

II

(Icke-lagstiftningsakter)

FÖRORDNINGAR

KOMMISSIONENS GENOMFÖRANDEFÖRORDNING (EU) 2018/502

av den 28 februari 2018

om ändring av kommissionens genomförandeförordning (EU) 2016/799 när det gäller krav för konstruktion, provning, installation, drift och reparation av färdskrivare och deras komponenter

(Text av betydelse för EES)

EUROPEISKA KOMMISSIONEN HAR ANTAGIT DENNA FÖRORDNING

med beaktande av fördraget om Europeiska unionens funktionssätt,

med beaktande av Europaparlamentets och rådets förordning (EU) nr 165/2014 av den 4 februari 2014 om färdskrivare vid vägtransporter ⁽¹⁾, särskilt artiklarna 11 och 12.7, och

av följande skäl:

- (1) Genom förordning (EU) nr 165/2014 infördes smarta färdskrivare, dvs. andra generationens digitala färdskrivare, vilket inbegriper en anslutning till en GNSS-anordning (Global Navigation Satellite System), en kommunikationsanordning för fjärravläst tidig upptäckt och ett frivilligt gränssnitt mot intelligenta transportsystem.
- (2) De tekniska kraven för konstruktion, provning, installation, drift och reparation av färdskrivare och deras komponenter fastställs i kommissionens genomförandeförordning (EU) 2016/799 ⁽²⁾.
- (3) I enlighet med artiklarna 8, 9 och 10 i förordning (EU) nr 165/2014 ska färdskrivare som är installerade i fordon som registreras för första gången den 15 juni 2019 eller senare vara smarta färdskrivare. Genomförandeförordning (EU) 2016/799 måste därför ändras så att de tekniska bestämmelser som fastställs i förordningen gäller från och med den dagen.
- (4) För att överensstämma med artikel 8 i förordning (EU) nr 165/2014, där det fastställs att fordonets position måste registreras var tredje timme under den sammanlagda körtiden, bör genomförandeförordning (EU) 2016/799 ändras för att möjliggöra att information om fordonets position lagras med tre timmars intervall med hjälp av en parameter som inte kan återställas och för att undvika förväxling med parametern "sammanhängande körtid" som har en annan funktion.
- (5) Fordonsenheten kan utgöras av en enda enhet, eller av flera enheter på olika platser i fordonet. Anordningarna för GNSS och DSRC (*Dedicated Short Range Communication*) kan därför vara interna eller externa i förhållande till fordonsenhetens huvudkomponent. När de är externa bör det vara möjligt att typgodkänna de båda anordningarna och fordonsenhetens huvudkomponent som separata komponenter för att anpassa förfarandet för typgodkännande av färdskrivare till marknadens behov.
- (6) Reglerna om lagring av händelser i form av tidskonflikter och tidsinställningar måste ändras för att åtskilja mellan å ena sidan de automatiska tidsinställningar som utlöses efter eventuella försök till manipulering eller funktionsfel i färdskrivaren och å andra sidan de tidsinställningar som har andra orsaker, t.ex. underhåll.
- (7) Dataidentifierarna bör kunna åtskilja data som laddas ned från en smart färdskrivare från data som laddas ned från en färdskrivare av en tidigare generation.

⁽¹⁾ EUT L 60, 28.2.2014, s. 1.⁽²⁾ Kommissionens genomförandeförordning (EU) 2016/799 av den 18 mars 2016 om genomförande av Europaparlamentets och rådets förordning (EU) nr 165/2014 när det gäller krav för konstruktion, provning, installation, drift och reparation av färdskrivare och deras komponenter (EUT L 139, 26.5.2016, s. 1).

- (8) Giltighetstiden för ett företagskort bör förlängas från två till fem år för att anpassas till förarkortets giltighetstid.
- (9) Beskrivningen av vissa fel och händelser, valideringen av angivelser av platser där arbetsperioder påbörjas och/eller avslutas, användningen av förarens samtycke avseende ITS-gränssnitt (*Intelligent Transport System*) när det gäller data som överförs av fordonsenheten genom fordonets datanät och andra tekniska frågor bör förtydligas.
- (10) För att säkerställa att certifieringen av färdskrivares plomberingar är aktuell behöver de ändras i enlighet med den nya standarden om säkerhet i fråga om mekaniska plomberingar som används för färdskrivare.
- (11) Denna förordning rör konstruktion, provning, installation och drift av system som även omfattar radioutrustning som regleras i Europaparlamentets och rådets direktiv 2014/53/EU ⁽¹⁾. I det direktivet regleras utsläppande på marknaden och ibruktagande av alla slag av elektronisk och elektrisk utrustning som utnyttjar radiovågor för kommunikation och/eller radiobestämning, särskilt i fråga om elsäkerhet, kompatibilitet med andra system, tillgång till radiospektrum, tillgång till larmtjänster och/eller ytterligare andra delegerade bestämmelser. För att garantera en effektiv användning av radiospektrum, förhindra skadlig radiointerferens, säkerställa radioutrustningens säkerhet och elektromagnetiska kompatibilitet och ge möjlighet till eventuella andra specifika delegerade krav bör denna förordning inte påverka tillämpningen av direktivet.
- (12) Genomförandeförordning (EU) 2016/799 bör därför ändras i enlighet med detta.
- (13) De åtgärder som föreskrivs i denna förordning är förenliga med yttrandet från den kommitté som avses i artikel 42.3 i förordning (EU) nr 165/2014.

HÄRIGENOM FÖRESKRIVS FÖLJANDE.

Artikel 1

Genomförandeförordning (EU) 2016/799 ska ändras på följande sätt:

1. Artikel 1 ska ändras på följande sätt:

a) Punkterna 2 och 3 ska ersättas med följande:

"2. Konstruktion, provning, installation, besiktning, drift och reparation av smarta färdskrivare och deras komponenter ska uppfylla de tekniska krav som fastställs i bilaga IC till denna förordning.

3. Andra färdskrivare än smarta färdskrivare ska fortsättningsvis, i fråga om konstruktion, provning, installation, besiktning, drift och reparation, uppfylla kraven i antingen bilaga I till förordning (EU) nr 165/2014 eller bilaga IB till rådets förordning (EEG) nr 3821/85 (*), enligt vad som är tillämpligt.

(*) Rådets förordning (EEG) nr 3821/85 av den 20 december 1985 om färdskrivare vid vägtransporter (EGT L 370, 31.12.1985, s. 8)."

b) Följande punkt ska läggas till som punkt 5:

"5. Denna förordning påverkar inte tillämpningen av Europaparlamentets och rådets direktiv 2014/53/EU (*).

(*) Europaparlamentets och rådets direktiv 2014/53/EU av den 16 april 2014 om harmonisering av medlemsstaternas lagstiftning om tillhandahållande på marknaden av radioutrustning och om upphävande av direktiv 1999/5/EG (EUT L 153, 22.5.2014, s. 62.)"

2. Artikel 2 ska ändras på följande sätt:

a) Definition 3 ska ersättas med följande:

"3. *informationsmapp*: en fullständig dokumentation, i elektronisk form eller på papper, med all information som lämnas av tillverkaren eller dennes företrädare till den typgodkännande myndigheten för typgodkännande av en färdskrivare eller en ingående komponent, inklusive de intyg som avses i artikel 12.3 i förordning (EU) nr 165/2014, resultaten av de prov som anges i bilaga IC till denna förordning, samt ritningar, fotografier och andra relevanta dokument."

⁽¹⁾ Europaparlamentets och rådets direktiv 2014/53/EU av den 16 april 2014 om harmonisering av medlemsstaternas lagstiftning om tillhandahållande på marknaden av radioutrustning och om upphävande av direktiv 1999/5/EG (EUT L 153, 22.5.2014, s. 62).

b) Definition 7 ska ersättas med följande:

"7. *smart färdskrivare* eller *andra generationens färdskrivare*: en digital färdskrivare som överensstämmer med artiklarna 8, 9 och 10 i förordning (EU) nr 165/2014 samt med bilaga IC till den här förordningen."

c) Definition 8 ska ersättas med följande:

"8. *färdskrivarkomponent*: någon av följande delar: fordonsenhet, rörelsesensor, diagramblad, extern GNSS-anordning eller anordning för fjärravläst tidig upptäckt."

d) Följande definition ska läggas till som definition 10:

"10. *fordonsenhet*: färdskrivaren förutom rörelsesensorn och anslutningskablar till rörelsesensorn.

Den kan bestå av en enda enhet eller av flera enheter på olika platser i fordonet och inbegriper en databehandlingsenhet, ett dataminne, en funktion för tidmätning, två kortläsare för smartkort (förare och medförare), en skrivare, en bildskärm, anslutningar och anordningar för indata från användaren, en GNSS-mottagare och en kommunikationsanordning för fjärravläsning.

Fordonsenheten kan bestå av följande komponenter som är föremål för typgodkännande:

- Fordonsenhet, som en enda komponent (inklusive GNSS-mottagare och kommunikationsanordning för fjärravläsning).
- Huvudkomponent för fordonsenheten (inklusive kommunikationsanordning för fjärravläsning) och extern GNSS-anordning.
- Huvudkomponent för fordonsenheten (inklusive GNSS-mottagare) och extern kommunikationsanordning för fjärravläsning.
- Huvudkomponent för fordonsenheten, extern GNSS-anordning och extern kommunikationsanordning för fjärravläsning.

Om fordonsenheten består av flera enheter på olika platser i fordonet är fordonsenhetens huvudkomponent den enhet som innehåller databehandlingsenheten, dataminnet och funktionen för tidmätning.

Termen 'fordonsenhet' (eller VU, *Vehicle Unit*) används för både fordonsenheten som helhet och fordonsenhetens huvudkomponent."

3. I artikel 6 ska punkt 3 ersättas med följande:

"Bilaga IC ska dock tillämpas från och med den 15 juni 2019, med undantag för tillägg 16 som ska tillämpas från och med den 2 mars 2016."

4. Bilaga IC ska ändras i enlighet med bilaga I till denna förordning.

5. Bilaga II ska ändras i enlighet med bilaga II till denna förordning.

Artikel 2

Ikraftträdande

Denna förordning träder i kraft den tjugonde dagen efter det att den har offentliggjorts i *Europeiska unionens officiella tidning*.

Denna förordning är till alla delar bindande och direkt tillämplig i alla medlemsstater.

Utfärdad i Bryssel den 28 februari 2018.

