER(0..4294967295), -- Tidspunkt for foregående
kalibreringsdata
tp15638DateTachoConnected INTEGER(0..4294967295), -- Dato for tilslutning af takograf

             tp15638CurrentSpeed             INTEGER (0..255), -- Seneste aktuelle registrerede hastighed
             tp15638Timestamp                INTEGER(0..4294967295) -- Tidsstempel for aktuel registrering[2]
             }
Rtm-ContextMark ::= SEQUENCE {
  standardIdentifier    StandardIdentifier, -- identifikator for TARV-delen og dennes version

  RtmCommProfile          INTEGER {
                                C1 (1),
                                C2 (2)
                                } (0..255) DEFAULT 1
  }
RtmTransferAck ::= INTEGER {
                  Ok (1),
                  NoK (2)
                  } SIZE (1..255)
```

▼B

```
StandardIdentifier ::= OBJEKTIDENTIFIKATOR
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,
-- værdierne fra 16 til 255 forbeholdt ISO/CEN-brug
  }}

END
```

5.4.5 *Elementer af RtmData, udførte handlinger og definitioner*

DSC_41 Dataværdierne, som skal beregnes af køretøjsenheden og bruges til at ajourføre de sikrede data i DSRC-køretøjsenheden, skal beregnes i henhold til reglerne i tabel 14.3:

Tabel 14.3

Elementer af RtmData, udførte handlinger og definitioner

(1) RTM-dataelement	(2) Handling udført af køretøjsenhed		(3) ASN.1 Definition af data
RTM1 **Køretøjsregistrering Nummerplade**	Køretøjsenheden angiver værdien for *tp15638VehicleRegistrationPlate* dataelementet RTM1 fra den registrerede værdi for datatypen *VehicleRegistrationIdentification* som defineret i tillæg 1 *VehicleRegistrationIdentification*	Køretøjets nummerplade udtrykt som en streng af tegn	`tp15638VehicleRegstrationPlate LPN, --Køretøjets registrerings-nummer importeret fra ISO 14906 med den i EN 15509 anførte begrænsning, som er en SEKVENS bestående af landekoden efterfulgt af en bogstav-indikator efterfulgt af selve registreringsnummeret, som altid er 14 oktetter (udfyldt med nuller), så længden af EN 15509 LPN-typen er altid 17 oktetter, hvor af de 14 er det "egentlige" registrerings-nummer.`
RTM2 **Hastighedshændelse**	VU genererer en boolsk værdi for dataelement RTM2 tp15638SpeedingEvent. VU beregner værdien af tp15638SpeedingEvent på grundlag af antallet af Over Speeding Events, der er registreret i køretøjsenheden i løbet af de seneste 10 dages forekomst, som defineret i bilag 1C.	1 (TRUE) = angiver uregelmæssigheder med speed inden for de seneste 10 dages forekomst	`tp15638speedingEvent BOOLEAN,`

▼B

(1) RTM-dataelement	(2) Handling udført af køretøjsenhed		(3) ASN.1 Definition af data
	Hvis der er mindst en tp15638SpeedingEvent inden for de seneste 10 dages forekomst, sættes værdien tp15638SpeedingEvent til TRUE. ELSE, hvis der ikke har været nogen hændelser inden for de seneste 10 dages forekomst, sættes tp15638SpeedingEvent til FALSE.		
RTM3 **Kørsel uden gyldigt kort**	Køretøjsenheden genererer en boolsk værdi for dataelement RTM3 tp15638DrivingWithoutValidCard. Køretøjsenheden tildeler værdien TRUE til variablen tp15638DrivingudenValidCard, hvis køretøjsenhedsdataene har registreret mindst en hændelse inden for de seneste 10 dages forekomst, af typen Kørsel uden et korrekt kort som defineret i bilag 1C. ELSE, hvis der ikke har været nogen hændelser inden for de seneste 10 dages forekomst, sættes variablen tp15638DrivingWithoutValidCard til FALSE.	1 (TRUE) = Angiver brug af brug af kort	`tp15638DrivingWithoutValidCard` `BOOLEAN,`
RTM4 **Gyldigt førerkort**	Køretøjsenheden genererer en boolsk værdi af dataelement RTM4 tp15638DriverCard på grundlag af de lagrede data i køretøjsenheden og som defineret i tillæg 1. Hvis der ikke er et gyldigt førerkort til stede, sætter køretøjsenheden variablen til TRUE ELSE, hvis der er et gyldigt førerkort til stede, sætter køretøjsenheden variablen til FALSE	0 (FALSE) = Angiver et gyldigt førerkort	`tp15638DriverCard` `BOOLEAN,`
RTM5 **Isætning af kort under kørsel**	Køretøjsenheden genererer en boolsk værdi for dataelementet RTM5. Køretøjsenheden tildeler variablen tp15638CardInsertion værdien TRUE, hvis køretøjsenhedsdataene inden for de seneste 10 dages forekomst, har registreret mindst en hændelse af typen »Isætning af kort under kørsel« som defineret i bilag IC. ELSE, hvis der ikke er sket en sådan hændelse inden for de seneste 10 dages forekomst, sættes variablen tp15638CardInsertion til FALSE.	1 (TRUE) = Angiver isætning af kort under kørsel inden for de seneste 10 dages forekomst	`tp15638CardInsertion` `BOOLEAN,`
RTM6 **Fejl i bevægelsesdata**	Køretøjsenheden genererer en boolsk værdi for dataelementet RTM6. Køretøjsenheden tildeler variablen tp15638MotionDataError værdien TRUE, hvis køretøjsenhedsdataene inden for de seneste 10 dages forekomst, har registreret mindst en hændelse af typen »Fejl i bevægelsesdata« som defineret i bilag 1C. ELSE, hvis der ikke er sket en sådan hændelse inden for de seneste 10 dages forekomst, sættes variablen tp15638MotionDataError til FALSE.	1 (TRUE) = Angiver fejl datafejl inden for de seneste 10 dages forekomst	`tp15638motionDataError` `BOOLEAN,`

▼B

(1) RTM-dataelement	(2) Handling udført af køretøjsenhed		(3) ASN.1 Definition af data
RTM7 **Køretøjsbevægelseskonflikt**	Køretøjsenheden genererer en boolsk værdi for dataelementet RTM7. Køretøjsenheden tildeler variablen tp15638vehicleMotionConflict værdien TRUE, hvis køretøjsenhedsdataene inden for de seneste 10 dage har registreret mindst en hændelse af typen Køretøjsbevægelseskonflikt (værdi '0A'H). ELSE, hvis der ikke har været nogen hændelser inden for de seneste 10 dages forekomst, sættes variablen tp15638vehicleMotionConflict til FALSE.	1 (TRUE) = Angiver bevægelses-konflikt inden for de seneste 10 dages forekomst	`tp15638vehicleMotionConflict` `BOOLEAN,`
RTM8 **2. førerkort**	Køretøjsenheden genererer en boolsk værdi for dataelementet RTM8 på grundlag af bilag 1C (»Føreraktivitetsdata« CREW og CO-DRIVER). Hvis et 2. gyldigt førerkort er til stede, sætter køretøjsenheden variablen til TRUE ELSE, hvis der ikke er et 2. gyldigt førerkort til stede, sætter køretøjsenheden variablen til FALSE	1 (TRUE) = Angiver, at et andet førerkort er isat	`tp156382ndDriverCard BOOLEAN,`
RTM9 **Aktuel aktivitet**	Køretøjsenheden genererer en boolsk værdi for dataelementet RTM9. Hvis den aktuelle aktivitet er registreret i køretøjsenheden som en hvilken som helst anden aktivitet end »KØRSEL« som defineret i bilag 1C, sætter køretøjsenheden variablen til TRUE ELSE, hvis den aktuelle aktivitet registreres i køretøjsenheden som »KØRSEL«, sætter køretøjsenheden variablen til FALSE	1 (TRUE) = anden aktivitet valgt; 0 (FALSE) = kørsel valgt	`tp15638currentActivityDriving` `BOOLEAN`
RTM10 **Seneste session afsluttet**	Køretøjsenheden genererer en boolsk værdi for dataelementet RTM10. Hvis den seneste kortsession ikke blev lukket korrekt som defineret i bilag 1C, sætter køretøjsenheden variablen til TRUE ELSE, hvis den seneste kortsession blev lukket korrekt, sætter køretøjsenheden variablen til FALSE	1 (TRUE) = ikke lukket korrekt 0 (FALSE) = lukket korrekt	`tp15638lastSessionClosed` `BOOLEAN`
RTM11 **Afbrydning af strømforsyning**	Køretøjsenheden generer en heltalsværdi for dataelementet RTM11. Køretøjsenheden tildeler variablen tp15638PowerSupplyInterruption en værdi svarende til længste afbrydelse af strømforsyningen i overensstemmelse med artikel 9 i forordning (EU) 165/2014 af typen »Afbrydelse af strømforsyning« som defineret i bilag 1C.	— Antal afbrydelser af strømforsyningen inden for de seneste 10 dages forekomst	`tp15638powerSupplyInterruption` `INTEGER (0..127),`

▼B

(1) RTM-dataelement	(2) Handling udført af køretøjsenhed		(3) ASN.1 Definition af data
	ELSE, hvis der inden for de seneste 10 dages forekomst, ikke har været hændelser med afbrydelse af strømforsyningen, sættes værdien af heltallet til 0.		
RTM12 **Følerfejl**	Køretøjsenheden genererer en heltalsværdi for dataelementet RTM12. Køretøjsenheden tildeler variablen sensorFault en værdi på: — 1 hvis der er registreret en hændelse af typen '35H' Følerfejl inden for de seneste 10 dage, — 2 hvis der er registreret en hændelse af typen GNSS-modtagerfejl (enten intern eller ekstern med enum-værdien '51'H eller '52'H) inden for de seneste 10 dage. — 3 hvis der er registreret en hændelse af typen '53'H Ekstern GNSS-kommunikationsfejl inden for de seneste 10 dages forekomst. — 4 Hvis der er registreret både følerfejl og GNSS-modtagerfejl inden for de seneste 10 dages forekomst — 5 Hvis der er registreret både følerfejl og eksterne GNSS-kommunikationsfejl inden for de seneste 10 dages forekomst — 6 Hvis der er registreret både GNSS-modtagerfejl og eksterne GNSS-kommunikationsfejl inden for de seneste 10 dages forekomst — 7 Hvis alle tre følerfejl er blevet registreret inden for de seneste 10 dages forekomst ELSE tildeler den værdien 0, hvis der ikke er registreret nogen hændelser inden for de seneste 10 dages forekomst	— følerfejl en oktet i henhold til dataordlisten	`tp15638SensorFault INTEGER (0..255),`
RTM13 **Tidsjustering**	Køretøjsenheden genererer en heltalsværdi (timeReal fra tillæg 1) til dataelementet RTM13 på grundlag af tilstedeværelsen af data for indstilling af klokkeslæt som defineret i bilag 1C. Køretøjsenheden tildeler den tidsværdi, hvor den seneste hændelse med tidsindstillingsdata er forekommet. ELSE, hvis der ikke findes nogen »Indstilling af klokkeslæt«-hændelse som defineret i bilag 1C i dataene for køretøjsenheden, sættes værdien til 0	Tidspunkt for seneste indstilling	`tp15638TimeAdjustment INTEGER(0..4294967295),`
RTM14 **Forsøg på sikkerhedsbrud**	Køretøjsenheden genererer en heltalsværdi (timeReal fra tillæg 1) til dataelementet RTM14 på grundlag af en hændelse med forsøg på sikkerhedsbrud som defineret i bilag 1C. Køretøjsenheden sætter værdien til tidspunktet for den seneste hændelse med forsøg på sikkerhedsbrud, som køretøjsenheden har registreret.	Tidspunkt for seneste forsøg på sikkerhedsbrud — Standardværdi =0x00FF	`tp15638LatestBreachAttempt HELTAl(0..4294967295),`

▼B

(1) RTM-dataelement	(2) Handling udført af køretøjsenhed		(3) ASN.1 Definition af data
	ELSE, hvis der ikke findes nogen »forsøg på sikkerhedsbrud«-hændelse som defineret i bilag 1C i dataene for køretøjsenheden, sættes værdien til 0x00FF.		
RTM15 **Seneste kalibrering**	Køretøjsenheden genererer en heltalsværdi (timeReal fra tillæg 1) til dataelementet RTM15 på grundlag af tilstedeværelsen af seneste kalibreringsdata som defineret i bilag 1C. Køretøjsenheden sætter værdien til tidspunktet for de seneste to kalibreringer (RTM15 og RTM16), som angives i VuCalibrationData, jf. definitionen i tillæg 1. Køretøjsenheden sætter værdien for RTM15 til timeReal for den seneste kalibreringsregistrering.	Tidspunkt for seneste kalibreringsdata	`tp15638LastCalibrationData` `HELTAl(0..4294967295),`