På kommissionens vägnar

Jean-Claude JUNCKER

Ordförande

BILAGA I

Bilaga IC till förordning (EU) 2016/799 ska ändras på följande sätt:

(1) Innehållsförteckningen ska ändras på följande sätt:

(a) Punkt 3.12.5 ska ersättas med följande:

”3.12.5. Platser och positioner där dagens arbetsperioder påbörjas eller avslutas och/eller där tre timmars sammanlagd körtid uppnås”.

(b) Punkt 4.5.3.2.16 ska ersättas med följande:

”4.5.3.2.16 Data om platser avseende tre timmars sammanlagd körning”.

(c) Punkt 4.5.4.2.14 ska ersättas med följande:

”4.5.4.2.14 Data om platser avseende tre timmars sammanlagd körning”.

(d) Punkt 6.2 ska ersättas med följande:

”6.2 Kontroll av nya eller reparerade komponenter”.

(2) Punkt 1 ska ändras på följande sätt:

(a) Definition ll ska ersättas med följande:

”ll) *kommunikationsanordning för fjärravläsning eller anordning för fjärravläst tidig upptäckt*:

den utrustning i fordonsenheten som används för att utföra riktade vägkontroller.”

(b) Definition tt ska ersättas med följande:

”tt) tidsinställning:

en justering av aktuell tidpunkt som kan ske automatiskt med regelbundna intervall, med den tidsangivelse som ges av GNSS-mottagaren som referens, eller utförs i kalibreringsläge.”

(c) Den första strecksatsen i definition yy ska ersättas med följande:

”— endast installeras och används i fordon av typerna M1 och N1 (enligt definitionen i bilaga II till Europaparlamentets och rådets direktiv 2007/46/EG (*), i sin senaste lydelse),”

(d) En ny definition ska läggas till som definition fff:

”fff) sammanlagd körtid:

ett värde som står för det totala antalet sammanlagda minuter av körtid för ett visst fordon.

Värdet för den sammanlagda körtiden räknas upp löpande, baserat på alla minuter som räknas som körning (DRIVING) av färdskrivarens funktion som övervakar förarens aktiviteter, och det används endast för att utlösa registrering av fordonets position varje gång en multipel av tre timmars sammanlagd körtid uppnås. Räkningen startas när färdskrivaren aktiveras. Den påverkas inte av någon annan omständighet, t.ex. ’omfattas ej’ (OUT OF SCOPE) eller ’transport med färja/tåg’ (FERRY/TRAIN CROSSING).

Den sammanlagda körtiden är inte avsedd att visas, skrivas ut eller överföras.”

(3) I punkt 2.3.13 ska sista strecksatsen ersättas med följande:

— ”Fordonsenheterna har en normal drifts- och giltighetstid på 15 år, räknat från första giltighetsdagen för fordonsenhetens certifikat. Fordonsenheter kan användas i ytterligare tre månader, men endast för överföring av data.”

(4) I punkt 2.4 ska första stycket ersättas med följande:

”Systemsäkerheten är avsedd att skydda dataminnet så att obehörig tillgång till och manipulation av data förhindras, och att upptäcka sådana försök, att skydda integriteten och autenticiteten hos data som utväxlas mellan rörelse-sensorn och fordonsenheten, att skydda integriteten och autenticiteten hos data som utväxlas mellan färdskrivaren och färdskrivarkorten, att skydda integriteten och autenticiteten hos data som utväxlas mellan fordonsenheten och den externa GNSS-anordningen, om en sådan finns, att skydda sekretessen, integriteten och autenticiteten hos data som i kontrollsyfte utväxlas via fjärrkommunikation för tidig upptäckt, och att kontrollera integriteten och autenticiteten hos data som överförs.”

(5) I punkt 3.2.27 ska andra strecksatsen ersättas med följande:

— ”Positioner där den sammanlagda körtiden uppnår en multipel av tre timmar.”

(6) Punkt 3.4.49 ska ersättas med följande:

”49) Den första aktivitetsändring till rast/vila (BREAK/REST) eller tillgänglighet (AVAILABILITY) som sker inom 120 sekunder efter den automatiska omkopplingen till annat arbete (WORK) på grund av att fordonet stannar ska antas ha skett när fordonet stannar (och därmed sker eventuellt inte omkopplingen till annat arbete (WORK)).”

(7) Punkt 3.6.1.59 ska ersättas med följande:

”59) Föraren ska då ange fordonets aktuella plats, som ska betraktas som en tillfällig angivelse.

Under följande omständigheter valideras den tillfälliga angivelse som gjordes när kortet senast togs ut (dvs. den ska inte längre skrivas över):

— Angivelse av en plats där den innevarande arbetsperioden påbörjas, vid manuell angivelse i enlighet med krav 61.

— Nästa angivelse av en plats där den innevarande arbetsperioden påbörjas, om kortinnehavaren inte anger någon plats där arbetsperioden påbörjas eller avslutas vid den manuella angivelsen i enlighet med krav 61.

Under följande omständigheter ersätts den tillfälliga angivelse som gjordes när kortet senast togs ut av ett nytt värde som också valideras:

— Nästa angivelse av en plats där den innevarande arbetsperioden avslutas, om kortinnehavaren inte anger någon plats där arbetsperioden påbörjas eller avslutas vid den manuella angivelsen i enlighet med krav 61.”

(8) I punkt 3.6.2 ska sjätte och sjunde strecksatserna ersättas med följande:

— ”den plats där en föregående arbetsperiod avslutades, kopplad till den relevanta tidpunkten (vilket innebär att det som angavs när kortet senast togs ut skrivs över och valideras),

— den plats där den innevarande arbetsperioden påbörjades, kopplad till den relevanta tidpunkten (vilket innebär att det som tillfälligt angavs när kortet senast togs ut valideras).”

(9) Punkt 3.9.15 ska ersättas med följande:

”3.9.15 Tidskonflikt (händelse, 'Time conflict')

86) Denna händelse ska utlösas **när kalibreringsläget inte är inställt** om fordonsenheten upptäcker en avvikelse på mer än en (1) minut mellan tiden i fordonsenhetens tidmättningsfunktion och den tid som har sitt ursprung i GNSS-mottagaren. Denna händelse registreras tillsammans med fordonsenhetens interna klockvärde och åtföljs av en automatisk tidsinställning. Efter det att en händelse av typen tidskonflikt har utlösts kommer fordonsenheten inte att generera några andra händelser av samma typ under de följande 12 timmarna. Denna händelse ska inte utlösas om GNSS-mottagaren inte känt av någon giltig GNSS-signal under minst 30 dagar.”

(10) I punkt 3.9.17 ska följande strecksats läggas till:

”— Fel i ITS-gränssnitt (i förekommande fall).”

(11) Punkt 3.10 ska ändras på följande sätt:

(i) Gäller inte den svenska språkversionen.

(ii) Följande rad ska läggas till i tabellen:

”ITS-gränssnitt (frivilligt)	Korrekt drift”	
------------------------------	----------------	--

(12) Den andra strecksatsen i punkt 3.12 ska ersättas med följande:

”— Genomsnittligt antal positioner per dag: Minst sex positioner där en arbetsperiod påbörjas, sex positioner där den sammanlagda körtiden uppnår en multipel av tre timmar och sex positioner där en arbetsperiod avslutas, vilket innebär att '365 dagar' inbegriper minst 6570 positioner.”.

(13) Punkt 3.12.5 ska ändras på följande sätt:

(a) Rubriken och punkt 108 ska ersättas med följande:

”3.12.5 Platser och positioner där dagens arbetsperioder påbörjas eller avslutas och/eller där tre timmars sammanlagd körtid uppnås

108) Färdskrivaren ska registrera och lagra följande i sitt dataminne:

— Platser och positioner där föraren och/eller medföraren påbörjar dagens arbetsperioder.

— Positioner där den sammanlagda körtiden uppnår en multipel av tre timmar.

— Platser och positioner där föraren och/eller medföraren avslutar dagens arbetsperioder.”

(b) Den fjärde strecksatsen i punkt 110 ska ersättas med följande:

”— Typ av angivelse (början, slut eller tre timmars sammanlagd körtid).”

(c) Punkt 111 ska ersättas med följande:

"111) Det ska gå att lagra data om platser och positioner där dagens arbetsperioder påbörjas eller avslutas, och/eller där tre timmars sammanlagd körtid uppnås, i dataminnet i minst 365 dagar."

(14) Punkt 3.12.7.116 ska ersättas med följande:

"116) Färdskrivaren ska i sitt dataminne registrera och lagra fordonets momentana hastighet och motsvarande datum och tidpunkt vid varje sekund under åtminstone de senaste 24 timmar som fordonet varit i rörelse."

(15) Tabellen i punkt 3.12.8 ska ändras på följande sätt:

(a) Följande rad ska föras in mellan raderna "Positionsinformation från GNSS-mottagare saknas" och "Fel i rörelsedata":

"Fel i kommunikation med extern GNSS-anordning (<i>Communication error with the external GNSS facility</i>)"	— Den långvarigaste händelsen för vart och ett av de senaste tio dygn där händelsen inträffat — De fem långvarigaste händelserna under de senaste 365 dyggen	— Datum och tidpunkt för händelsens början — Datum och tidpunkt för händelsens slut — Korttyp, kortnummer, utfärdande medlemsstat och generation för ett eventuellt kort som var insatt vid händelsens början och/eller slut — Antal liknande händelser samma dag"
--	---	---

(b) Raden "Tidskonflikt" ska ersättas med följande:

"Tidskonflikt (<i>Time conflict</i>)"	— Den mest allvarliga händelsen för vart och ett av de senaste tio dygn där händelsen inträffat (dvs. de som uppvisar den största skillnaden mellan datum och tidpunkt enligt färdskrivaren och datum och tidpunkt enligt GNSS). — De fem mest allvarliga händelserna under de senaste 365 dyggen	— Datum och tidpunkt enligt färdskrivaren — Datum och tidpunkt enligt GNSS — Korttyp, kortnummer, utfärdande medlemsstat och generation för ett eventuellt kort som var insatt vid händelsens början och/eller slut — Antal liknande händelser samma dag"
---	--	--

(16) Punkt 3.20.200 ska ersättas med följande:

"200) Färdskrivaren får även vara utrustad med standardiserade gränssnitt som möjliggör att data som registrerats eller genererats av färdskrivaren kan användas av en extern anordning i drift- eller kalibreringsläge.

I tillägg 13 specificeras och standardiseras ett frivilligt ITS-gränssnitt. Fordonsenheten får också ha andra gränssnitt, förutsatt att de helt uppfyller kraven i tillägg 13 när det gäller förteckning över minsta uppsättning av data, säkerhet och förarens samtycke.

Förarens samtycke gäller inte data som överförs av färdskrivaren till fordonets datanät. Om personuppgifter som matats in i fordonets datanät behandlas vidare utanför fordonets datanät ansvarar fordonstillverkaren för att processen för denna behandling av personuppgifter överensstämmer med förordning (EU) 2016/679 (den allmänna dataskyddsförordningen).

Förarens samtycke gäller inte heller färdskrivardata som överförs till ett externt företag (krav 193), eftersom detta scenario övervakas via företagskortets tillträdesrättigheter.

Följande krav gäller för ITS-data som görs tillgängliga via detta gränssnitt:

- Dessa data är utvalda bland befintliga data från färdskrivarens datakatalog (tillägg 1).
- En delmängd av dessa utvalda data är markerade som 'personuppgifter'.
- Delmängden med personuppgifter är endast tillgänglig om förarens kontrollerbara samtycke är aktiverat, vilket innebär att förarens personuppgifter kan lämna fordonets interna datanät.
- Förarens samtycke kan när som helst aktiveras eller avaktiveras via menykommandon, förutsatt att förarkortet är insatt.
- Dessa data, inklusive delmängden med personuppgifter, sänds ut i alla riktningar från hytten via Bluetooth-protokoll för trådlös kommunikation och uppdateras en gång per minut.
- Parningen av den externa anordningen med ITS-gränssnittet skyddas med en dedikerad och slumpmässig PIN-kod på minst fyra siffror som registreras i varje fordonsenhet och är tillgänglig via dess bildskärm.
- Förekomsten av ett ITS-gränssnitt får under inga omständigheter störa eller påverka fordonsenhetens korrekta funktion och säkerhet.

Även andra data, utöver de utvalda befintliga som betraktas som en minsta uppsättning av data, får ingå i utdata, förutsatt att de inte kan betraktas som personuppgifter.

Färdskrivaren ska kunna kommunicera status för förarens samtycke till andra plattformar i fordonets datanät.

När fordonets tändning är påslagen (ON) ska dessa data kontinuerligt sändas ut i alla riktningar."

(17) Punkt 3.23.211 ska ersättas med följande:

"211) Tidsinställningen av fordonsenhetens interna klocka ska ske automatiskt med tolv timmars intervall. Om denna tidsinställning inte är möjlig eftersom ingen GNSS-signal är tillgänglig ska tidsinställningen göras så snart som fordonsenheten har tillgång till en giltig tidsreferens från GNSS-mottagaren, i enlighet med villkoren avseende fordonets tändning. Tidsreferensen för den automatiska tidsinställningen av fordonsenhetens interna klocka ska genereras från GNSS-mottagaren."

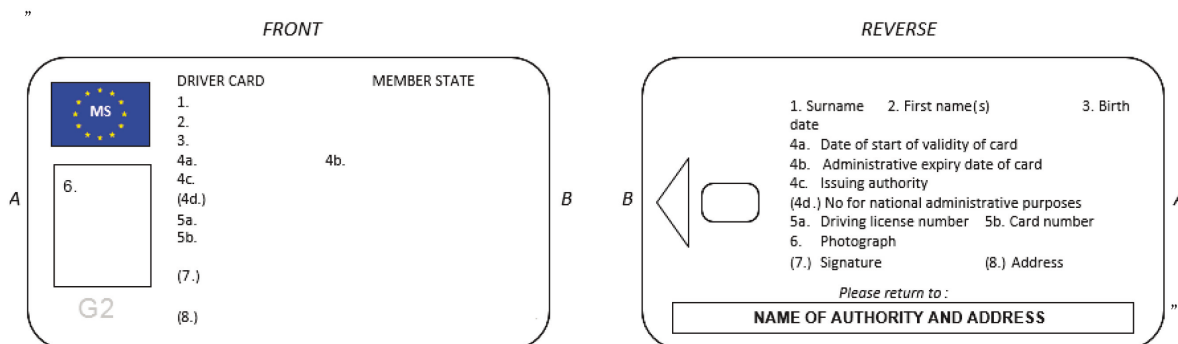
(18) Punkt 3.26.225 och 226 ska ersättas med följande:

"225) En typskylt ska fästas på varje enskild komponent i färdskrivaren och den ska visa följande:

- Tillverkarens namn och adress.
- Tillverkarens artikelnummer och tillverkningsår.
- Serienummer.
- Typgodkännandemärke.

226) Om det fysiska utrymmet inte är tillräckligt för att visa alla uppgifter som nämns ovan ska typskylten åtminstone visa tillverkarens namn eller logotyp och artikelnumret.”

(19) I punkt 4.1 ska bilden som visar förarkortets framsida och baksida ersättas med följande:



(20) Gäller inte den svenska språkversionen.

(21) Gäller inte den svenska språkversionen.

(22) Punkt 4.5.3.2.16 ska ersättas med följande:

”4.5.3.2.16 Data om platser avseende tre timmars sammanlagd körning

305) Det ska gå att lagra följande data på förarkortet om fordonets position när den sammanlagda körtiden uppnår en multipel av tre timmar:

- Datum och tidpunkt när den sammanlagda körtiden uppnår en multipel av tre timmar.
- Fordonets position.
- GNSS-precision, datum och tidpunkt när positionen fastställdes.
- Fordonets vägmätarställning.

306) Det ska gå att lagra minst 252 sådana poster på förarkortet.”

(23) Punkt 4.5.4.2.14 ska ersättas med följande:

”4.5.4.2.14 Data om platser avseende tre timmars sammanlagd körning

353) Det ska gå att lagra följande data på verkstadskortet om fordonets position när den sammanlagda körtiden uppnår en multipel av tre timmar:

- Datum och tidpunkt när den sammanlagda körtiden uppnår en multipel av tre timmar.

- Fordonets position.
- GNSS-precision, datum och tidpunkt när positionen fastställdes.
- Fordonets vägmätarställning.

354) Det ska gå att lagra minst 18 sådana poster på verkstadskortet.”.

(24) Punkt 5.2.396 ska ersättas med följande:

”396) På skylten ska åtminstone följande uppgifter finnas:

- Godkänd montörs eller verkstads namn och adress eller handelsbeteckning.
- Fordonets karakteristiska koefficient, uttryckt som ' $w = \dots \text{ imp/km}$ '.
- Färdskrivarkonstanten, uttryckt som ' $k = \dots \text{ imp/km}$ '.
- Däckens effektiva omkrets, uttryckt som ' $l = \dots \text{ mm}$ '.
- Däcksdimension.
- Datum för mätning av fordonets karakteristiska koefficient och däckens effektiva omkrets.
- Fordonets identifieringsnummer.
- Förekomst (eller inte) av en extern GNSS-anordning.
- Den externa GNSS-anordningens serienummer, i förekommande fall.
- Serienummer för kommunikationsanordningen för fjärravläsning, i förekommande fall.
- Serienummer för samtliga befintliga plomberingar.
- Den del av fordonet där adaptern, i förekommande fall, är installerad.
- Den del av fordonet där rörelsesensorn är installerad om den inte är ansluten till växellådan eller en adapter inte används.
- Beskrivning av färgen på kabeln mellan adaptern och den del av fordonet som tillhandahåller adapterns inkommande impulser.
- Serienumret på adapterns inbyggda rörelsesensor.”

(25) Punkt 5.3 ska ändras på följande sätt:

(a) Efter punkt 398 ska en ny punkt införas som punkt 398a:

”398a) De plomberingar som nämns ovan ska certifieras i enlighet med standarden SS-EN 16882:2016.”

(b) I punkt 401 ska andra stycket ersättas med följande:

"Det unika identifieringsnumret definieras som MMNNNNNNNN och ska vara outplånligt, där MM är en unik identifiering av tillverkaren (som är registrerad i en databas som förvaltas av EU-kommissionen) och NNNNNNNN är plomberingens alfanumeriska nummer som är unikt inom tillverkarens domän."

(c) Punkt 403 ska ersättas med följande:

"403) Tillverkare av plomberingar ska registreras i en särskild databas när de får en modell av plombering certifierad i enlighet med SS-EN 16882:2016, och de ska offentliggöra sina plomberingsnummer genom ett förfarande som ska fastställas av Europeiska kommissionen."

(d) Punkt 404 ska ersättas med följande:

"404) Godkända verkstäder och fordonstillverkare ska, inom ramen för förordning (EU) nr 165/2014, endast använda plomberingar som är certifierade i enlighet med SS-EN 16882:2016 och som kommer från de tillverkare av plomberingar som ingår i den ovan nämnda databasen."

(26) Punkt 6.2 ska ersättas med följande:

"6.2. Kontroll av nya eller reparerade komponenter

407) Varje enskild anordning, oavsett om den är ny eller reparerad, ska genom kalibrering kontrolleras med avseende på att den fungerar riktigt och att dess avlästa och registrerade värden ligger inom de i avsnitten 3.2.1, 3.2.2, 3.2.3 och 3.3 fastställda gränserna."

(27) Punkt 6.3.408 ska ersättas med följande:

"408) När hela utrustningen (inbegripet färdskrivaren) monteras i ett fordon ska den överensstämma med bestämmelserna om största tillåtna toleranser i avsnitten 3.2.1, 3.2.2, 3.2.3 och 3.3. Hela utrustningen ska plomberas i enlighet med avsnitt 5.3, och även kalibreras."

(28) Punkt 8.1 ska ändras på följande sätt:

(a) I punkt 8.1 ska inledningen före punkt 425 ersättas med följande:

"I detta kapitel avses med termen 'färdskrivare' 'färdskrivare eller dess komponenter'. Inget typgodkännande krävs för kablarna mellan rörelsesensorn och fordonsenheten, mellan den externa GNSS-anordningen och fordonsenheten eller mellan den externa kommunikationsanordningen för fjärravläsning och fordonsenheten. Det papper som används i färdskrivaren ska anses vara en av färdskrivarens komponenter.

Alla tillverkare får ansöka om typgodkännande av färdskrivarkomponenter tillsammans med alla andra färdskrivarkomponenter, under förutsättning att varje komponent uppfyller kraven i denna bilaga. Som ett alternativ får tillverkare även ansöka om typgodkännande av färdskrivare.