RTM16 **Foregående kalibrering**	Køretøjsenheden genererer en heltalsværdi (timeReal fra tillæg 1) for dataelementet RTM16 for kalibreringsregistreringen forud for den seneste kalibrering ELSE, hvis der ikke findes nogen tidligere kalibrering, sætter køretøjsenheden værdien for RTM16 til 0.	Tidspunkt for foregående kalibrerings-data	`tp15638PrevCalibrationData INTEGER(0..4294967295),`
RTM17 **Dato for tilslutning af takograf**	For dataelementet RTM17 genererer køretøjsenheden en heltalsværdi (timeReal fra tillæg 1). Køretøjsenheden sætter værdien for tidspunktet for den første installering af køretøjsenheden. Køretøjsenheden henter disse data fra VuCalibrationData (tillæg 1) fra vuCalibrationRecords med CalibrationPurpose lig med: ‘03’H	Dato for tilslutning af takograf	`tp15638DateTachoConnected` `HELTAl(0..4294967295),`
RTM18 **Aktuel hastighed**	Køretøjsenheden generer en heltalsværdi for dataelementet RTM18. Køretøjsenheden sætter værdien for RTM16 til den senest registrerede aktuelle hastighed på tidspunktet for den seneste ajourføring af RtmData.	Senest registrerede aktuelle hastighed	`tp15638CurrentSpeed INTEGER (0..255),`
RTM19 **Tidsstempel**	For dataelementet RTM19 genererer køretøjsenheden en heltalsværdi (timeReal fra tillæg 1). Køretøjsenheden sætter værdien for RTM19 til tidspunktet for den seneste ajourføring af RtmData.	Tidsstempel for aktuel TachographPayload-post	`tp15638Timestamp` `INTEGER(0..4294967295),`

5.4.6 *Dataoverførselsmekanisme*

DSC_42 REDCR anmoder om tidligere defineret dataindhold efter initialiseringsfasen, der herefter overføres af *DSRC-køretøjsenheden* i det tildelte vindue. REDCR benytter kommandoen GET til at hente data.

▼B

DSC_43 Ved alle DSRC-udvekslinger skal dataene kodes med PER (Packed Encoding Rules).

5.4.7 *Detaljeret DSRC-transaktionsbeskrivelse*

DSC_44 Initialiseringen udføres i henhold til DSC_44-DSC_48 og tabel 14.4-14.9. Under initialiseringsfasen begynder REDCR at sende en ramme, der indeholder en BST (Beacon Service Table) i henhold til EN 12834 og EN 13372, 6.2, 6.3, 6.4 og 7.1 med indstillinger som angivet i nedenstående tabel 14.4.

Tabel 14.4

Initialisering — BST-rammeindstillinger

Felt	Indstillinger
Link-identifikator	Sendeadresse
BeaconId	I henhold til EN 12834
Klokkeslæt	I henhold til EN 12834
Profil	Ingen udvidelse, 0 eller 1 benyttes
MandApplications	Ingen udvidelse, EID ikke til stede, Parameter ikke til stede, AID = 2 Freight&Fleet
NonMandApplications	Ikke til stede
ProfileList	Ingen udvidelse, antal profiler på listen = 0
Fragmenterings-header	Ingen fragmentering
Indstillinger for lag 2	Kommando-PDU, UI-kommando

Følgende tabel 14.5 indeholder et praktisk eksempel på indstillingerne i tabel 14.4 med angivelse af bitkodninger.

Tabel 14.5

Initialisering — eksempel på BST-rammeindhold

Oktet nr.	Attribut/Felt	Bit in oktet	Beskrivelse
1	MARKØR	0111 1110	Startmarkør
2	Sende-ID	1111 1111	Sendeadresse
3	MAC-kontrolfelt	1010 0000	Kommando-PDU
4	LLC-kontrolfelt	0000 0011	UI-kommando

▼B

Oktet nr.	Attribut/Felt	Bit in oktet	Beskrivelse
5	Fragmenterings-header	1xxx x001	Ingen fragmentering
6	BST	1000	Initialiseringsanmodning
	SEQUENCE {		
	OPTION indicator BeaconID SEQUENCE { ManufacturerId INTEGER (0..65535)	0	NonMand-applikationer ikke til stede
		xxx	Fabrikantidentifikator
7		xxxx xxxx	
8		xxxx x	
	IndividualID INTEGER (0..134217727)	xxx	27 bit ID tilgængelig for fabrikant
9		xxxx xxxx	
10		xxxx xxxx	
11	}	xxxx xxxx	
12	Klokkeslæt INTEGER (0..4294967295)	xxxx xxxx	32 bit UNIX realtid
13		xxxx xxxx	
14		xxxx xxxx	
15		xxxx xxxx	
16	Profil INTEGER (0..127,…)	0000 0000	Ingen udvidelse. Eksempelprofil 0
17	MandApplications SEQUENCE (SIZE(0..127,…)) OF {	0000 0001	Ingen undtagelse, Antal mandApplications = 1
18	SEQUENCE {		
	OPTION indicator	0	EID ikke til stede
	OPTION indicator	0	Parameter ikke til stede
	AID DSRCApplicationEntityID } }	00 0010	Ingen udvidelse. AID = 2 Freight&Fleet

▼B

Oktet nr.	Attribut/Felt	Bit in oktet	Beskrivelse
19	ProfileList SEQUENCE (0..127,…) OF Profile }	0000 0000	Ingen udvidelse, antal profiler på listen = 0
20	FCS	xxxx xxxx	Sekvens for rammekontrol
21		xxxx xxxx	
22	Markør	0111 1110	Slutmarkør

DSC_45 Når en *DSRC-køretøjsenhed* modtager en BST, kræver den tildeling af et privat vindue som specificeret i EN 12795 og EN 13372, 7.1.1, uden specifikke RTM-indstillinger. Tabel 14.6 indeholder et eksempel på bitkodning.

Tabel 14.6

Initialisering — Indhold af ramme til anmodning om tildeling af privat vindue

Oktet nr.	Attribut/Felt	Bit i oktet	Beskrivelse
1	MARKØR	0111 1110	Startmarkør
2	Privat LID	xxxx xxxx	Linkadresse for specifik DSRC-køretøjsenhed
3		xxxx xxxx	
4		xxxx xxxx	
5		xxxx xxxx	
6	MAC-kontrolfelt	0110 0000	Anmodning om privat vindue
7	FCS	xxxx xxxx	Sekvens for rammekontrol
8		xxxx xxxx	
9	Markør	0111 1110	Slutmarkør

DSC_46 Herefter svarer REDCR'en ved at tildele et privat vindue som specificeret i EN 12795 og EN 13372, 7.1.1, uden specifikke RTM-indstillinger.

Tabel 14.7 indeholder et eksempel på bitkodning.

Tabel 14.7

Initialisering — Indhold af ramme til anmodning om tideling af privat vindue

Oktet nr.	Attribut/Felt	Bit i oktet	Beskrivelse
1	MARKØR	0111 1110	Startmarkør
2	Privat LID	xxxx xxxx	Linkadresse på den specifikke DSRC-køretøjsenhed
3		xxxx xxxx	

▼B

Oktet nr.	Attribut/Felt	Bit i oktet	Beskrivelse
4		xxxx xxxx	
5		xxxx xxxx	
6	MAC-kontrolfelt	0010 s000	Tildeling af privat vindue
7	FCS	xxxx xxxx	Sekvens for rammekontrol
8		xxxx xxxx	
9	Markør	0111 1110	Slutmarkør

DSC_47 Når *DSRC-køretøjsenheden* modtager tildelingen af det private vindue, sender den sin VST (Vehicle Service Table) som defineret i EN 12834 og EN 13372, 6.2, 6,3, 6.4 og 7.1 med indstillinger som specificeret i tabel 14.8 ved hjælp af det tildelte transmissionsvindue.

Tabel 14.8

Initialisering — VST-rammeindstillinger

Felt	Indstillinger
Privat LID	I henhold til EN 12834
VST-parametre	Fill = 0, herefter for hver understøttet applikation: EID til stede, parameter til stede, AID = 2, EID som genereret af OBU
Parameter	Ingen udvidelse, Indeholder RTM-kontekstmarkør
ObeConfiguration	Det valgfrie felt ObeStatus kan være til stede, men skal ikke benyttes af REDCR'en
Fragmenterings-header	Ingen fragmentering
Indstillinger for lag 2	Kommando-PDU, UI-kommando

DSC_48 *DSRC-køretøjsenheden* skal understøtte applikationen ”Freight&Fleet”, som identificeres med applikationsidentifikatoren ”2”. Andre applikationsidentifikatorer kan også understøttes, men behøver ikke være til stede i denne VST, eftersom BST kun kræver AID = 2. Feltet ”Applikationer” indeholder en liste over de understøttede applikationsforekomster i *DSRC-køretøjsenheden*. For hver understøttet applikationsforekomst indsættes der en henvisning til den relevante standard bestående af et RTM Context-mærke, der består af en OBJECT IDENTIFIER, som repræsenterer den tilhørende standard, dens del (9 for RTM) og eventuelt dens version, plus en EID, som genereres af DSRC-køretøjsenheden, og som er tilknyttet den pågældende applikationshændelse.

Tabel 14.9 indeholder et praktisk eksempel på de indstillinger, der angives i tabel 14.8, med angivelse af bitkodninger.

▼B

Tabel 14.9

Initialisering — Eksempel på VST-rammeindhold

Oktet nr.	Attribut/Felt	Bit i oktet	Beskrivelse
1	MARKØR	0111 1110	Startmarkør
2	Privat LID	xxxx xxxx	Linkadresse på den specifikke DSRC-køretøjsenhed
3		xxxx xxxx	
4		xxxx xxxx	
5		xxxx xxxx	
6	MAC-kontrolfelt	1100 0000	Kommando-PDU
7	LLC-kontrolfelt	0000 0011	UI-kommando
8	Fragmenterings-header	1xxx x001	Ingen fragmentering
9	VST SEQUENCE {	1001	Initialiseringssvar
	Fyld BIT STRING (SIZE(4))	0000	Ikke i brug og sat til 0
10	Profil INTEGER (0..127,…) Applikationer SEQUENCE OF {	0000 0000	Ingen udvidelse. Eksempelprofil 0
11		0000 0001	Ingen udvidelse, 1 applikation
12	SEQUENCE {		
	OPTION-indikator	1	EID til stede
	OPTION-indikator	1	Parameter til stede
	AID DSRCApplicationEntityID	00 0010	Ingen udvidelse. AID= 2 Freight&Fleet
13	EID Dsrc-EID	xxxx xxxx	Defineret inde i OBU'en og identificerer applikationsforekomsten.
14	Parametercontainer {	0000 0010	Ingen udvidelse, Containervalg = 02, Oktetstreng
15		0000 1000	Ingen udvidelse, længde af RTM-kontekstmarkering = 8

▼B

Oktet nr.	Attribut/Felt	Bit i oktet	Beskrivelse
16	Rtm-ContextMark::= SEQUENCE	0000 0110	Objektidentifikator for den understøttede standard, del og version. Eksempel: ISO (1) standard (0) TARV (15638) del9 (9) version1 (1). Første oktet er 06H, som er objektidentifikatoren, anden oktet er 06H, som er dens længde. De efterfølgende 6 oktetter koder objektidentifikatoren i eksemplet Bemærk, at kun ét element af sekvensen er til stede (det valgfri element RtmCommProfile udelades)
17	{	0000 0110	
18	StandardIdentifier standardIdentifier	0010 1000	
19		1000 0000	
20		1111 1010	
21		0001 0110	
22		0000 1001	
23		0000 0001	
24	ObeConfiguration-sekvens { OPTION-indikator	0	ObeStatus ikke til stede
	EquipmentClass INTEGER (0..32767)	xxx xxxx	
25		xxxx xxxx	
26	ManufacturerId INTEGER (0..65535)	xxxx xxxx	Fabrikantidentifikator for DSRC-køretøjsenheden som beskrevet i ISO 14816-registret
27		xxxx xxxx	
28	FCS	xxxx xxxx	Sekvens for rammekontrol
29		xxxx xxxx	
30	Markør	0111 1110	Slutmarkør

DCS_49 Herefter læser REDCR'en dataene ved at udsende en GET-kommando, der er i overensstemmelse med GET-kommandoen, som defineres i EN 13372, 6.2, 6.3, 6.4 og EN 12834 med indstillinger som specificeret i tabel 14.10.

Tabel 14.10

Præsentation — Rammeindstillinger for GET-anmodning

Felt	Indstillinger
Identifikator for aktiverende applikationsenhed (IID)	Ikke til stede
Linkidentifikator (LID)	Linkadresse på den specifikke DSRC-køretøjsenhed
Sammenkædning	Nej
Elementidentifikator (EID)	Som specificeret i VST. Ingen udvidelse

▼B

Felt	Indstillinger
Adgangsoplysninger	Nej
AttributeIdList	Ingen udvidelse, 1 attribut, AttributeID = 1 (RtmData)
Fragmentering	Nej
Lag2-indstillinger	Kommando-PDU, Udsendt ACn-kommando

Tabel 14.11 viser et eksempel på læsning af RTM-dataene.

Tabel 14.11

Præsentation — Eksempel på ramme for Get-anmodning

Oktet nr.	Attribut/Felt	Bit i oktet	Beskrivelse
1	MARKØR	0111 1110	Startmarkør
2	Privat LID	xxxx xxxx	Linkadresse på den specifikke DSRC-køretøjsenhed
3		xxxx xxxx	
4		xxxx xxxx	
5		xxxx xxxx	
6	MAC-kontrolfelt	1010 s000	Kommando-PDU
7	LLC-kontrolfelt	n111 0111	Udsendt ACn-kommando, n bit
8	Fragmenterings-header	1xxx x001	Ingen fragmentering
9	Get.request SEQUENCE {	0110	Hent anmodning
	OPTION-indikator	0	Adgangsoplysninger ikke til stede
	OPTION-indikator	0	IID ikke til stede
	OPTION-indikator	1	AttributeIdList til stede
	Fyld BIT STRING(SIZE(1))	0	Sæt til 0.
10	EID INTEGER(0..127,…)	xxxx xxxx	EID-for RTM-applikationshændelsen som specificeret i VST. Ingen udvidelse
11	AttributeIdList SEQUENCE OF { AttributeId }}	0000 0001	Ingen udvidelse, antal attributter = 1
12		0000 0001	AttributeId=1, RtmData. Ingen udvidelse
13	FCS	xxxx xxxx	Sekvens for rammekontrol
14		xxxx xxxx	
15	Markør	0111 1110	Slutmarkør

▼B

DSC_50 Når *DSRC-køretøjsenheden* modtager GET-anmodningen, sender den et GET-svar med de ønskede data i henhold til GET-svaret som defineret i EN 13372, 6.2, 6.3, 6.4 and EN 12834 med indstillinger som specificeret i tabel 14.12.

Tabel 14.12

Præsentation — Rammeindstillinger for GET-svar

Felt	Indstillinger
Identifikator for aktiverende applikationsenhed (IID)	Ikke til stede
Linkidentifikator (LID)	I henhold til EN 12834
Sammenkædning	Nej
Elementidentifikator (EID)	Som specificeret i VST.
Adgangsoplysninger	Nej
Fragmentering	Nej
Lag2-indstillinger	Svar-PDU, Svar tilgængeligt og kommando accepteret, ACn-kommando

Tabel 14.13 viser et eksempel på læsning af RTM-dataene.

Tabel 14.13

Præsentation — Eksempel på indhold af svarramme

Oktet nr.	Attribut/Felt	Bit i oktet	Beskrivelse
1	MARKØR	0111 1110	Startmarkør
2	Privat LID	xxxx xxxx	Linkadresse på den specifikke DSRC-køretøjsenhed
3		xxxx xxxx	
4		xxxx xxxx	
5		xxxx xxxx	
6	MAC-kontrolfelt	1101 0000	Svar-PDU
7	LLC-kontrolfelt	n111 0111	Svar tilgængeligt, ACn-kommando n bit
8	LLC-statusfelt	0000 0000	Svar tilgængeligt og kommando accepteret
9	Fragmenterings-header	1xxx x001	Ingen fragmentering
10	Get.response SEQUENCE {	0111	Get response

▼B

Oktet nr.	Attribut/Felt	Bit i oktet	Beskrivelse
	OPTION-indikator	0	IID ikke til stede
	OPTION-indikator	1	Attributliste til stede
	OPTION-indikator	0	Returstatus ikke til stede
	Fyld BIT STRING(SIZE(1))	0	(ikke anvendt)
11	EID INTEGER(0..127,…)	xxxx xxxx	Svar fra RTM-applikationen Hændelse. Ingen udvidelse,
12	AttributeList SEQUENCE OF {	0000 0001	Ingen udvidelse, antal attributter = 1
13	Attributter SEQUENCE { AttributeId	0000 0001	Ingen udvidelse, AttributeId=1 (RtmData)
14	AttributeValue CONTAINER {	0000 1010	Ingen udvidelse, Containervalg = 10_{10}.
15		kkkk kkkk	RtmData
16		kkkk kkkk	
17		kkkk kkkk	
…		…	
n	}}}}	kkkk kkkk	
n + 1	FCS	xxxx xxxx	Sekvens for rammekontrol
n + 2		xxxx xxxx	
n + 3	Markør	0111 1110	Slutmarkør

DSC_51 Herefter lukker REDCR'en forbindelsen ved at udsende en EVENT_REPORT_RELEASE-kommando i henhold til EN 13372, 6.2, 6.3, 6.4 og EN 12834, 7.3.8 uden specifikke RTM-indstillinger. Tabel 14.14 viser et bitkodningseksempel på RELEASE-kommandoen.

Tabel 14.14

Afslutning. EVENT_REPORT Frigiv rammeindhold

Oktet nr.	Attribut/Felt	Bit i oktet	Beskrivelse
1	MARKØR	0111 1110	Startmarkør
2	Privat LID	xxxx xxxx	Linkadresse på den specifikke DSRC-køretøjsenhed
3		xxxx xxxx	
4		xxxx xxxx	

▼B

Oktet nr.	Attribut/Felt	Bit i oktet	Beskrivelse
5		xxxx xxxx	
6	MAC-kontrolfelt	1000 s000	Rammen indeholder en kommando-LPDU
7	LLC-kontrolfelt	0000 0011	UI-kommando
8	Fragmenterings-header	1xxx x001	Ingen fragmentering
9	EVENT_REPORT.request SEQUENCE {	0010	EVENT_REPORT (Release)
	OPTION-indikator	0	Adgangsoplysninger ikke til stede
	OPTION-indikator	0	Begivenhedsparameter ikke til stede
	OPTION-indikator	0	IID ikke til stede
	Tilstand BOOLEAN	0	Intet svar forventet
10	EID INTEGER (0..127,…)	0000 0000	Ingen udvidelse, EID = 0 (System)
11	EventType INTEGER (0..127,…) }	0000 0000	Begivenhedstype 0 = Frigiv
12	FCS	xxxx xxxx	Sekvens for rammekontrol
13		xxxx xxxx	
14	Markør	0111 1110	Slutmarkør

DSC_52 *DSRC-køretøjsenheden* forventes ikke at svare på RELEASE-kommandoen. Herefter afsluttes kommunikationen.

5.4.8 *Beskrivelse af DSRC-afprøvningstransaktion*

DSC_53 Fuldstændig afprøvning, der omfatter sikring af dataene, skal gennemføres som defineret i tillæg 11, Fælles sikkerhedsmekanismer, af godkendte personer med adgang til sikkerhedsprocedurer ved hjælp af de normale GET-kommandoer, som defineres ovenfor.

DSC_54 Idriftsættelse og periodiske inspektionsprøvninger, der kræver dekryptering og forståelse af det dekrypterede dataindhold, skal foretages som specificeret i tillæg 11, Fælles sikkerhedsmekanismer, og tillæg 9, Typegodkendelsesliste over minimumskrav vedrørende afprøvning.

Den grundlæggende DSRC-kommunikation kan imidlertid afprøves med kommandoen ECHO. Sådanne afprøvninger kan være påkrævet ved idriftsættelse, ved periodiske inspektioner eller på andre tidspunkter efter krav fra den kompetente kontrolmyndighed eller forordning (EU) nr. 165/2014 (Se 6 nedenfor)

▼B

DSC_55 For at udføre denne basale kommunikationsafprøvning udsteder REDCR ECHO-kommandoen under en session, dvs. når en initialiseringsfase er afsluttet planmæssigt. Sekvensen af interaktioner svarer derfor til en anmodning:

— Trin 1 *REDCR'en* sender en "Beacon Service Table" (BST), der indeholder applikationsidentifikatorerne (AID'er) på den tjenesteliste, som den understøtter. I RTM-applikationerne bliver dette ganske enkelt tjenesten med AID-værdien = 2.

DSRC-køretøjsenheden evaluerer den modtagne BST, og når den konstaterer, at BST'en forespørger Freight&Fleet (AID = 2), svarer DSRC-køretøjsenheden. Hvis *REDCR'en* ikke sender AID = 2, afslutter *DSRC-køretøjsenheden* sin transaktion med *REDCR'en*.

— Trin 2 *DSRC-køretøjsenheden* sender en anmodning om tildeling af et privat vindue.

— Trin 3 REDCR'en sender en tildeling af et privat vindue.

— Trin 4 *DSRC-køretøjsenheden* anvender det tildelte private vindue til at sende sin køretøjsservicetabel (Vehicle Service Table — VST). Denne VST indeholder en liste med alle de forskellige applikationsforekomster, som denne *DSRC-køretøjsenhed* understøtter i AID = 2-rammen. De forskellige forekomster identificeres ved hjælp af entydige EID'er, hver tilhørende en parameterværdi, der viser forekomsten af den understøttede applikation.

— Trin 5 Derefter analyserer *REDCR'en* den tilbudte VST og afslutter enten forbindelsen (RELEASE), da den ikke er interesseret i noget af det, VST'en kan tilbyde (dvs. at den modtager en VST fra en *DSRC-køretøjsenhed*, der er en RTM-køretøjsenhed, eller hvis den modtager en passende VST, starter den en app-forekomst.

— Trin 6 *REDCR'en* udsteder en kommando (ECHO) til den specifikke *DSRC-køretøjsenhed* og tildeler et privat vindue.

— Trin 7 *DSRC-køretøjsenheden* bruger det nye tildelte private vindue til at sende en ECHO-svarramme.

Følgende tabeller indeholder et praktisk eksempel på en ECHO-udvekslingssession.

DSC_56 Initialiseringen udføres i henhold til 5.4.7 (DSC_44-DSC_48) og tabel 14.4-14.9.

DSC_57 Herefter udsteder REDCR'en en ECHO-kommando i henhold til ISO 14906, der indeholder 100 dataoktetter, og uden specifikke indstillinger for RTM. Tabel 14.15 viser indholdet af den ramme, som REDCR'en sender.

▼B

Tabel 14.15

Eksempel på ramme for ACTION, ECHO-anmodning

Oktet nr.	Attribut/Felt	Bit i oktet	Beskrivelse
1	MARKØR	0111 1110	Startmarkør
2	Privat LID	xxxx xxxx	Linkadresse på den specifikke DSRC-køretøjsenhed
3		xxxx xxxx	
4		xxxx xxxx	
5		xxxx xxxx	
6	MAC-kontrolfelt	1010 s000	Kommando-PDU
7	LLC-kontrolfelt	n111 0111	Udsendt ACn-kommando, n bit
8	Fragmenterings-header	1xxx x001	Ingen fragmentering
9	ACTION.request SEQUENCE {	0000	Anmodning om handling (ECHO)
	OPTION-indikator	0	Adgangsoplysninger ikke til stede
	OPTION-indikator	1	Handlingsparameter til stede
	OPTION-indikator	0	IID ikke til stede
	Tilstand BOOLEAN	1	Svar forventet
10	EID INTEGER (0..127,…)	0000 0000	Ingen udvidelse, EID = 0 (System)
11	ActionType INTEGER (0..127,…)	0000 1111	Ingen udvidelse, anmodning om handlingstypen ECHO
12	ActionParameter CONTAINER {	0000 0010	Ingen udvidelse, Containervalg = 2
13		0110 0100	Ingen udvidelse. Strenglængde = 100 oktetter
14		xxxx xxxx	Data, der skal besvares
…		…	
113	}}	xxxx xxxx	
114	FCS	xxxx xxxx	Sekvens for rammekontrol
115		xxxx xxxx	
116	Markør	0111 1110	Slutmarkør

▼B

DSC_58 Når *DSRC-køretøjsenheden* modtager ECHO-anmodningen, sender den et ECHO-svar på 100 dataoktetter ved at gentage den modtagne kommando i henhold til ISO 14906 uden specifikke indstillinger for RTM. Tabel 14.16 viser et eksempel på bitniveaukodning.

Tabel 14.16

Eksempel på ramme for ACTION, ECHO-svar

Oktet nr.	Attribut/Felt	Bit i oktet	Beskrivelse
1	MARKØR	0111 1110	Startmarkør
2	Privat LID	xxxx xxxx	Linkadresse på den specifikke køretøjsenhed
3		xxxx xxxx	
4		xxxx xxxx	
5		xxxx xxxx	
6	MAC-kontrolfelt	1101 0000	Svar-PDU
7	LLC-kontrolfelt	n111 0111	ACn-kommando n bit
8	LLC-statusfelt	0000 0000	Svar tilgængeligt
9	Fragmenterings-header	1xxx x001	Ingen fragmentering
10	ACTION.response SEQUENCE {	0001	ACTION-svar (ECHO)
	OPTION-indikator	0	IID ikke til stede
	OPTION-indikator	1	Svarparameter til stede
	OPTION-indikator	0	Returstatus ikke til stede
	Fyld BIT STRING (SIZE (1))	0	(ikke anvendt)
11	EID INTEGER (0..127,…)	0000 0000	Ingen udvidelse, EID = 0 (System)
12	ResponseParameter CONTAINER {	0000 0010	Ingen udvidelse, Containervalg = 2
13		0110 0100	Ingen udvidelse. Strenglængde = 100 oktetter
14		xxxx xxxx	Besvarede data
…		…	
113	}}	xxxx xxxx	
114	FCS	xxxx xxxx	Sekvens for rammekontrol
115		xxxx xxxx	
116	Markør	0111 1110	Slutmarkør

▼B

5.5 **Understøttelse af direktiv 2015/71/EF**

5.5.1 *Oversigt*

DSC_59 For at understøtte direktiv 2015/719/EF om største tilladte dimensioner og største tilladte vægt for tunge lastbiler bliver transaktionsprotokollen til overførsel af OWS-data via 5,8 GHz DSRC-interfaceforbindelsen den samme, som bruges til RTM-data (se 5.4.1), idet den eneste forskel bliver, at den objektidentifikator, der vedrører TARV-standarden, vil henholde sig til ISO 15638-standarden (TARV), del 20, vedrørende WOB/OWS.

5.5.2 *Kommandoer*

DSC_60 Kommandoen til en OWS-transaktion vil være den samme som til en RTM-transaktion.

5.5.3 *Kommandosekvens ved anmodning*

DSC_61 Kommandosekvensen til anmodning om OWS-data vil være den samme som for RTM-data.

5.5.4 *Datastrukturer*

DSC_62 Indholdsdataene (OWS-data) består af en sammenkædning af

1. EncryptedOwsPayload-data, som er krypteringen af OwsPayload som defineret i ASN.1 i afsnit 5.5.5. Krypteringsmetoden er den samme, som anvendes til RtmData, som specificeres i tillæg 11

2. DSRCSecurityData, beregnet med de samme algoritmer, som anvendes til RtmData, som specificeres i tillæg 11.

▼B

5.5.5 *ASN.1-modul til OWS DSRC-transaktionen*

DSC_63. ASN.1-moduldefinitionen for DSRC-dataene inden for RTM-applikationen defineres som følger:

```
   TarvOws {iso(1) standard(0) 15638 part20(20)
   version1(1)} DEFINITIONER AUTOMATISKE ETIKETTER
   ::= BEGIN
   IMPORTS
   -- Importerer dataattributter og -elementer fra EFC, der anvendes til OWS
   LPN
   FROM EfcDsrcApplication {iso(1) standard(0) 14906 application(0) version5(5)}

   -- Importerer funktionsparametre fra EFC-applikationsinterfacedefinitionen
   SetMMIRq
   FROM EfcDsrcApplication {iso(1) standard(0) 14906 application(0) version5(5)}

   -- Importerer L7 DSRCData-moduldata fra EFC-applikationsinterfacedefinitionen
   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)};

   -- Definitioner af OWS-funktionerne:
   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} (MED KOMPONENTER {..., eid, iid ABSENT})
   OWS-TerminateComm::= Event-Report-Request {OwsContainer}(MED KOMPONENTER {mode (FALSE), eid (0),
   eventType (0)})
   OWS-TestComm-Request::= Action-Request {OwsContainer} (MED KOMPONENTER {..., eid (0), actionType
   (15), accessCredentials ABSENT, iid ABSENT})
   OWS-TestComm-Response::= Action-Response {OwsContainer} (MED KOMPONENTER {..., fill (SIZE(1)), eid
   (0), iid ABSENT})

   -- Definitioner af OWS-attributterne:
   OwsData :: = SEQUENCE {
        encryptedOwsPayload OCTET STRING (SIZE(51)) (BEGRÆNDET AF { -- beregnet ved kryptering af
   OwsPayload i henhold til tillæg 11 --}),
        DSRCSecurityData OCTET STRING
        }
   OwsPayload :: = SEQUENCE {
               tp15638VehicleRegistrationPlate LPN -- Køretøjets nummerplader i henhold til EN 15509.
               recordedWeight INTEGER (0..65535),            -- 0= Samlet målt vægt af den tunge lastbil
                                                                  -- med en opløsning på 10 Kg.
               axlesConfiguration OCTET STRING SIZE (3),     -- 0= 20 bit tilladt for antal
                                                                  -- aksler ved 10 aksler.
               axlesRecordedWeight OCTET STRING SIZE (20),   -- 0= Registreret vægt for hver aksel
                                                                  -- med en opløsning på 10 Kg.
               tp15638TimestampINTEGER(0..4294967295)        -- Tidsstempel for aktuel post
        }

Ows-ContextMark ::= SEQUENCE {
  standardIdentifier    StandardIdentifier, -- identifikator for TARV-delen og dennes version
        }

StandardIdentifier ::= OBJEKTIDENTIFIKATOR
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,
-- værdierne fra 16 til 255 forbeholdt ISO/CEN-brug
        }}

END
```

▼B

5.5.6 *Elementer i OwsData, udførte handlinger og definitioner*

Elementerne i OwsData defineres med henblik på at understøtte direktiv 2015/719/EF om de største tilladte dimensioner og den største tilladte vægt for tunge varekøretøjer. De har følgende betydning:

— recordedWeight står for det tunge varekøretøjs samlede målte vægt med en opløsning på 10 kg som defineret i EN ISO 14906. En værdi på 2500 står således for en vægt på 25 t.

— axlesConfiguration står for det tunge varekøretøjs konfiguration som antallet af aksler. Konfigurationen defineres med bitmasken på 20 bit (en udvidelse i forhold til EN ISO 14906).

En bitmaske på 2 bit repræsenterer konfigurationen af en aksel med følgende format:

— Værdien 00B betyder, at værdien er "ikke tilgængelig", fordi køretøjet ikke har udstyr til at registrere vægten på akslen.

— Værdien 01B betyder, at akslen ikke er til stede.

— Værdien 10B betyder, at akslen er til stede, og at vægten er beregnet og indsamlet og vises i feltet axlesRecordedWeight.

— Værdien 11B er forbehold fremtidig brug.

De sidste 4 bit er forbeholdt fremtidig brug.

Antal aksler										
Antal aksler på trækkerenheden			Antal akser på anhængeren							
00/01/10/11	00/01/10/11	00/01/10/11	00/01/10/11	00/01/10/11	00/01/10/11	00/01/10/11	00/01/10/11	00/01/10/11	00/01/10/11	RFU (4 bit)

— axlesRecordedWeight står for den specifikke registrerede vægt for hver aksel med en opløsning på 10 kg. Der benyttes to oktetter til hver aksel. En værdi på 150 står således for en vægt på 1 500 kg.

De øvrige datatyper defineres i 5.4.5.

5.5.7 *Dataoverførselsmekanismer*

DSC_64 Dataoverførselsmekanismen for OWS-data mellem interrogatoren og DSRC-enheden på køretøjet er den samme som for RTM-data (se 5.4.6).

DSC_65 Dataoverførslen mellem platformen, der indsamler data om maksimal vægt, og DSRC-enheden på køretøjet er baseret på den fysiske forbindelse og interfaces og protokol som defineres i afsnit 5.6.

5.6 **Dataoverførsel mellem DSRC-køretøjsenheden og køretøjsenheden**

5.6.1 *Fysisk forbindelse og interfaces*

DSC_66 Forbindelsen mellem *køretøjsenheden* og *DSRC-køretøjsenheden* kan enten etableres med et fysisk kabel eller med trådløs kommunikation med kort rækkevidde baseret på Bluetooth v4.0 BLE.

▼B

DSC_67 Uanset valget af den fysiske forbindelse og interfacet skal følgende krav være opfyldt:

DSC_68 a) For at give mulighed for at bestille køretøjsenheden og DSRC-køretøjsenheden og forskellige partier af DSRC-køretøjsenheder fra forskellige leverandører skal forbindelsen mellem køretøjsenheden og DSRC-køretøjsenheden være en åben standardforbindelse. Køretøjsenheden forbindes enten med DSRC-køretøjsenheden

i) via et fast kabel på mindst 2 m, hvorpå der er monteret et lige DIN 41612 H11-stik — godkendt hanstik med 11 stikben fra DSRC-køretøjsenheden, så den passer til et tilsvarende DIN/ISO-godkendt hunstik fra køretøjsenheden

ii) ved hjælp af Bluetooth Low Energy (BLE)

iii) ved hjælp af en standard ISO 11898- eller SAE J1939-forbindelse.

DSC_69 b) Definitionen af interfacene og forbindelsen mellem køretøjsenheden og DSRC-køretøjsenheden skal understøtte kommandoerne til applikationsprotokollen, som defineres i 5.6.2.

DSC_70 c) Køretøjsenheden og DSRC-køretøjsenheden skal understøtte dataoverførsel via forbindelsen for så vidt angår ydelse og strømforsyning.

5.6.2 *Applikationsprotokol*

DSC_71 Applikationsprotokollen mellem køretøjsenhedens fjernkommunikationsudstyr og DSRC-køretøjsenheden skal periodisk overføre data fra fjernkommunikationsudstyret til DSRC'en.

DSC_72 Følgende centrale kommandoer er identificeret:

1. Initialisering af kommunikationsforbindelsen — Anmodning

2. Initialisering af kommunikationsforbindelsen — Svar

3. Send Data med RTM-applikationens identifikator og dataindhold defineret ved RTM-data

4. Bekræftelse af dataene

5. Afslutning af kommunikationsforbindelsen — Anmodning

6. Afslutning af kommunikationsforbindelsen — Svar.

DSC_73 I ASN1.0 kan de forudgående kommandoer være defineret som:

▼B