Enligt vad som beskrivs i definitionen i artikel 2.10 i denna förordning kan det finnas varianter av fordonsenheter med olika sammansättningar av komponenter. Oavsett fordonsenhetens sammansättning av komponenter omfattas den externa antennen och (i förekommande fall) den antennsplitter som är ansluten till GNSS-mottagaren eller till kommunikationsanordningen för fjärravläsning inte av fordonsenhetens typgodkännande.

Icke desto mindre ska tillverkare som erhållit typgodkännande för färdskrivare upprätthålla en allmänt tillgänglig förteckning över kompatibla antenner och splitter för varje typ av godkänd fordonsenhet, extern GNSS-anordning och extern kommunikationsanordning för fjärravläsning.”

(b) Punkt 427 ska ersättas med följande:

”427) Medlemsstaternas myndigheter för typgodkännande får inte bevilja något intyg om typgodkännande så länge de inte innehar

— ett säkerhetsintyg (om så krävs enligt denna bilaga),

— ett funktionsintyg, och

— ett intyg om driftskompatibilitet (om så krävs enligt denna bilaga)

för den färdskrivare eller det färdskrivarkort som är föremål för ansökan om typgodkännande.”

(29) Tillägg 1 ska ändras på följande sätt:

(a) Innehållsförteckningen ska ändras på följande sätt:

(i) Punkt 2.63 ska ersättas med följande:

”2.63 Reserverat för framtida användning (RFU, Reserved for future use)”.

(ii) Punkt 2.78 ska ersättas med följande:

”2.78 GNSSAccumulatedDriving”.

(iii) Punkt 2.79 ska ersättas med följande:

”2.79 GNSSAccumulatedDrivingRecord”.

(iv) Punkt 2.111 ska ersättas med följande:

”2.111 NoOfGNSSADRecords”.

(v) Punkt 2.160 ska ersättas med följande:

”2.160 Reserverat för framtida användning (RFU, Reserved for future use)”.

(vi) Punkt 2.203 ska ersättas med följande:

”2.203 VuGNSSADRecord”.

(vii) Punkt 2.204 ska ersättas med följande:

”2.204 VuGNSSADRecordArray”.

(viii) Punkt 2.230 ska ersättas med följande:

”2.230 Reserverat för framtida användning (RFU, Reserved for future use)”.

(ix) Punkt 2.231 ska ersättas med följande:

”2.231 Reserverat för framtida användning (RFU, Reserved for future use)”.

- (b) I punkt 2 ska följande text läggas till före punkt 2.1:

”För datatyper som används för tillämpningar i generation 1 och generation 2 är den storlek som anges i detta tillägg den som gäller tillämpningar i generation 2. Läsaren antas redan känna till storleken för tillämpningar i generation 1. De numrerade krav i bilaga IC som rör sådana datatyper omfattar tillämpningar i både generation 1 och generation 2.”

- (c) Punkt 2.19 ska ersättas med följande:

2.19 CardEventData

Generation 1:

Information lagrad i ett förarkort eller verkstadskort om händelser som förknippas med kortinnehavaren (krav 260 och 318 i bilaga IC).

```
CardEventData ::= SEQUENCE SIZE(6) OF {
    cardEventRecords          SET SIZE(NoOfEventsPerType) OF
                                CardEventRecord
}
```

CardEventData är en sekvens, som är ordnad efter stigande värde på EventFaultType, av cardEventRecords (utom poster rörande försök till säkerhetsöverträdelse, som samlas i slutet av sekvensen).

cardEventRecords är en mängd händelseposter av en viss händelsetyp (eller kategori för händelser av typen försök till säkerhetsöverträdelse).

Generation 2:

Information lagrad i ett förarkort eller verkstadskort om händelser som förknippas med kortinnehavaren (krav 285 och 341 i bilaga IC).

```
CardEventData ::= SEQUENCE SIZE(11) OF {
    cardEventRecords          SET SIZE(NoOfEventsPerType) OF
                                CardEventRecord
}
```

CardEventData är en sekvens, som är ordnad efter stigande värde på EventFaultType, av cardEventRecords (utom poster rörande försök till säkerhetsöverträdelse, som samlas i slutet av sekvensen).

cardEventRecords är en mängd händelseposter av en viss händelsetyp (eller kategori för händelser av typen försök till säkerhetsöverträdelse)."

- (d) Punkt 2.30 ska ersättas med följande:

2.30 CardRenewalIndex

Ett korts förnyelseindex (definition i)).

```
CardRenewalIndex ::= IA5String(SIZE(1))
```

Värdetilldelning (se kapitel 7 i denna bilaga)

'0' Första utfärdande.

Ökningsföljd: '0, ..., 9, A, ..., Z'.

- (e) I punkt 2.61 ska texten efter rubriken "Generation 2" ersättas med följande:

```
"DriverCardApplicationIdentification ::= SEQUENCE {
  typeOfTachographCardId      EquipmentType,
  cardStructureVersion         CardStructureVersion,
  noOfEventsPerType            NoOfEventsPerType,
  noOfFaultsPerType            NoOfFaultsPerType,
  activityStructureLength      CardActivityLengthRange,
  noOfCardVehicleRecords      NoOfCardVehicleRecords,
  noOfCardPlaceRecords        NoOfCardPlaceRecords,
  noOfGNSSADRecords           NoOfGNSSADRecords,
  noOfSpecificConditionRecords NoOfSpecificConditionRecords,
  noOfCardVehicleUnitRecords  NoOfCardVehicleUnitRecords
}
```

Jämfört med generation 1 används följande ytterligare dataelement:

noOfGNSSADRecords är det antal GNSS-poster om sammanlagd körning som kortet kan lagra.

noOfSpecificConditionRecords är det antal poster för särskilda omständigheter som kortet kan lagra.

noOfCardVehicleUnitRecords är det antal poster om använda fordonsenheter som kortet kan lagra..

- (f) Punkt 2.63 ska ersättas med följande:

"2.63 **Reserverat för framtida användning** (RFU, *Reserved for future use*)".

- (g) I punkt 2.67 ska texten efter rubriken "Generation 2" ersättas med följande:

"Samma värden används som för generation 1, med följande tillägg:

```
--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
--Driver Card (Sign) (17), --only to be used in the CHA
field of a signing certificate
--Workshop Card (Sign) (18), --only to be used in the CHA
field of a signing certificate
--Vehicle Unit (Sign) (19), --only to be used in the CHA
field of a signing certificate
--RFU (20..255)
```

Anmärkning 1: Värdena för skylt, adapter och extern GNSS-anslutning i generation 2, liksom värdena för fordonsenhet och rörelsesensor i generation 1, får användas i SealRecord, dvs. om detta är tillämpligt.

Anmärkning 2: I fältet CardHolderAuthorisation (CHA) i ett certifikat för generation 2 ska värdena (1), (2) och (6) tolkas som att de anger ett certifikat för ömsesidig autentisering för respektive typ av utrustning. För att ange respektive certifikat för att skapa en digital signatur måste värdet (17), (18) eller (19) användas."

(h) I punkt 2.70 ska texten efter rubriken "Generation 2" ersättas med följande:

"Generation 2:

'0x'H	Allmänna händelser.
'00'H	Inga närmare detaljer.
'01'H	Insättning av ogiltigt kort.
'02'H	Kortkonflikt.
'03'H	Tidsöverlappning.
'04'H	Körning utan korrekt kort.
'05'H	Insättning av kort under körning.
'06'H	Senaste kortsession ej korrekt avslutad.
'07'H	Hastighetsöverträdelse.
'08'H	Avbrott i strömtillförseln.
'09'H	Fel i rörelsedata.
'0A'H	Konflikt i fordonets rörelsedata.
'0B'H	Tidskonflikt (GNSS jämfört med fordonsenhetens interna klocka).
'0C'H	Fel i kommunikation med kommunikationsanordning för fjärravläsning.
'0D'H	Positionsinformation från GNSS-mottagare saknas.
'0E'H	Fel i kommunikation med extern GNSS-anordning.
'0F'H	RFU.
'1x'H	Händelser som gäller försök till säkerhetsöverträdelse med avseende på fordonsenhet.
'10'H	Inga närmare detaljer.
'11'H	Fel vid autentisering av rörelsesensor.
'12'H	Fel vid autentisering av färdskrivarkort.
'13'H	Icke auktoriserad ändring av rörelsesensor.
'14'H	Integritetsfel hos inmatade kortdata.
'15'H	Integritetsfel hos lagrade användardata.
'16'H	Internt fel vid överföring av data.
'17'H	Ej auktoriserad öppning av höljet.
'18'H	Maskinvarusabotage.
'19'H	GNSS-manipulering upptäckt.
'1A'H	Fel vid autentisering av extern GNSS-anordning.
'1B'H	Certifikat för extern GNSS-anordning har löpt ut.
'1C'H to '1F'H	RFU.
'2x'H	Händelser som gäller försök till säkerhetsöverträdelse med avseende på sensor.
'20'H	Inga närmare detaljer.
'21'H	Misslyckad autentisering.
'22'H	Integritetsfel hos lagrade data.
'23'H	Internt fel vid överföring av data.
'24'H	Ej auktoriserad öppning av höljet.
'25'H	Maskinvarusabotage.
'26'H to '2F'H	RFU.
'3x'H	Färdskrivarfel.
'30'H	Inga närmare detaljer.
'31'H	Internt fel i fordonsenheten.
'32'H	Skrivarfel.
'33'H	Bildskärmsfel.
'34'H	Överföringsfel.
'35'H	Sensorfel.
'36'H	Intern GNSS-mottagare.
'37'H	Extern GNSS-anordning.
'38'H	Kommunikationsanordning för fjärravläsning.
'39'H	ITS-gränssnitt.
'3A'H to '3F'H	RFU.
'4x'H	Kortfel.
'40'H	Inga närmare detaljer.
'41'H to '4F'H	RFU.
'50'H to '7F'H	RFU.
'80'H to 'FF'H	Tillverkarspecifikt.

- (i) Punkt 2.71 ska ersättas med följande:

2.71 ExtendedSealIdentifier

Generation 2:

En unik identifierare för en plombering (krav 401 i bilaga IC).

```
ExtendedSealIdentifier ::= SEQUENCE{
    manufacturerCode      OCTET STRING (SIZE(2)),
    sealIdentifier         OCTET STRING (SIZE(8))
}
```

manufacturerCode är en kod för tillverkaren av plomberingen.

sealIdentifier är en identifierare för plomberingen som är unik bland tillverkarens plomberingar”.