```
DT-protokol til fjernkommunikation DEFINITIONER ::= BEGIN

     Initialisering af RCDT-kommunikationslink - Anmodning ::=
          SEQUENCE { LinkIdentifier INTEGER
     }

     Initialisering af RCDT-kommunikationslink - Svar ::= SEQUENCE {
          LinkIdentifier INTEGER,
          svar        BOOLEAN
     }

          RCDT- Send Data ::=
          SEQUENCE { LinkIdentifier
          INTEGER, DataTransactionId
          INTEGER, RCDTData
          SignedTachographPayload
     }

          RCDT Databekræftelse ::
          SEQUENCE { LinkIdentifier
          INTEGER, DataTransactionId
          INTEGER,
          svar         BOOLEAN
     }

          Afbrydelse af RCDT-kommunikationslink - Anmodning ::=
          SEQUENCE { LinkIdentifier INTEGER
     }

          Afbrydelse af RCDT-kommunikationslink - Svar ::= SEQUENCE {
          LinkIdentifier INTEGER,
          svar         BOOLEAN
     }

End
```

DSC_74 Kommandoerne og parametrene beskrives som følger:

— RCDT-Communication Link Initialization – Request
bruges til at initialisere kommunikationsforbindelsen. Køretøjsenheden sender kommandoen til DSRC-køretøjsenheden. LinkIdentifier fastsættes af køretøjsenheden og kommunikeres til DSRC-køretøjsenheden for at spore en bestemt kommunikationsforbindelse.

(Bemærk: Dette sker for at understøtte fremtidige forbindelser og andre applikationer/moduler som Weighing on board).

— RCDT-Communication Link Initialization – Response
bruges af DSRC-køretøjsenheden til at sende svaret på anmodningen om at initialisere kommunikationsforbindelsen. DSRC-køretøjsenheden sender kommandoen til køretøjsenheden. Kommandoen giver resultatet af initialiseringen som svar 1 (lykkedes) eller 0 (mislykkedes).

DSC_75 Initialiseringen af kommunikationsforbindelsen foretages først efter installering, kalibrering og start af motor/køretøjsenhed.

▼B

— RCDT-Send Data bruges af køretøjsenheden til at sende de underskrevne RCDT-data (dvs. *fjernkommunikationsdataene*) til DSRC-køretøjsenheden. Dataene sendes hvert 60. sekund. Parameteren DataTransactionId identificerer den specifikke transmission af data. LinkIdentifier bruges også til at sikre, at den pågældende forbindelse er korrekt.

— RCDT-Data Acknowledgment sendes af DSRC-køretøjsenheden for at give feedback til køretøjsenheden om modtagelse af data fra en RCDT-Send Data-kommando, som identificeres af DataTransactionId-parameteren. Svarparameteren er 1 (lykkedes) eller 0 (mislykkedes). Hvis en bevægelsessensor modtager mere end tre svar på 0, eller hvis køretøjsenheden ikke modtager en RCDT-databekræftelse for en bestemt tidligere fremsendt RCDT-Send Data med en specifik DataTransactionId, genererer og registrerer køretøjsenheden en hændelse.

— RCDT-Communication Link Termination request sendes af køretøjsenheden til DSRC-køretøjsenheden for at afslutte en forbindelse for en bestemt LinkIdentifier.

DSC_76 Ved genstart af DSRC-køretøjsenheden eller en bevægelsessensor skal alle eksisterende kommunikationsforbindelser afbrydes, da der kan være forbindelser, der "hænger" som følge af en pludselig nedlukning af en bevægelsessensor.

— RCDT-Communication Link Termination – Response sendes af DSRC-køretøjsenheden til køretøjsenheden for at bekræfte køretøjsenhedens anmodning om afbrydelse af forbindelsen for den specifikke LinkIdentifier.

5.7 **Fejlhåndtering**

5.7.1 *Registrering og kommunikation af data i DSRC-køretøjsenheden*

DSC_77 *Dataene* skal leveres af *VUSM*-funktionen til *DSRC-køretøjsenheden* og skal allerede være sikrede. *VUSM'en* kontrollerer, at dataene, der er registreret i *DSRC-køretøjsenheden*, er blevet registeret korrekt. Registrering og indberetning af eventuelle fejl i dataoverførslen fra køretøjsenheden til *DSRC-køretøjsenhedens* hukommelse skal registreres med typen EventFaultType og en enum-værdi på "62"H kommunikationsfejl ved fjernkommunikation sammen med tidsstemplet.

DSC_78 Køretøjsenheden fører et register, der identificeres med et entydigt navn, om inspektørerne nemt kan identificere i forbindelse med registrering af "interne kommunikationsfejl i køretøjsenhed".

DSC_79 Hvis VUPM'en forsøger at hente køretøjsenhedsdata fra sikkerhedsmodulet (for at sende dem videre til DSRC-køretøjsenheden), men dette ikke lykkes, registrerer den denne fejl med typen EventFaultType og en enum-værdi på *'62'H kommunikationsfejl ved fjernkommunikation* sammen med

▼B

tidsstemplet. Kommunikationsfejlen detekteres, når der ikke modtages en `RCDT Data Acknowledgment`-meddelelse for den tilhørende (dvs. med det samme DataTransactionId i meddelelserne `Send Data and Acknowledgment`) `RCDT Send Data` mere end tre på hinanden følgende gange.

5.7.2 *Fejl i trådløs kommunikation*

DSC_80 Håndteringen af kommunikationsfejl skal ske i henhold til de tilhørende DSRC-standarder, dvs. EN 300 674-1, EN 12253, EN 12795, EN 12834 og de tilhørende parametre i EN 13372.

5.7.2.1 *Krypterings- og underskriftfejl*

DSC_81 Krypterings- og signaturfejl skal håndteres som defineret i tillæg 11, Fælles sikkerhedsmekanismer, og findes ikke i nogen fejlmeddelelser i forbindelse med DSRC-dataoverførslen.

5.7.2.2 *Fejlregistrering*

DSRC-mediet er en dynamisk trådløs kommunikation i et miljø med usikre atmosfæriske forhold og interferensforhold, navnlig i kombinationerne ”transportabel REDCR” og ”køretøj i bevægelse”, som denne applikation omfatter. Derfor er det nødvendigt at vurdere forskellen mellem en ”læsefejl”- og en ”fejl”-tilstand. I en transaktion via et trådløst interface er læsefejl almindelige, og konsekvensen er normalt, at man prøver igen, dvs. at BST'en sendes igen, og man forsøger sekvensen igen, og i de fleste tilfælde vil det føre til en vellykket kommunikationsforbindelse og dataoverførsel, medmindre det pågældende køretøj bevæger sig uden for rækkevidde i løbet af det tidsinterval, som er nødvendigt for at sende dataene igen (en ”vellykket” ”læsning” kan have omfattet flere forsøg og gentagelser).

Læsefejl kan skyldes, at antennerne ikke var parret korrekt (”sigtefejl”), at en af antennerne er skærmet — dette kan være bevidst, men kan også skyldes, at et andet køretøj er fysisk til stede, radiointerferens, navnlig fra omkring 5,8 GHz WIFI eller andre typer af trådløs kommunikation med offentlig adgang, eller at der forekommer radarinterferens eller problematiske atmosfæriske forhold (f.eks. under et tordenvejr) eller ganske enkelt, fordi man bevæger sig uden for DSRC-kommunikationsudstyrets rækkevidde. Individuelle forekomster af læsefejl kan i sagens natur ikke registreres, fordi kommunikationen ganske enkelt ikke finder sted.

Men hvis repræsentanten for den kompetente kontrolmyndighed retter opmærksomheden mod et køretøj og forsøger at sende en anmodning til dets *DSRC-køretøjsenhed*, men der sker ikke nogen vellykket dataoverførsel, kan fejlen være opstået som følge af bevidst manipulation, og derfor har repræsentanten for den kompetente kontrolmyndighed behov for et værktøj til at logge fejlen og gøre kollegerne længere henne opmærksom på, at der kan være tale om en overtrædelse. Herefter kan kollegerne standse køretøjet og foretage en fysisk inspektion. Men eftersom der ikke er foregået nogen vellykket kommunikation, kan DSRC-køretøjsenheden ikke levere data vedrørende fejlen. Denne rapportering skal derfor være en funktion i designet af REDCR-udstyret.

”Læsefejl” er teknisk set forskellig fra en ”fejl”. I denne forbindelse er en ”fejl” indhentning af en forkert værdi.

▼B

Data, der overføres til *DSRC-køretøjsenheden*, leveres i en allerede sikret form, og skal derfor verificeres af dataleverandøren (se 5.4).

Data, der efterfølgende overføres via luft-interfacet, kontrolleres med cykliske redundanskontroller (CRC) på kommunikationsniveau. Hvis CRC valideres, er dataene korrekte. Hvis CRC ikke valideres, sendes dataene igen. Sandsynligheden for, at data kan slippe forkert igennem en CRC, er statistisk set så lille, at den lades ude af betragtning.

Hvis CRC'en ikke valideres, og der ikke er tid til at gensende og modtage de korrekte data, bliver resultatet ikke en fejl, men en forekomst af en bestemt type læsefejl.

De eneste meningsfulde ”fejl”-data, der kan registreres, er antallet af vellykkede transaktionsindledninger, der forekommer, og som ikke fører til en vellykket overførsel af data til REDCR.

DSC_82 *REDCR'en* registrerer og tidsstempler derfor antallet af tilfælde, hvor ”initialiseringsfasen” for en DSRC-anmodning lykkes, men hvor transaktionen afsluttes, inden REDCR'en har modtaget *dataene*. Disse data skal være tilgængelige for repræsentanten for den kompetente kontrolmyndighed og skal gemmes i REDCR-udstyrets hukommelse. Dette opnås ved hjælp af produktets udformning eller i henhold til specifikationen fra en kompetent kontrolmyndighed.

De eneste meningsfyldte ”fejl”-data, der kan registreres, er antallet af tilfælde, hvor REDCR'en ikke kan dekryptere de modtagne *data*. Det skal imidlertid bemærkes, at dette udelukkende vil vedrøre effektiviteten af REDCR'ens software. Data kan dekrypteres teknisk, men uden at give mening rent semantisk.

DSC_83 *REDCR'en* skal derfor registrere og tidsstemple antallet af tilfælde, hvor den har forsøgt af dechifrere data modtaget via DSRC-interfacet, men hvor dette er mislykkedes.

6 IDRIFTSÆTTELSE OG PERIODISKE INSPEKTIONSAFPRØVNINGER FOR FJERNKOMMUNIKATIONSFUNKTIONEN

6.1 **Generelt**

DSC_84 Der er mulighed for to typer afprøvning af fjernkommunikationsfunktionen:

1) En ECHO-afprøvning for at validere den trådløse kommunikationskanal mellem *DSRC-REDCR >>-:-<DSRC-køretøjsenheden*.

2) En ende-til-ende-sikkerhedsafprøvning for at sikre, at der forefindes et værkstedskort, der giver mulighed for at få adgang til det krypterede og underskrevne dataindhold, som køretøjsenheden har genereret og transmitteret via den trådløse kommunikationskanal.

6.2 **ECHO**

Dette punkt indeholder bestemmelser, der er udformet specifikt til kun at afprøve, om *DSRC-REDCR >>-:-<DSRC-køretøjsenheden* er funktionelt aktiv.

▼B

Formålet med ECHO-kommandoen er at give værksteder eller prøveanlæg til typegodkendelse mulighed for at efterprøve, at DSRC-forbindelsen fungerer uden at kræve adgang til sikkerhedsoplysninger. Derfor skal afprøvningsudstyret kun være i stand til at initialisere en DSRC-kommunikation (at sende en BST med AID = 2) og derefter sende ECHO-kommandoen, og, hvis man antager, at DSRC'en virker, modtage ECHO-svaret. Se 5.4.8 for nærmere oplysninger. Idet man går ud fra, at dette svar modtages korrekt, kan DSRC-forbindelsen (*DSRC-REDCR >>-:-<DSRC-køretøjsenheden*) valideres som fungerende korrekt.

6.3 **Afprøvning til validering af sikkert dataindhold**

DSC_85 Dette afprøvning gennemføres for at validere ende-til-ende-sikkerheden for datastrømmen. Der er behov for en DSRC-testlæser til en sådan afprøvning. DSRC-testlæseren udfører den samme funktion, og anvendes med de samme specifikationer som den læser, de retshåndhævende myndigheder benytter, med den forskel, at der skal benyttes et værkstedskort til at godkende brugeren af DSRC-testlæseren i stedet for et kontrolkort. Afprøvningen kan udføres efter den indledende aktivering af en intelligent takograf eller ved afslutningen af kalibreringsproceduren. Efter aktiveringen genererer køretøjsenheden de sikrede data til tidlig fjernafsløring og sender disse til DSRC-køretøjsenheden.

DSC_86 Værkstedspersonalet skal anbringe DSRC-testlæseren i en afstand af mellem 2 og 10 meter foran køretøjet.

DSC_87 Herefter isætter værkstedspersonalet et værkstedskort i DSRC-testlæseren for at anmode køretøjsenheden om data vedrørende tidlig fjernafsløring. Efter en vellykket anmodning går værkstedspersonalet ind i dataene for at sikre, at de er dekrypterede og valideret korrekt for så vidt angår integriteten.

▼B

Tillæg 15

MIGRATION: FORVALTNING AF SAMEKSISTENSEN AF UDSTYRSGENERATIONER

INDHOLDSFORTEGNELSE

1. DEFINITIONER

2. ALMINDELIGE BESTEMMELSER

2.1. Oversigt over overgangen

2.2. Interoperabilitet mellem køretøjsenhed og kort

2.3. Interoperabilitet mellem køretøjsenhed og bevægelsesføler

2.4. Interoperabilitet mellem køretøjsenheder, takografkort og udstyr til dataoverførsel

2.4.1 IDE'ens direkte overførsel af kort

2.4.2 Overførsel af kort via en køretøjsenhed

2.4.3 Overførsel fra køretøjsenhed

2.5. Interoperabilitet mellem køretøjsenhed og kalibrerings-udstyr

3. VIGTIGSTE SKRIDT I PERIODEN OP TIL INDFØRELSESDATOEN

4. BESTEMMELSER I PERIODEN EFTER INDFØRELSESDATOEN

1. DEFINITIONER

I dette tillæg anvendes følgende definitioner.

digitalt takografsystem*:* som defineret i dette bilag (kapitel 1: definition bbb)

digitalt takografsystem af første generation*:* som defineret i denne forordning (kapitel 2: definition b)

digitalt takografsystem af anden generation*:* som defineret i denne forordning (kapitel 2: definition j)

indførelsesdato*:* som beskrevet i dette bilag (kapitel 1: definition ccc)

intelligent dedikeret udstyr (IDE)*:* udstyr, der anvendes til at foretage dataoverførsel som defineret i tillæg 7 i dette bilag.

2. ALMINDELIGE BESTEMMELSER

2.1. **Oversigt over overgangen**

Præamblen til dette bilag indeholder en oversigt over overgangen mellem digitale takografsystemer af første og anden generation.

Ud over bestemmelserne i denne præambel:

— vil bevægelsesfølere af første generation ikke være interoperable med køretøjsenheder af anden generation

— vil bevægelsesfølere af anden generation begynde at blive installeret i køretøjer samtidig med køretøjsenheder af anden generation

▼B

— skal udstyr til dataoverførsel og kalibrering udvikles for at understøtte begge generationer af kontrolapparat og takografkort.

2.2. **Interoperabilitet mellem køretøjsenhed og kort**

Det forudsættes, at første generation af takografkort er interoperable med køretøjsenheder af første generation (i henhold til bilag 1B i denne forordning), mens takografkort af anden generation er interoperable med køretøjsenheder af anden generation (i henhold til bilag 1C i denne forordning). Desuden gælder følgende krav.

MIG_001 Bortset fra bestemmelserne i krav MIG_004 og MIG_005 kan takografkort af første generation fortsat benyttes i køretøjsenheder af anden generation, indtil deres gyldighedsperiode udløber. Indehaverne kan imidlertid anmode om at få dem udskiftet med takografkort af anden generation, så snart disse er til rådighed.

MIG_002 Køretøjsenheder af anden generation skal kunne anvende et hvilket som helst gyldigt fører-, kontrol- og virksomhedskort, der isættes.

MIG_003 Værksteder kan ophæve denne mulighed i sådanne køretøjsenheder, så takografkort af første generation ikke længere kan benyttes. Dette kan først ske, når Kommissionen har iværksat en procedure, der giver mulighed for at anmode værkstederne om at gøre dette, f.eks. under den periodiske inspektion af kontrolapparatet.

MIG_004 Køretøjsenheder af anden generation må kun kunne anvende værkstedskort af anden generation.

MIG_005 Med henblik på at fastlægge funktionstilstanden skal køretøjsenheder af anden generation udelukkende tage hensyn til typerne af de isatte gyldige kort, uanset generation.

MIG_006 Ethvert gyldigt takografkort af anden generation skal kunne benyttes i køretøjsenheder af første generation på præcis samme måde som et takografkort af første generation af samme type.

2.3. **Interoperabilitet mellem køretøjsenhed og bevægelsesføler**

Det forudsættes, at bevægelsesfølere af første generation er interoperable med køretøjsenheder af første generation, mens bevægelsesfølere af anden generation er interoperable med køretøjsenheder af anden generation. Desuden gælder følgende krav.

MIG_007 Køretøjsenheder af anden generation vil ikke kunne parres og anvendes med bevægelsesfølere af første generation.

MIG_008 Bevægelsesfølere af anden generation kan kun parres og anvendes med køretøjsenheder af anden generation eller med begge generationer af køretøjsenheder.

2.4. **Interoperabilitet mellem køretøjsenheder, takografkort og udstyr til dataoverførsel**

MIG_009 Udstyr til dataoverførsel kan kun benyttes sammen med køretøjsenheder og takografkort fra en generation eller med begge.

▼B

2.4.1 *IDE'ens direkte overførsel af kort*

MIG_010 IDE'en skal overføre data fra takografkort af en generation, som isættes deres kortlæsere, ved hjælp af sikkerhedsmekanismerne og dataoverførselsprotokollen for den pågældende generation, og de overførte data skal have det format, der er defineret for denne generation.

MIG_011 For at give kontrolmyndigheder uden for EU mulighed for at kontrollere førerne skal det ligeledes være muligt at overføre fører- (og værksteds-) kort af anden generation på præcis samme måde som fører- (og værksteds-) kort af første generation. En sådan overførsel omfatter:

— ikke-underskrevne elementærfilers `IC` og `ICC`

— ikke-underskrevne elementærfilers (første generation) `Card_Certificate` og `CA_Certificate`

— andre applikationsdatas elementærfiler (inden for `TACHO` DF), som overførselsprotokollen for kort af første generation forespørger. Disse oplysninger skal sikres med en digital underskrift i henhold til sikkerhedsmekanismerne af første generation.

En sådan overførsel skal ikke omfatte applikationsdatas elementærfiler, som kun findes på fører- (og værksteds-) kort af anden generation (applikationsdatas elementærfiler inden for `TACHO_G2` DF).

2.4.2 *Overførsel af kort via en køretøjsenhed*

MIG_012 Data skal overføres fra et kort af anden generation, der er isat en køretøjsenhed af første generation, ved hjælp af dataoverførselsprotokollen for første generation. Kortet skal besvare køretøjsenhedens kommandoer på præcis samme måde som et kort af første generation, og de overførte data skal have samme format som data, der er overført fra et kort af første generation.

MIG_013 Data skal overføres fra et kort af første generation, der er isat en køretøjsenhed af anden generation, ved hjælp af den dataoverførselsprotokol, der defineres i tillæg 7 til dette bilag. Køretøjsenheden sender kommandoer til kortet på præcis samme måde som en køretøjsenhed af første generation, og de overførte data skal overholde formatet, der er defineret for kort af første generation.

2.4.3 *Overførsel fra køretøjsenhed*

MIG_014 Data skal overføres fra køretøjsenheder af anden generation ved hjælp af sikkerhedsmekanismer af anden generation og dataoverførselsprotokollen, som specificeres i tillæg 7 til dette bilag.

MIG_015 For at give kontrolmyndigheder uden for EU mulighed for at foretage førerkontrol og værksteder uden for EU mulighed for at overføre data fra køretøjsenheder kan der gives mulighed for at overføre data fra køretøjsenheder af anden generation ved hjælp af sikkerhedsmekanismer af første generation og dataoverførselsprotokollen af første generation. De overførte data skal have samme format som data, der overføres fra en køretøjsenhed af første generation. Denne mulighed kan vælges via menukommandoerne.

▼B

2.5. **Interoperabilitet mellem køretøjsenhed og kalibreringsudstyr**

MIG_016 Kalibreringsudstyr skal kunne foretage kalibrering af hver generation af kontrolapparatet ved hjælp af den pågældende generations kalibreringsprotokol. Kalibreringsudstyr kan benyttes sammen med kun en generation af kontrolapparatet eller med begge.

3. VIGTIGSTE SKRIDT I PERIODEN OP TIL INDFØRELSESDATOEN

MIG_017 Prøvenøgler og certifikater skal være til rådighed for fabrikanter senest **30 måneder** før indførelsesdatoen.

MIG_018 Interoperabilitetsprøvning skal kunne sættes i gang, hvis fabrikanterne anmoder om dette, senest **15 måneder** før indførelsesdatoen.