- (j) Punkterna 2.78 och 2.79 ska ersättas med följande:

2.78 GNSSAccumulatedDriving

Generation 2:

Information lagrad på ett förarkort eller verkstadskort om fordonets GNSS-position om den sammanlagda körtiden uppnår en multipel av tre timmar (krav 306 och 354 i bilaga IC).

```
GNSSAccumulatedDriving := SEQUENCE {
    gnssADPointerNewestRecord    INTEGER(0..NoOfGNSSADRecords -1),
    gnssAccumulatedDrivingRecords SET SIZE(NoOfGNSSADRecords) OF
                                   GNSSAccumulatedDrivingRecord
}
```

gnssADPointerNewestRecord är index för senast uppdaterade GNSS-post om sammanlagd körning.

Värdetilldelning är det tal som motsvarar numeratören för GNSS-posten om sammanlagd körning, och som börjar med '0' för den första GNSS-posten om sammanlagd körning som förekommer i strukturen.

gnssAccumulatedDrivingRecords är den mängd poster som innehåller datum och tidpunkt när den sammanlagda körningen uppnår en multipel av tre timmar, samt information om fordonets position.

2.79 GNSSAccumulatedDrivingRecord

Generation 2:

Information lagrad på ett förarkort eller verkstadskort om fordonets GNSS-position om den sammanlagda körtiden uppnår en multipel av tre timmar (krav 305 och 353 i bilaga IC).

```
GNSSAccumulatedDrivingRecord ::= SEQUENCE {
    timeStamp              TimeReal,
    gnssPlaceRecord         GNSSPlaceRecord,
    vehicleOdometerValue    OdometerShort
}
```

timeStamp är datum och tidpunkt när den sammanlagda körtiden uppnår en multipel av tre timmar.

gnssPlaceRecord innehåller information om fordonets position.

vehicleOdometerValue är vägmätarställningen när den sammanlagda körtiden uppnår en multipel av tre timmar.”

- (k) Punkt 2.86 ska ersättas med följande:

"2.86 KeyIdentifier

En unik identifierare för en öppen nyckel som används för att referera till och välja nyckeln. Den identifierar även nyckelinnehavaren.

```
KeyIdentifier ::= CHOICE {
    extendedSerialNumber      ExtendedSerialNumber,
    certificateRequestID       CertificateRequestID,
    certificationAuthorityKID  CertificationAuthorityKID
}
```

Det första alternativet (CHOICE) är lämpligt för att referera till en fordonsenhets, ett färdskrivarkorts eller en extern GNSS-anordnings öppna nyckel.

Det andra alternativet är lämpligt för att referera till en fordonsenhets öppna nyckel (i de fall fordonsenhets serienummer inte är känt vid tidpunkten för generering av certifikat).

Det tredje alternativet är lämpligt för att referera till en medlemsstats öppna nyckel."

- (l) Punkt 2.92 ska ersättas med följande:

"2.92 MAC

Generation 2:

En kryptografisk kontrollsumma med en längd av 8, 12 eller 16 byte, motsvarande de chifferföljder som anges i tillägg 11.

```
MAC ::= CHOICE {
    Mac8          OCTET STRING (SIZE(8)),
    Mac12         OCTET STRING (SIZE(12)),
    Mac16         OCTET STRING (SIZE(16)),
};
```

- (m) Punkt 2.111 ska ersättas med följande:

"2.111 NoOfGNSSADRecords

Generation 2:

Det antal poster om sammanlagd körning enligt GNSS som ett kort kan lagra.

```
NoOfGNSSADRecords ::= INTEGER (0..216-1)
```

Värdetilldelning: Se tillägg 2".

- (n) I punkt 2.120 ska värdetilldelningen "16H" ersättas med följande:

```
"'16'H VuGNSSADRecord";
```

- (o) Punkt 2.160 ska ersättas med följande:

"2.160 Reserverat för framtida användning (RFU, *Reserved for future use*)".

- (p) Punkt 2.162 ska ersättas med följande:

"2.162 TimeReal

Kod för ett kombinerat datum- och tidsfält, där datum och tid uttrycks som sekunder efter 00h.00m.00s. den 1 januari 1970 UTC.

TimeReal { INTEGER:TimeRealRange } ::= INTEGER (0..TimeRealRange)

Värdetilldelning – oktetgrupperad: Antal sekunder sedan midnatt den 1 januari 1970 UTC.

Senaste möjliga datum/tidpunkt är under år 2106."

- (q) Punkt 2.179 ska ersättas med följande:

"2.179 VuCardRecord

Generation 2:

Information lagrad i en fordonsenhet om ett färdskrivarkort som används (krav 132 i bilaga IC).

```
VuCardRecord ::= SEQUENCE {  
  cardNumberAndGenerationInformation      FullCardNumberAndGeneration,  
  cardExtendedSerialNumber                ExtendedSerialNumber,  
  cardStructureVersion                    CardStructureVersion,  
  cardNumber                              CardNumber  
}
```

cardNumberAndGenerationInformation är det fullständiga kortnumret och generationen för det kort som används (datatyp 2.74).

cardExtendedSerialNumber såsom det läses från filen EF_ICC under kortets huvudfil (MF).

cardStructureVersion såsom det läses från filen EF_Application_Identification under DF_Tachograph_G2.

cardNumber såsom det läses från filen EF_Identification under DF_Tachograph_G2."

- (r) Punkterna 2.203 och 2.204 ska ersättas med följande:

"2.203 VuGNSSADRecord

Generation 2:

Information lagrad i en fordonsenhet om fordonets GNSS-position om den sammanlagda körtiden uppnår en multipel av tre timmar (krav 108 och 110 i bilaga IC).

```
VuGNSSADRecord ::= SEQUENCE {  
  timeStamp                        TimeReal,  
  cardNumberAndGenDriverSlot      FullCardNumberAndGeneration,  
  cardNumberAndGenCodriverSlot   FullCardNumberAndGeneration,  
  gnssPlaceRecord                 GNSSPlaceRecord,  
  vehicleOdometerValue            OdometerShort  
}
```

timeStamp är datum och tidpunkt när den sammanlagda körtiden uppnår en multipel av tre timmar.

cardNumberAndGenDriverSlot identifierar det kort, inbegripet dess generation, som är insatt i förarens kortplats.

cardNumberAndGenCodriverSlot identifierar det kort, inbegripet dess generation, som är insatt i medförarens kortplats.

gnssPlaceRecord innehåller information om fordonets position.

vehicleOdometerValue är vägmätarställningen när den sammanlagda körtiden uppnår en multipel av tre timmar.

2.204 **VuGNSSADRecordArray**

Generation 2:

Information lagrad i en fordonsenhet om fordonets GNSS-position om den sammanlagda körtiden uppnår en multipel av tre timmar (krav 108 och 110 i bilaga IC).

```
VuGNSSADRecordArray ::= SEQUENCE {
    recordType          RecordType,
    recordSize          INTEGER(1..65535),
    noOfRecords         INTEGER(0..65535),
    records             SET SIZE(noOfRecords) OF VuGNSSADRecord
}
```

recordType anger typen av post (VuGNSSADRecord).

Värdetilldelning: Se RecordType.

recordSize är storleken av VuGNSSADRecord i byte.

noOfRecords är antalet poster i postmängden.

records är en mängd poster om sammanlagd körning enligt GNSS."

- (s) Punkterna 2.230 och 2.231 ska ersättas med följande:

2.230 Reserverat för framtida användning (RFU, *Reserved for future use*)

2.231 Reserverat för framtida användning (RFU, *Reserved for future use*)".

- (t) I punkt 2.234 ska texten efter rubriken "Generation 2" ersättas med följande:

```
"WorkshopCardApplicationIdentification ::= SEQUENCE {
    typeOfTachographCardId      EquipmentType,
    cardStructureVersion         CardStructureVersion,
    noOfEventsPerType            NoOfEventsPerType,
    noOfFaultsPerType            NoOfFaultsPerType,
    activityStructureLength       CardActivityLengthRange,
    noOfCardVehicleRecords       NoOfCardVehicleRecords,
    noOfCardPlaceRecords         NoOfCardPlaceRecords,
    noOfCalibrationRecords       NoOfCalibrationRecords,
    noOfGNSSADRecords            NoOfGNSSADRecords,
    noOfSpecificConditionRecords NoOfSpecificConditionRecords,
    noOfCardVehicleUnitRecords   NoOfCardVehicleUnitRecords
}
```

Jämfört med generation 1 används följande ytterligare dataelement:

noOfGNSSADRecords är det antal GNSS-poster om sammanlagd körning som kortet kan lagra.

noOfSpecificConditionRecords är det antal poster för särskilda omständigheter som kortet kan lagra.

noOfCardVehicleUnitRecords är det antal poster om använda fordonsenheter som kortet kan lagra.”

(30) Tillägg 2 ska ändras på följande sätt:

(a) I artikel 1.1 ska följande förkortningar läggas till:

”CHA *Certificate Holder Authorisation* (certifikatinnehavarens auktorisering)

DO *Data Object* (dataobjekt)”.

(b) Punkt 3.3 ska ändras på följande sätt:

(i) TCS_24 ska ersättas med följande:

”TCS_24 Dessa säkerhetsvillkor kan förenas på följande sätt:

AND: Alla säkerhetsvillkor måste vara uppfyllda

OR: Minst ett säkerhetsvillkor måste vara uppfyllt

Tillträdesreglerna för filsystemet, dvs. för kommandona SELECT, READ BINARY och UPDATE BINARY, specificeras i kapitel 4. Tillträdesreglerna för övriga kommandon specificeras i nedanstående tabeller. ’Ej tillämpligt’ anger att det inte finns något krav på stöd för kommandot. I så fall kanske det finns stöd för kommandot, men tillträdesvillkoret är inte relevant.”