MIG_019 Officielle nøgler og certifikater skal være til rådighed for fabrikanterne senest **12 måneder** før indførelsesdatoen.

MIG_020 Medlemsstaterne skal kunne udstede værkstedskort af anden generation senest **3 måneder** før indførelsesdatoen.

MIG_021 Medlemsstaterne skal kunne udstede alle typer af takografkort af anden generation senest **1 måned før indførelsesdatoen**.

4. BESTEMMELSER I PERIODEN EFTER INDFØRELSESDATOEN

MIG_022 Efter indførelsesdatoen må medlemsstaterne kun udstede takografkort af anden generation.

MIG_023 Fabrikanter af køretøjsenheder/bevægelsesfølere har tilladelse til at fremstille køretøjsenheder/bevægelsesfølere af første generation, så længe de bruges i praksis, således at det er muligt at udskifte fejlbehæftede komponenter.

MIG_024 Fabrikanter af køretøjsenheder/bevægelsesfølere har tilladelse til at anmode om og få typegodkendt vedligeholdelse af typer af køretøjsenheder/bevægelsesfølere af første generation, der allerede er typegodkendt.

▼B

Tillæg 16.

ADAPTER TIL KØRETØJER I KLASSE M1 OG N1

INDHOLDSFORTEGNELSE

1. FORKORTELSER OG REFERENCEDOKUMENTER
1.1. Forkortelser
1.2. Referencestandarder
2. ADAPTERENS GENERELLE EGENSKABER OG FUNKTIONER
2.1. Generel beskrivelse af adapteren
2.2. Funktioner
2.3. Sikkerhed
3. KRAV TIL KONTROLAPPARATET, NÅR EN ADAPTER ER INSTALLERET
4. KONSTRUKTIONS- OG FUNKTIONSKRAV TIL ADAPTEREN
4.1. Tilkobling og tilpasning af de indkommende hastighedsimpulser
4.2. Tilførsel af de indkommende impulser til den indlejrede bevægelsesføler
4.3. Indlejret bevægelsesføler
4.4. Sikkerhedskrav
4.5. Funktionsspecifikationer
4.6. Materialer
4.7. Påskrifter
5. INSTALLERING AF KONTROLAPPARATET, NÅR EN ADAPTER BENYTTES
5.1. Installering
5.2. Plombering
6. KONTROL, EFTERSYN OG REPARATIONER
6.1. Periodiske eftersyn
7. TYPEGODKENDELSE AF KONTROLAPPARATET, NÅR EN ADAPTER BENYTTES
7.1. Almindelige bestemmelser
7.2. Funktionsattest

1. FORKORTELSER OG REFERENCEDOKUMENTER

1.1. **Forkortelser**

TBD Endnu ikke fastlagt

VU Køretøjsenhed

1.2. **Referencestandarder**

ISO 16844-3 Road vehicles — Tachograph systems — Part 3: Motion sensor interface

2. ADAPTERENS GENERELLE EGENSKABER OG FUNKTIONER

2.1. **Generel beskrivelse af adapteren**

ADA_001 Adapteren skal forsyne en tilsluttet køretøjsenhed med sikrede køredata, der vedvarende repræsenterer kørehastighed og/eller tilbagelagt distance.

Adapteren er alene beregnet til køretøjer, som skal udstyres med et kontrolapparat i overensstemmelse med denne forordning.

▼B

Den skal kun installeres og anvendes i de under yy) "adapter" definerede køretøjstyper i bilag IC, når det mekanisk set ikke er muligt at installere nogen anden eksisterende type af bevægelsesfølere, som er i overensstemmelse med de øvrige bestemmelser i dette bilag og de tilhørende tillæg 1 til 16.

Adapteren må ikke være mekanisk forbundet med en bevægelig del af køretøjet, men alene forbindes med det sted, hvor de hastigheds-/afstandsrelaterede impulser frembringes af integrerede følere eller alternative tilkoblinger.

ADA_002 En typegodkendt bevægelsesfølere (i henhold til bestemmelserne i bilag IC, afsnit 8, Typegodkendelse af kontrolapparatur og takografkort) monteres i adapterhuset, som også skal indeholde en impulskonverteringsanordning, der tilfører de indkommende impulser til den indlejrede bevægelsesfølere. Den indlejrede bevægelsesfølere tilsluttes køretøjsenheden således, at tilkoblingen mellem køretøjsenheden og adapteren opfylder kravene i ISO16844-3.

2.2. **Funktioner**

ADA_003 Adapteren skal kunne udføre følgende funktioner:

— tilkobling og tilpasning af de indkommende hastighedsimpulser

— tilførsel af de indkommende impulser til den indlejrede bevægelsesfølere

— alle den indlejrede bevægelsesfølers funktioner, herunder sikrede køredata til køretøjsenheden.

2.3. **Sikkerhed**

ADA_004 Adapteren behøver ikke at være sikkerhedscertificeret ifølge det fælles sikkerhedsmål for bevægelsesfølere, som defineres i dette bilags tillæg 10. I stedet anvendes de sikkerhedsrelaterede krav, som specificeres i dette tillægs punkt 4.4.

3. KRAV TIL KONTROLAPPARATET, NÅR EN ADAPTER ER INSTALLERET

Kravene i de følgende kapitler angiver, hvorledes kravene i dette bilag skal fortolkes, når en adapter anvendes. Numrene på de tilknyttede krav i bilag IC anføres i parenteser.

ADA_005 Kontrolapparatet i ethvert køretøj, der udstyres med en adapter, skal opfylde alle bestemmelser i dette bilag, medmindre andet specificeres i dette tillæg.

ADA_006 Når en adapter er installeret, omfatter kontrolapparatet kabler, adapteren (inklusive en bevægelsesfølere) og en køretøjsenheden (01).

ADA_007 Detektionen af hændelser og/eller fejl ved kontrolapparater ændres på følgende måde:

— Hændelsen "afbrydelse af strømforsyning" skal udløses af køretøjsenheden, uden at apparatet er i kalibreringstilstand, såfremt afbrydelsen af den indlejrede bevægelsesfølers strømforsyning varer mere end 200 millisekunder [79].

▼B

— Hændelsen ”fejl i køredata” skal udløses af køretøjsenheden ved afbrydelse af den normale dataudveksling mellem den indlejrede bevægelsesføler og køretøjsenheden og/eller ved fejl i dataintegritet eller -ægthedskontrol under dataudveksling mellem den indlejrede bevægelsesføler og køretøjsenheden [83].

— Hændelsen ”forsøg på sikkerhedsbrud” skal udløses af køretøjsenheden ved enhver anden hændelse, som berører sikkerheden af den indlejrede bevægelsesføler, og som ikke finder sted i kalibreringstilstand [85].

— ”Fejl ved kontrolapparatet” skal udløses af køretøjsenheden, når et svigt i den indlejrede bevægelsesføler forekommer, uden at apparatet er i kalibreringstilstand [88].

ADA_008 Fejl ved adapteren, der detekteres af kontrolapparatet, skal være fejl i relation til den indlejrede bevægelsesføler [88].

ADA_009 Køretøjsenhedens kalibreringsfunktion skal give mulighed for, at den indlejrede bevægelsesføler automatisk samparres med køretøjsenheden [202, 204].

4. KONSTRUKTIONS- OG FUNKTIONSKRAV TIL ADAPTEREN

4.1. **Tilkobling og tilpasning af de indkommende hastighedsimpulser**

ADA_011 Adapterens indgangssignaltilkobling skal modtage frekvensimpulser, der er repræsentative for køretøjshastigheden og den tilbagelagte distance. De elektriske egenskaber af de indkommende impulser er: *Fastlægges af fabrikanten*. Med tilpasninger, som kun er tilgængelige for adapterfabrikanten og det godkendte værksted, der installerer adapteren, skal det om nødvendigt være muligt at foretage en korrekt tilkobling af adapterens indgangssignal til køretøjet.

ADA_012 Adapterens indgangssignaltilkobling skal om nødvendigt kunne multiplicere eller dividere frekvensimpulserne fra de indkommende hastighedsimpulser med en fastlagt faktor, for at tilpasse signalet til det k-faktorbånd, som defineres i dette bilag (4 000 til 25 000 impulser pr. km). Denne fastsatte faktor må kun programmeres af adapterfabrikanten og det godkendte værksted, som installerer adapteren.

4.2. **Tilførsel af de indkommende impulser til den indlejrede bevægelsesføler**

ADA_013 De indkommende impulser, der eventuelt tilpasses som specificeret ovenfor, tilføres den indlejrede bevægelsesføler således, at hver indkommende impuls detekteres af bevægelsesføleren.

4.3. **Indlejret bevægelsesføler**

ADA_014 Den indlejrede bevægelsesføler skal aktiveres af de tilførte impulser, så den kan generere køredata, som nøjagtigt repræsenterer køretøjets bevægelse, som om den var mekanisk forbundet med en bevægelig del af køretøjet.

ADA_015 Køretøjsenheden skal benytte den indlejrede bevægelsesfølers identifikationsdata til at identificere adapteren [95].

▼B

ADA_016 Monteringsdata, der lagres i den indlejrede bevægelsesføler, skal anses for at udgøre adapterens monteringsdata [122].

4.4. **Sikkerhedskrav**

ADA_017 Adapterhuset skal udformes således, at det ikke kan åbnes. Det skal plomberes, så forsøg på fysisk manipulation let kan afsløres (f.eks. ved besigtigelse, se ADA_035). Plomberingen skal overholde samme krav som plomberingen af bevægelsesfølerne [398 til 406].

ADA_018 Det må ikke være muligt at fjerne den indbyggede bevægelsesføler fra adapteren uden at bryde plomberingen af adapterhuset eller bryde plomberingen mellem føleren og adapterhuset (se ADA_034).

ADA_019 Adapteren skal sikre, at køredata alene beregnes og udledes på grundlag af adapterens indgangssignal.

4.5. **Funktionsspecifikationer**

ADA_020 Adapteren skal være fuldt funktionsdygtig i det temperaturinterval, som fabrikanten har defineret.

ADA_021 Adapteren skal være fuldt funktionsdygtig i fugtighedsintervallet 10 % til 90 % [214].

ADA_022 Adapteren skal være beskyttet mod overspænding, omvendt polaritet af strømtilførslen samt kortslutning [216].

ADA_023 Adapteren skal enten:

— reagere på et magnetisk felt, som forstyrrer detekteringen af køretøjets bevægelse. I dette tilfælde vil køretøjsenheden registrere og gemme en fejl ved føleren [88], eller

— have et følerelement, som er beskyttet mod eller er upåvirkelig af magnetfelter [217].

ADA_024 Adapteren skal være i overensstemmelse med den internationale bestemmelse UN ECE R10 om elektromagnetisk kompatibilitet og skal være beskyttet mod elektrostatiske udladninger og spændingsvariationer [218].

4.6. **Materialer**

ADA_025 Adapteren skal opfylde beskyttelsesgraden (*fastsættes af fabrikanten, afhængig af hvor den installeres*) [220, 221].

ADA_026 Adapterhusets farve skal være gul.

4.7. **Påskrifter**

ADA_027 En typeplade med følgende oplysninger anbringes på adapteren:

— adapterfabrikantens navn og adresse

— fabrikantens reservedelsnummer og adapterens fremstillingsår

— godkendelsesmærke for adaptertypen eller for kontrolapparattypen, som omfatter adapteren

— datoen, hvor adapteren er installeret

▼B

— identifikationsnummer på det køretøj, hvori den er installeret.

ADA_028 Typepladen skal desuden indeholde følgende oplysninger (hvis disse ikke kan aflæses direkte på ydersiden af den indlejrede bevægelsesføler):

— navn på fabrikanten af den indlejrede bevægelsesføler

— fabrikantens reservedelsnummer og den indlejrede bevægelsesfølers fremstillingsår

— godkendelsesmærke for den indlejrede bevægelsesføler.

5. INSTALLERING AF KONTROLAPPARATET, NÅR EN ADAPTER BENYTTES

5.1. **Installering**

ADA_029 Adaptere, der skal installeres i køretøjer, må kun installeres af køretøjsfabrikanten eller af godkendte værksteder, der har tilladelse til at installere, aktivere og kalibrere digitale takografer og intelligente takografer.

ADA_030 Et sådant godkendt værksted, der installerer adapteren, justerer indgangssignaltilkoblingen og vælger omsætningsforhold til indgangssignalet (hvis dette er relevant).

ADA_031 Et sådant godkendt værksted, der installerer adapteren, plomberer adapterhuset.

ADA_032 Adapteren installeres så tæt som muligt på den del af køretøjet, der frembringer indkommende impulser til denne.

ADA_033 Kablerne, som forsyner adapteren med strøm, skal være henholdsvis rød (positiv forsyning) og sort (stel).

5.2. **Plombering**

ADA_034 Følgende plomberingskrav finder anvendelse:

— Adapterhuset plomberes (se ADA_017).

— Den indlejrede bevægelsesfølers hus plomberes fast til adapterhuset, medmindre det ikke er muligt at fjerne føleren fra adapterhuset uden at bryde adapterhusets plombe(r) (se ADA_018).

— Adapterhuset plomberes fast på køretøjet.

— Forbindelsen mellem adapteren og det udstyr, der frembringer impulserne til denne, plomberes i begge ender (i det omfang, dette med rimelighed kan lade sig gøre).

6. KONTROL, EFTERSYN OG REPARATIONER

6.1. **Periodiske eftersyn**

ADA_035 Når der benyttes adapter, skal hvert periodiske eftersyn (periodiske eftersyn skal forstås i overensstemmelse med krav [409] til krav [413] i bilag 1C) af kontrolapparatet omfatte kontrol af følgende:

— at adapteren er forsynet med den relevante typegodkendelsesmærkning

— at plomberne på adapteren og dennes forbindelser er ubeskadigede

▼B

— at adapteren er installeret som angivet på installationspladen

— at adapteren er installeret som specificeret af adapter- og/eller køretøjsfabrikanten

— at det er tilladt at montere en adapter på det inspicerede køretøj.

ADA_036 Disse eftersyn omfatter en kalibrering og udskiftning af alle plomberinger uanset deres stand.

7. TYPEGODKENDELSE AF KONTROLAPPARATET, NÅR EN ADAPTER BENYTTES

7.1. **Almindelige bestemmelser**

ADA_037 Ved forelæggelse til typegodkendelse skal kontrolapparatet være komplet med adapter [425].

ADA_038 Enhver adapter kan forelægges med henblik på en selvstændig typegodkendelse eller til typegodkendelse som en komponent i et kontrolapparat.

ADA_039 En sådan typegodkendelse skal omfatte funktionsprøver med adapteren. Positive resultater for hver af disse prøver angives ved en passende attest [426].

7.2. **Funktionsattest**

ADA_040 Der udstedes først en funktionsattest for en adapter eller et kontrolapparat med en adapter til adapterfabrikanten, efter at alle de følgende minimumsfunktionsprøver er afsluttet med et tilfredsstillende resultat.

Nr.	Test	Beskrivelse	Tilknyttede krav
1.	**Administrativ undersøgelse**		
1.1	Dokumentation	Adapterdokumentationens korrekthed	
2.	**Besigtigelse**		
2.1.	Overensstemmelse med dokumentationen		
2.2.	Identifikation/mærkning af adapteren		ADA_027, ADA_028
2.3	Adapterens materialer		[219] til [223] ADA_026
2.4.	Plombering		ADA_017, ADA_018, ADA_034
3.	**Funktionsprøver**		
3.1	Tilførsel af hastighedsimpulser til den indlejrede bevægelsesføler		ADA_013

▼B

Nr.	Test	Beskrivelse	Tilknyttede krav
3.2	Tilkobling og tilpasning af de indkommende hastighedsimpulser		ADA_011, ADA_012
3.3	Nøjagtighed af målingen af bevægelsen		[30] til [35], [217]
4.	**Miljøprøver**		
4.1	Fabrikantens prøvningsresultater	Resultater af fabrikantens prøvninger	ADA_020, ADA_021, ADA_022, ADA_024
5.	**Elektromagnetisk kompatibilitet**		
5.1	Strålingsemission og følsomhed	Overensstemmelse med direktiv 2006/28/EF verificeres	ADA_024
5.2	Fabrikantens prøvningsresultater	Resultater af fabrikantens prøvninger	ADA_024

▼C1

BILAG II

GODKENDELSESMÆRKE OG TYPEGODKENDELSESDOKUMENT

I. GODKENDELSESMÆRKE

1. Godkendelsesmærket består af:

a) et rektangel, i hvilket er anbragt bogstavet »e« efterfulgt af kodetallet eller kendingsbogstavet for det land, som har meddelt typegodkendelsen i overensstemmelse med følgende oversigt:

Belgien	6,
Bulgarien	34,
Den Tjekkiske Republik	8,
Danmark	18,
Tyskland	1,
Estland	29,
Irland	24,
Grækenland	23,
Spanien	9,
Frankrig	2,
Kroatien	25,
Italien	3,
Cypern	CY,
Letland	32,
Litauen	36,
Luxembourg	13,
Ungarn	7,
Malta	MT,
Nederlandene	4,
Østrig	12,
Polen	20,
Portugal	21,
Rumænien	19,
Slovenien	26,
Slovakiet	27,
Finland	17,
Sverige	5,
Det Forenede Kongerige	11,

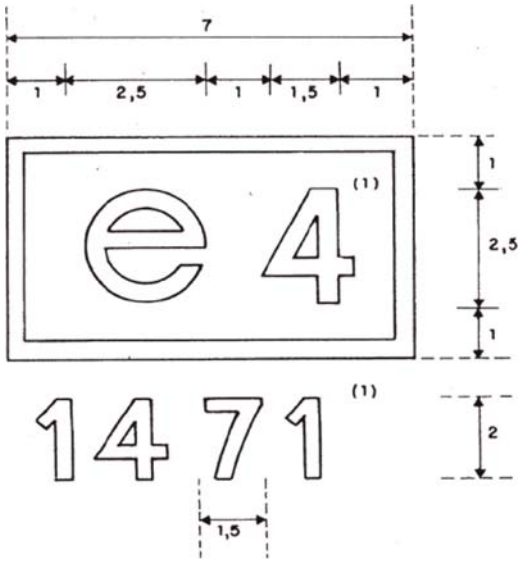
og

b) et typegodkendelsesnummer, som svarer til nummeret i det typegodkendelsesdokument, der er udstedt for modellen af kontrolapparatet eller diagramarket eller for et takografkorts nummer, og som anbringes et sted i nærheden af rektanglet.

▼C1

2. Godkendelsesmærket anbringes på hvert apparats typeplade, på hvert diagramark og på hvert takografkort. Mærket må ikke kunne udslettes og skal til enhver tid være letlæseligt.

3. De nedenfor angivne mål ([1]) for godkendelsesmærket er udtrykt i millimeter og udgør mindstemålene. Forholdene mellem disse mål skal overholdes.



([1]) Disse tal er kun vejledende.

▼C1

II. TYPEGODKENDELSESDOKUMENT FOR ANALOGE TAKOGRAFER

Den medlemsstat, der har meddelt en typegodkendelse, udsteder en typegodkendelsesattest til ansøgeren efter følgende model. Til underretning af andre medlemsstater om den meddelte typegodkendelse eller om eventuelle tilbagekaldelser skal medlemsstaterne anvende kopier af denne attest.

TYPEGODKENDELSESATTEST

Navnet på den kompetente myndighed .....

Meddelelse vedrørende ([1]):

— typegodkendelse for modellen af et kontrolapparat

— tilbagekaldelse af typegodkendelse for modellen af et kontrolapparat

— godkendelse af modeller af diagramark

— tilbagekaldelse af godkendelse af modeller af diagramark

Godkendelsesnr.:

.....

1. Varemærke eller -navn .....

2. Modellens eller typens betegnelse .....

3. Fabrikantens navn .....

4. Fabrikantens adresse .....

5. Forelagt til godkendelse den .....

6. Afprøvningssted .....

7. Afprøvningsdato og nr. .....

8. Godkendelsesdato .....

9. Dato for tilbagekaldelse af godkendelse .....

10. Modellen af det kontrolapparat (eller de apparater), til hvilket (hvilke) diagramarket benyttes

11. Sted .....

12. Dato .....

13. Bilag (beskrivelser mv.) .....

14. Bemærkninger (herunder eventuelle plombers placering)

(Underskrift)

([1]) Det ikke gældende overstreges.

▼C1

III. TYPEGODKENDELSESDOKUMENT FOR DIGITALE TAKOGRAFER

Den medlemsstat, der har meddelt en typegodkendelse, udsteder en typegodkendelsesattest til ansøgeren efter følgende model. Til underretning af andre medlemsstater om den meddelte typegodkendelse eller om eventuelle tilbagekaldelser skal medlemsstaterne anvende kopier af denne attest.

GODKENDELSESATTEST FOR DIGITALE TAKOGRAFER

Navnet på den kompetente myndighed .....

Meddelelse vedrørende ([1]):

☐ godkendelse af: ☐ tilbagekaldelse af godkendelse af:

☐ kontrolapparatmodel

☐ komponent til kontrolapparat ([2])

☐ et førerkort

☐ et værkstedskort

☐ et virksomhedskort

☐ et kontrolkort

Godkendelsens nr.:

.....

1. Fabrikat eller varemærke .....
2. Modellens betegnelse .....
3. Fabrikantens navn .....
4. Fabrikantens adresse .....
5. Godkendelse ansøgt for .....
6. Laboratorium(er) .....
7. Afprøvningsrapportens dato og nr. .....
8. Godkendelsesdato .....
9. Dato for tilbagekaldelse af godkendelse .....
10. Model af kontrolapparat(er), som komponenten er bestemt til anvendelse sammen med
11. Sted .....
12. Dato .....
13. Bilag (beskrivelser mv.) .....
14. Bemærkninger (herunder eventuelle plombers placering)

(Underskrift)

([1]) Afkryds de relevante felter.
([2]) Angiv, hvilken komponent meddelelsen vedrører.

▼C1

IV. GODKENDELSESATTEST FOR INTELLIGENTE TAKOGRAFER

Den medlemsstat, der har meddelt en typegodkendelse, udsteder en typegodkendelsesattest til ansøgeren efter følgende model. Til underretning af andre medlemsstater om den meddelte typegodkendelse eller om eventuelle tilbagekaldelser skal medlemsstaterne anvende kopier af denne attest.

GODKENDELSESATTEST FOR INTELLIGENTE TAKOGRAFER

Navnet på den kompetente myndighed .....

Meddelelse vedrørende ([1]):

☐ godkendelse af: ☐ tilbagekaldelse af godkendelse af:

☐ kontrolapparatmodel

☐ komponent til kontrolapparat ([2])

☐ et førerkort

☐ et værkstedskort

☐ et virksomhedskort

☐ et kontrolkort

Godkendelsens nr.:

.....

1. Fabrikat eller varemærke .....
2. Modellens betegnelse .....
3. Fabrikantens navn .....
4. Fabrikantens adresse .....
5. Godkendelse ansøgt for .....
6. a) Prøvelaboratorium for funktionsgodkendelse .....
   b) Prøvelaboratorium for sikkerhedsgodkendelse .....
   c) Prøvelaboratorium for interoperabilitetsgodkendelse .....
7. a) Dato og nummer på funktionsattest .....
   b) Dato og nummer på sikkerhedsattest .....
   c) Dato og nummer på interoperabilitetsattest .....
8. Godkendelsesdato .....
9. Dato for tilbagekaldelse af godkendelse .....
10. Model af kontrolapparat(er), som komponenten er bestemt til anvendelse sammen med
11. Sted .....
12. Dato .....
13. Bilag (beskrivelser mv.) .....
14. Bemærkninger (herunder eventuelle plombers placering)

(Underskrift)

([1]) Afkryds de relevante felter.
([2]) Angiv, hvilken komponent meddelelsen vedrører.