(ii) I TCS_25 ska tabellen ersättas med följande:

”Kommando	Förarkort	Verkstadskort	Kontrollkort	Företagskort
EXTERNAL AUTHENTICATION				
— För autentisering (generation 1)	ALW	ALW	ALW	ALW
— För autentisering (generation 2)	ALW	PWD	ALW	ALW
INTERNAL AUTHENTICATION	ALW	PWD	ALW	ALW
GENERAL AUTHENTICATION	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	Ej tillämpligt	Ej tillämpligt	Ej tillämpligt	Ej tillämpligt
PSO: COMPUTE DIGITAL SIGNATURE	ALW OR SM-MAC-G2	ALW OR SM-MAC-G2	Ej tillämpligt	Ej tillämpligt
PSO: HASH	Ej tillämpligt	Ej tillämpligt	ALW	Ej tillämpligt

Kommando	Förarkort	Verkstadskort	Kontrollkort	Företagskort
PERFORM HASH OF FILE	ALW OR SM-MAC-G2	ALW OR SM-MAC-G2	Ej tillämpligt	Ej tillämpligt
PSO: VERIFY CERTIFICATE	ALW	ALW	ALW	ALW
PSO: VERIFY DIGITAL SIGNATURE	Ej tillämpligt	Ej tillämpligt	ALW	Ej tillämpligt
Verify	Ej tillämpligt	ALW	Ej tillämpligt	Ej tillämpligt"

(iii) I TCS_26 ska tabellen ersättas med följande:

"Kommando	Förarkort	Verkstadskort	Kontrollkort	Företagskort
EXTERNAL AUTHENTICATE				
— För autentisering (generation 1)	Ej tillämpligt	Ej tillämpligt	Ej tillämpligt	Ej tillämpligt
— För autentisering (generation 2)	ALW	PWD	ALW	ALW
INTERNAL AUTHENTICATE	Ej tillämpligt	Ej tillämpligt	Ej tillämpligt	Ej tillämpligt
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	Ej tillämpligt	ALW	ALW	Ej tillämpligt
PSO: COMPUTE DIGITAL SIGNATURE	ALW OR SM-MAC-G2	ALW OR SM-MAC-G2	Ej tillämpligt	Ej tillämpligt
PSO: HASH	Ej tillämpligt	Ej tillämpligt	ALW	Ej tillämpligt
PERFORM HASH OF FILE	ALW OR SM-MAC-G2	ALW OR SM-MAC-G2	Ej tillämpligt	Ej tillämpligt
PSO: VERIFY CERTIFICATE	ALW	ALW	ALW	ALW
PSO: VERIFY DIGITAL SIGNATURE	Ej tillämpligt	Ej tillämpligt	ALW	Ej tillämpligt
Verify	Ej tillämpligt	ALW	Ej tillämpligt	Ej tillämpligt"

(iv) I TCS_27 ska tabellen ersättas med följande:

"Kommando	Förarkort	Verkstadskort	Kontrollkort	Företagskort
EXTERNAL AUTHENTICATE				
— För autentisering (generation 1)	Ej tillämpligt	Ej tillämpligt	Ej tillämpligt	Ej tillämpligt
— För autentisering (generation 2)	ALW	PWD	ALW	ALW
INTERNAL AUTHENTICATE	Ej tillämpligt	Ej tillämpligt	Ej tillämpligt	Ej tillämpligt
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	Ej tillämpligt	Ej tillämpligt	Ej tillämpligt	Ej tillämpligt
PSO: COMPUTE DIGITAL SIGNATURE	Ej tillämpligt	Ej tillämpligt	Ej tillämpligt	Ej tillämpligt
PSO: HASH	Ej tillämpligt	Ej tillämpligt	Ej tillämpligt	Ej tillämpligt
PERFORM HASH OF FILE	Ej tillämpligt	Ej tillämpligt	Ej tillämpligt	Ej tillämpligt
PSO: VERIFY CERTIFICATE	ALW	ALW	ALW	ALW
PSO: VERIFY DIGITAL SIGNATURE	Ej tillämpligt	Ej tillämpligt	Ej tillämpligt	Ej tillämpligt
Verify	Ej tillämpligt	ALW	Ej tillämpligt	Ej tillämpligt"

(c) I punkt 3.4 ska TCS_29 ersättas med följande:

"TCS_29 Statusregistret SW1 SW2 återsänds i alla svarsmeddelanden och anger bearbetningsstatus för kommandot.

SW1	SW2	Betydelse
90	00	Normal bearbetning.
61	XX	Normal bearbetning. XX = antal byte för svar som finns tillgängliga.
62	81	Varningsbearbetning. En del av återsända data kan vara skadade.
63	00	Autentisering misslyckades (varning).
63	CX	Felaktig CHV (PIN). Räknare av återstående försök tillhandahålls genom 'X'.

SW1	SW2	Betydelse
64	00	Exekveringsfel – Tillståndet hos det permanenta minnet oförändrat. Integritetsfel.
65	00	Exekveringsfel – Tillståndet hos det permanenta minnet förändrat.
65	81	Exekveringsfel – Tillståndet hos det permanenta minnet förändrat. Minnesfel.
66	88	Säkerhetsfel: felaktig kryptografisk kontrollsumma (vid säker meddelandehantering) eller felaktigt certifikat (vid verifiering av certifikat) eller felaktigt kryptogram (vid extern autentisering) eller felaktig signatur (vid verifiering av signatur).
67	00	Felaktig längd (felaktigt Lc eller Le).
68	83	Sista kommandot i kedjan förväntas.
69	00	Förbjudet kommando (inget svar tillgängligt i T = 0).
69	82	Säkerhetsstatus ej uppnådd.
69	83	Blockerad autentiseringsmetod.
69	85	Användningsvillkor ej uppfyllda.
69	86	Kommandot ej tillåtet (ingen aktuell elementfil).
69	87	Förväntade dataobjekt för säker meddelandehantering saknas.
69	88	Inkorrekta dataobjekt för säker meddelandehantering.
6A	80	Felaktiga parametrar i datafält.
6A	82	Filen ej funnen.
6A	86	Felaktiga parametrar P1-P2.
6A	88	Referensdata ej funna.
6B	00	Felaktiga parametrar (offset utanför elementfilen).
6C	XX	Felaktig längd, SW2 anger exakt längd. Inget datafält återsänds.
6D	00	Instruktionskoden stöds ej eller är ogiltig.
6E	00	Klassen stöds ej.
6F	00	— Övriga kontrollfel.

Ytterligare statusregister enligt vad som definieras i ISO/IEC 7816-4 kan återsändas, om deras funktion inte uttryckligen omnämns i detta tillägg.

Exempelvis kan följande statusregister alternativt återsändas:

6881: Logikkanal stöds inte.

6882: Säker meddelandehantering stöds inte.”

(d) I punkt 3.5.1.1 ska sista strecksatsen i TCS_38 ersättas med följande:

”— Om den valda tillämpningen anses vara skadad (integritetsfel upptäcks i filattributen), återsänds bearbetningsstatus **'6400'** eller **'6500'**.”

(e) I punkt 3.5.1.2 ska sista strecksatsen i TCS_41 ersättas med följande:

”— Om den valda filen anses vara skadad (integritetsfel upptäcks i filattributen), återsänds bearbetningsstatus **'6400'** eller **'6500'**.”

(f) I punkt 3.5.2.1 ska sjätte strecksatsen i TCS_43 ersättas med följande:

”— Om ett integritetsfel upptäcks i filattributen, ska kortet anse filen vara skadad och omöjlig att återställa, och återsända bearbetningsstatus **'6400'** eller **'6500'**.”

(g) Punkt 3.5.2.1.1 ska ändras på följande sätt:

(i) I TCS_45 ska tabellen ersättas med följande:

"Byte	Längd	Värde	Beskrivning
#1	1	'81h'	T _{PV} : Tagg för data med klarvärde
#2	L	'NNh' eller '81 NNh'	L _{PV} : Längd på återsända data (= ursprunglig Le). L är 2 byte om L _{PV} > 127 byte.
#(2+L) - #(1+L+NN)	NN	'XX..XXh'	Data med klarvärde
#(2+L+NN)	1	'99h'	Tagg för bearbetningsstatus (SW1-SW2) – frivillig uppgift för säker meddelandehantering (generation 1)
#(3+L+NN)	1	'02h'	Längd för bearbetningsstatus – frivillig uppgift för säker meddelandehantering (generation 1)
#(4+L+NN) - #(5+L+NN)	2	'XX XXh'	Bearbetningsstatus för APDU för oskyddat svar – frivillig uppgift för säker meddelandehantering (generation 1)
#(6+L+NN)	1	'8Eh'	T _{CC} : Tagg för kryptografisk kontrollsumma
#(7+L+NN)	1	'XXh'	L _{CC} : Längd på efterföljande kryptografiska kontrollsumma: '04h' för säker meddelandehantering (generation 1) (se del A i tillägg 11) '08h', '0Ch' eller '10h' beroende på AES-nyckelns längd för säker meddelandehantering (generation 2) (se del B i tillägg 11)

Byte	Längd	Värde	Beskrivning
#(8+L+NN)-#(7+M+L+NN)	M	'XX..XXh'	Kryptografisk kontrollsumma
SW	2	'XXXXh'	Statusregister (SW1,SW2)"

(ii) I TCS_46 ska tabellen ersättas med följande:

"Byte	Längd	Värde	Beskrivning
#1	1	'87h'	T _{PI CG} : Tagg för krypterade data (kryptogram)
#2	L	'MMh' eller '81 MMh'	L _{PI CG} : Längd på återsända krypterade data (inte samma som ursprunglig Le för kommandot på grund av utfyllnad). L är 2 byte om L _{PI CG} > 127 byte.
#(2+L)-#(1+L+MM)	MM	'01XX..XXh'	Krypterade data: Utfyllnadsindikator och kryptogram
#(2+L+MM)	1	'99h'	Tagg för bearbetningsstatus (SW1-SW2) – frivillig uppgift för säker meddelandehantering (generation 1)
#(3+L+MM)	1	'02h'	Längd för bearbetningsstatus – frivillig uppgift för säker meddelandehantering (generation 1)
#(4+L+MM) - #(5+L+MM)	2	'XX XXh'	Bearbetningsstatus för APDU för oskyddat svar – frivillig uppgift för säker meddelandehantering (generation 1)
#(6+L+MM)	1	'8Eh'	T _{CC} : Tagg för kryptografisk kontrollsumma
#(7+L+MM)	1	'XXh'	L _{CC} : Längd på efterföljande kryptografiska kontrollsumma: '04h' för säker meddelandehantering (generation 1) (se del A i tillägg 11) '08h', '0Ch' eller '10h' beroende på AES-nyckelns längd för säker meddelandehantering (generation 2) (se del B i tillägg 11)
#(8+L+MM)- #(7+N+L+MM)	N	'XX..XXh'	Kryptografisk kontrollsumma
SW	2	'XXXXh'	Statusregister (SW1,SW2)"

(h) I punkt 3.5.2.2 ska sjätte strecksatsen i TCS_50 ersättas med följande:

— Om ett integritetsfel upptäcks i filattributen, ska kortet anse filen vara skadad och omöjlig att återställa, och återsända bearbetningsstatus '**6400**' eller '**6500**'."

(i) I punkt 3.5.2.3 ska TCS_52 ändras på följande sätt:

(i) Sista raden i tabellen ska ersättas med följande:

"Le	1	'XXh'	Enligt ISO/IEC 7816-4"
-----	---	-------	------------------------

(ii) Följande meningar ska läggas till:

"Om $T = 0$ antar kortet att $Le = '00h'$, om ingen säker meddelandehantering tillämpas.

Om $T = 1$ återsänds bearbetningsstatus '**6700**' om $Le = '01h'$."

(j) I punkt 3.5.2.3 ska sjätte strecksatsen i TCS_53 ersättas med följande:

"— Om ett integritetsfel upptäcks i filattributen, ska kortet anse filen vara skadad och omöjlig att återställa, och återsända bearbetningsstatus '**6400**' eller '**6500**'."

(k) I punkt 3.5.3.2 ska sjätte strecksatsen i TCS_63 ersättas med följande:

"— Om ett integritetsfel upptäcks i filattributen, ska kortet anse filen vara skadad och omöjlig att återställa, och återsända bearbetningsstatus '**6400**' eller '**6500**'."

(l) Gäller inte den svenska språkversionen.

(m) I punkt 3.5.8 ska TCS_95 ersättas med följande:

"TCS_95 Om kommandot INTERNAL AUTHENTICATE lyckas tas aktuell sessionsnyckel för generation 1 i förekommande fall bort och upphör att vara tillgänglig. För att göra en ny sessionsnyckel för generation 1 tillgänglig måste kommandot EXTERNAL AUTHENTICATE för autentiseringsmekanismen i generation 1 utföras med gott resultat.

Anmärkning: För sessionsnycklar för generation 2, se CSM_193 och CSM_195 i tillägg 11. Om sessionsnycklar för generation 2 är fastställda och färdskrivarkortet tar emot APDU för kommandot INTERNAL AUTHENTICATE i klartext avbryter kortet sessionen med säker meddelandehantering för generation 2 och förstör sessionsnycklarna för generation 2."

(n) I punkt 3.5.9 ska TCS_97 ersättas med följande:

"TCS_97 Kommandovarianten för ömsesidig autentisering mellan fordonsenhet och kort i generation 2 kan utföras på huvudfil (MF) och i DF Tachograph och DF Tachograph_G2 (se även TCS_34). Om kommandot EXTERNAL AUTHENTICATE för generation 2 lyckas tas aktuell sessionsnyckel för generation 1 i förekommande fall bort och upphör att vara tillgänglig.

Anmärkning: För sessionsnycklar för generation 2, se CSM_193 och CSM_195 i tillägg 11. Om sessionsnycklar för generation 2 är fastställda och färdskrivarkortet tar emot APDU för kommandot EXTERNAL AUTHENTICATE i klartext avbryter kortet sessionen med säker meddelandehantering för generation 2 och förstör sessionsnycklarna för generation 2."

- (o) I punkt 3.5.10 ska följande rad läggas till i tabellen i TCS_101:

"5 + L + 1	1	'00h'	Enligt ISO/IEC 7816-4"
------------	---	-------	------------------------

- (p) I punkt 3.5.11.2.3 ska följande stycken läggas till i TCS_114:

"— Om kortets *currentAuthenticatedTime* är senare än sista giltighetsdag för den valda öppna nyckeln återsänds bearbetningsstatus '**6A88**'.

Anmärkning: För ett kommando MSE:SET AT för autentisering av fordonsenhet är den refererade nyckeln en öppen VU_MA-nyckel. Kortet ska ställa in den öppna VU_MA-nyckeln för användning, om den finns tillgänglig i kortets minne, som stämmer överens med den CHR (*Certificate Holder Reference*) som anges i kommandots datafält (kortet kan identifiera öppna VU_MA-nycklar med hjälp av certifikatets CHA-fält). Kortet ska återsända '6A 88' till detta kommando om endast den öppna VU_Sign-nyckeln eller ingen öppen nyckel alls är tillgänglig i fordonsenheten. Se definitionen av CHA-fältet i tillägg 11 och datatypen *equipmentType* i tillägg 1.

På samma sätt gäller att för ett kommando MSE:SET DST som refererar till en EQT (dvs. en fordonsenhet eller ett kort), och som sänds till ett kontrollkort, är den refererade nyckeln enligt CSM_234 alltid en EQT_Sign-nyckel som måste användas för att verifiera en digital signatur. Enligt figur 13 i tillägg 11 kommer kontrollkortet alltid att ha den relevanta öppna EQT_Sign-nyckeln lagrad. I vissa fall kan kontrollkortet ha den motsvarande öppna EQT_MA-nyckeln lagrad. Kontrollkortet ska alltid ställa in den öppna EQT_Sign-nyckeln för användning när kortet tar emot kommandot MSE:SET DST."

- (q) Punkt 3.5.13 ska ändras på följande sätt:

- (i) TCS_121 ska ersättas med följande:

"TCS_121 Det tillfälligt lagrade värdet för hash of file ska raderas om ett nytt värde för hash of file beräknas med hjälp av kommandot PERFORM HASH of FILE om en dedikerad fil (DF) väljs, och om färdskrivarkortet återställs."

- (ii) TCS_123 ska ersättas med följande:

"TCS_123 Färdskrivartillämpningen (generation 2) ska stödja algoritmen SHA-2 (SHA-256, SHA-384 eller SHA-512), angiven genom chifferföljden i del B i tillägg 11, för Card_Sign-nyckeln för kort-signering."

- (iii) Tabellen i TCS_124 ska ersättas med följande:

"Byte	Längd	Värde	Beskrivning
CLA	1	'80h'	CLA
INS	1	'2Ah'	Perform Security Operation
P1	1	'90h'	Tagg: Hash
P2	1	'00h'	Indirekt kända algoritmer: För färdskrivartillämpning (generation 1): SHA-1 För färdskrivartillämpning (generation 2): Algoritmen SHA-2 (SHA-256, SHA-384 eller SHA-512), angiven genom chifferföljden i del B i tillägg 11, för Card_Sign-nyckeln för kortsigntering."

- (r) Punkt 3.5.14 ska ändras på följande sätt:

Texten från rubriken och fram till TCS_126 ska ersättas med följande:

"Detta kommando används för att beräkna den digitala signaturen hos tidigare beräknad hashkod (se PERFORM HASH OF FILE, avsnitt 3.5.13).

Endast förarkortet och verkstadskortet måste stödja detta kommando i DF Tachograph och DF Tachograph_G2.

Andra typer av färdskrivarkort kan ha, men måste inte ha, detta kommando infört. För färdskrivartillämpningar i generation 2 har endast förarkortet och verkstadskortet en signaturnyckel för generation 2, medan andra kort inte kan utföra kommandot med gott resultat, utan avbryter med en lämplig felkod.

Kommandot kan vara, men måste inte vara, åtkomligt i huvudfilen (MF). Om kommandot inte är åtkomligt i huvudfilen ska det avbrytas med en lämplig felkod.

Detta kommando överensstämmer med ISO/IEC 7816-8. Användningen av detta kommando är begränsad med avseende på berörd standard."

- (s) Punkt 3.5.15 ska ändras på följande sätt:

- (i) Tabellen i TCS_133 ska ersättas med följande:

"Byte	Längd	Värde	Beskrivning
CLA	1	'00h'	CLA
INS	1	'2Ah'	Perform Security Operation
P1	1	'00h'	
P2	1	'A8h'	Tagg: datafältet innehåller dataobjekt som är relevanta för verifiering
Lc	1	'XXh'	Längd Lc på efterföljande datafält
#6	1	'9Eh'	Tagg för digital signatur
#7 eller #7-#8	L	'NNh' eller '81 NNh'	Längd på digital signatur (L är 2 byte om den digitala signaturen är längre än 127 byte): 128 byte kodade i enlighet med del A i tillägg 11 för färdskrivartillämpning (generation 1) Beroende på den valda kurvan för färdskrivartillämpning (generation 2) (se del B i tillägg 11)
#(7+L)-#(6+L+NN)	NN	'XX..XXh'	Innehåll i digital signatur"

- (ii) Följande strecksats ska läggas till i TCS_134:

"— Om den valda öppna nyckeln (som används för att verifiera den digitala signaturen) har en CHA.LSB (CertificateHolderAuthorisation.equipmentType) som inte är lämplig för verifieringen av den digitala signaturen enligt tillägg 11 återsänds bearbetningsstatus **'6985'**."

(t) Punkt 3.5.16 ska ändras på följande sätt:

(i) I TCS_138 ska följande rad läggas till i tabellen:

"5 + L + 1	1	'00h'	Enligt ISO/IEC 7816-4"
------------	---	-------	------------------------

(ii) Följande strecksats ska läggas till i TCS_139:

"— '6985' anger att den tidsstämpeln (4 byte) som finns i kommandots datafält är tidigare än *cardValidityBegin* eller senare än *cardExpiryDate*."

(u) Punkt 4.2.2 ska ändras på följande sätt:

(i) I datastrukturen i TCS_154 ska raderna från DF Tachograph G2 till EF CardMA_Certificate, samt raderna från EF GNSS_Places till slutet av TCS_154, ersättas med följande:

"

Fil/dataelement	Antal poster	Storlek (byte)		Standardvärden
		Min	Max	
DF Tachograph_G2		20268	40316	
EF Application_Identification		17	17	
DriverCardApplicationIdentification		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 00}
noOfGNSSADRecords		2	2	{00 00}
noOfSpecificConditionRecords		2	2	{00 00}
noOfCardVehicleUnitRecords		2	2	{00 00}
EF CardMA_Certificate		204	341	

...

EF GNSS_Places		4538	6050	
GNSSContinuousDriving		4538	6050	
gnssADPointerNewestRecord		2	2	{00 00}
gnssAccumulatedDrivingRecords		4536	6048	
GNSSContinuousDrivingRecord	n ₈	18	18	
timeStamp		4	4	{00..00}
gnssPlaceRecord		14	14	
timeStamp		4	4	{00..00}
gnssAccuracy		1	1	{00}
geoCoordinates		6	6	{00..00}
vehicleOdometerValue		3	3	{00..00}

„

(ii) I TCS_155 ska posten NoOfGNSSCDRecords i tabellen ersättas med följande:

"n ₈ "	NoOfGNSSADRecords	252	336"
-------------------	-------------------	-----	------

(v) I punkt 4.3.1 ska den text som beskriver förkortningen SC4 i TCS_156 ersättas med följande:

"**SC4** För kommandot READ BINARY med jämn INS-byte:

(SM-C-MAC-G1 AND SM-R-ENC-MAC-G1) OR

(SM-C-MAC-G2 AND SM-R-ENC-MAC-G2)

För kommandot READ BINARY med udda INS-byte (om detta stöds): NEV".

(w) Punkt 4.3.2 ska ändras på följande sätt:

(i) I datastrukturen i TCS_162 ska raderna från DF Tachograph G2 till EF CardMA_Certificate, raderna från EF Calibration till extendedSealIdentifier och raderna från EF GNSS_Places till vehicleOdometerValue ersättas med följande:

”

Fil/dataelement	Antal poster	Storlek (byte)		Standard-värden
		Min.	Max.	
DF Tachograph_G2	1878	49787		
EF Application_Identification	19	19		
└ WorkshopCardApplicationIdentificatio	19	19		
└ 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 00}
└ noOfCalibrationRecords	2	2		{00 00}
└ noOfGNSSADRecords	2	2		{00 00}
└ noOfSpecificConditionRecords	2	2		{00 00}
└ noOfCardVehicleUnitRecords	2	2		{00 00}
EF CardMA_Certificate	204	341		
...				
EF Calibration	15668	45394		
└ WorkshopCardCalibrationData	15668	45394		
└ calibrationTotalNumber	2	2		{00 00}
└ calibrationPointerNewestRecord	2	2		{00}
└ calibrationRecords	15664	45390		
└ WorkshopCardCalibrationRecord	n ₅	178	178	
└ 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}
└ sensorGNSSSerialNumber	8	8		{00..00}
└ rcmSerialNumber	8	8		{00..00}
└ vuAbility	1	1		{00}
└ sealDataCard	56	56		
└ └ noOfSealRecords	1	1		{00}
└ SealRecords	55	55		
└ └ SealRecord	5	11	11	
└ └ └ equipmentType	1	1		{00}
└ └ └ extendedSealIdentifier	10	10		{00..00}

...

EF	GNSS_Places	326	434	
	└ GNSSContinuousDriving	326	434	
	└┐ gnssADPointerNewestRecord	2	2	{00 00}
	└ gnssAccumulatedDrivingRecords	324	432	
	└┐ GNSSContinuousDrivingRecord	n ₈	18	18
	└┐┐ timeStamp	4	4	{00..00}
	└┐ gnssPlaceRecord	14	14	
	└┐┐ timeStamp	4	4	{00..00}
	└┐┐ gnssAccuracy	1	1	{00}
	└┐┐ geoCoordinates	6	6	{00..00}
	└┐┐ vehicleOdometerValue	3	3	{00..00}

”

(ii) Raden NoOfGNSSCDRecords i tabellen i TCS_163 ska ersättas med följande:

”n ₈ ”	NoOfGNSSADRecords	18	24”
-------------------	-------------------	----	-----

(31) I tillägg 3 ska punkt 2 ändras på följande sätt:

(a) Följande rad ska införas efter raden med piktogrammen ”Startplats för arbetsperiod” och ”Slutplats för arbetsperiod”:

” Position efter tre timmars sammanlagd körtid”.

(b) Det kombinerade piktogrammet ”Tidsinställning (av verkstad)” ska ersättas med följande:

” Tidskonflikt eller tidsinställning (av verkstad)”.

(c) Följande kombinerade piktogram ska läggas till i förteckningen över ”Händelser”:

” Positionsinformation från GNSS-mottagare saknas eller fel i kommunikation med extern GNSS-anordning

” Fel i kommunikation med kommunikationsanordning för fjärravläsning”.

(32) Tillägg 4 ska ändras på följande sätt:

(a) Punkt 2 ska ändras på följande sätt:

(i) Punkt 11.4 ska ersättas med följande:

”11.4 Angivelse av plats där en arbetsperiod påbörjas och/eller avslutas

pi = plats för påbörjande/avslutande, tid, land, region

Longitud för den registrerade positionen

Latitud för den registrerade positionen

Tidsstämpel när positionen fastställdes

Vägmätarvärde

pihh:mm Cou Reg

lon ±DDD°MM.M'

lat ± DD°MM.M'

hh:mm

x xxx xxx km”

(ii) Punkt 11.5 ska ersättas med följande:

"11.5 Positioner efter tre timmars sammanlagd körtid
pi = position efter tre timmars sammanlagd

körtid

Longitud för den registrerade positionen

Latitud för den registrerade positionen

Tidsstämpel när positionen fastställdes

Vägmätarvärde

```
pihh:mm
lon ± DDD°MM.M'
lat ± DD°MM.M '
hh:mm
x xxx xxx km"
```

(b) I punkt 3.1 ska position 11.5 i formatet för dagsutskrift ersättas med följande:

"11.5

Positioner efter tre timmars sammanlagd körtid, i kronologisk ordning"

(c) I punkt 3.2 ska formatet för dagsutskrift ersättas med följande:

"1	Datum och tidpunkt för utskrift av dokumentet
2	Typ av utskrift
3	Identifiering av kortinnehavare (för alla kort som är insatta i fordonsenheten, samt generation)
4	Identifiering av fordonet (från vilket utskrift görs)
5	Identifiering av fordonsenhet (från vilken utskrift görs, samt generation)
6	Senaste kalibrering av denna fordonsenhet
7	Senaste kontroll av denna färdskrivare
9	Gränstecken för föraraktiviteter
10	Gränstecken för förarens kortplats (kortplats 1)
10a	Omständighet av typen "omfattas ej" (OUT OF SCOPE) i början av den här dagen
10.1 /10.2/10.3/ 10.3a/10.4	Aktiviteter i kronologisk ordning (förarens kortplats)
10	Gränstecken för medförarens kortplats (kortplats 2)
10a	Omständighet av typen "omfattas ej" (OUT OF SCOPE) i början av den här dagen
10.1/10.2/10.3/ 10.3a/10.4	Aktiviteter i kronologisk ordning (medförarens kortplats)
11	Gränstecken för dagssammanfattning
11.1	Sammanfattning av perioder utan kort i förarens kortplats
11.4	Angivna platser i kronologisk ordning
11.5	Positioner efter tre timmars sammanlagd körtid, i kronologisk ordning
11.7	Aktivitetssammanfattning
11.2	Sammanfattning av perioder utan kort i medförarens kortplats
11.4	Angivna platser i kronologisk ordning
11.5	Positioner efter tre timmars sammanlagd körtid, i kronologisk ordning

11.8	Aktivitetssammanfattning
11.3	Sammanfattning av aktiviteter för en förare, båda kortplatserna
11.4	Platser som denna förare angivit i kronologisk ordning
11.5	Positioner efter tre timmars sammanlagd körtid, i kronologisk ordning
11.9	Aktivitetssammanfattning för denna förare
13.1	Gränstecken för händelser/fel
13.4	Poster för händelser/fel (de fem senaste händelser eller fel som finns lagrade eller är pågående i fordonsenheten)
22.1	Kontrollplats
22.2	Kontrollantens (kontrolltjänstemannens) namnteckning
22.3	Från tidpunkt (utrymme där en förare utan kort kan ange
22.4	Till tidpunkt vilka perioder som gäller honom/henne själv)
22.5	Förarens namnteckning"

(d) Gäller inte den svenska språkversionen.

"1	Datum och tidpunkt för utskrift av dokumentet
2	Type of printout
3	Card holder identifications (of all cards inserted in the VU)
23	Most recent card inserted in the VU
23.1	Inserted cards (up to 88 records)
12.3	Faults delimiter"

(33) Tillägg 7 ska ändras på följande sätt:

(a) Punkt 1.1 ska ersättas med följande:

"1.1 Tillämpningsområde

Data kan överföras till ett externt lagringsmedium på följande sätt:

- Från en fordonsenhet, av en IDE-enhet (*Intelligent Dedicated Equipment*) som är ansluten till fordonsenheten.
- Från ett färdskrivarkort, av en IDE-enhet utrustad med en kortläsare (IFD, *Interface Device*).
- Från ett färdskrivarkort via en fordonsenhet, av en IDE-enhet ansluten till fordonsenheten.

För att göra det möjligt att verifiera autenticitet och integritet hos överförda data som lagras på ett externt lagringsmedium, överförs data med en signatur i enlighet med tillägg 11 om gemensamma säkerhetsmekanismer. Identifiering av källutrustning (fordonsenhet eller kort) och dess säkerhetsintyg (medlemsstat och utrustning) överförs också. Den som kontrollerar dessa data måste oberoende av andra ha en betrodd europeisk öppen nyckel.

Data som överförs från en fordonsenhet signeras med hjälp av de gemensamma säkerhetsmekanismerna i del B i tillägg 11 (för färdskrivarsystem i generation 2), förutom när förarkontroll utförs med hjälp av ett kontrollkort i generation 1 av en kontrollmyndighet i ett tredjeland, i vilket fall data signeras med hjälp av de gemensamma säkerhetsmekanismerna i del A i tillägg 11 (för färdskrivarsystem i generation 1), enligt vad som krävs i tillägg 15 om migrering, krav MIG_015.

I det här tillägget specificeras därför två typer av dataöverföringar från fordonsenheten:

- Dataöverföring från fordonsenheten enligt generation 2, med datastrukturen för generation 2 och signering med hjälp av de gemensamma säkerhetsmekanismerna i del B i tillägg 11.
- Dataöverföring från fordonsenheten enligt generation 1, med datastrukturen för generation 1 och signering med hjälp av de gemensamma säkerhetsmekanismerna i del A i tillägg 11.

På liknande sätt finns det två typer av dataöverföring från andra generationens förarkort som är insatta i en fordonsenhet, enligt vad som anges i punkterna 3 och 4 i detta tillägg.”.

(b) Punkt 2.2.2 ska ändras på följande sätt:

(i) Tabellen ska ersättas med följande:

”Meddelandestruktur		Max. 4 byte Startdel				Max. 255 byte Data			1 byte Kontrollsumma
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									
Verifiera överföringshastighet (Verify Baud Rate) (steg 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
Positivt svar på verifiering av överföringshastighet (Positive Response Verify Baud Rate)		80	F0	EE	02	C7		01	28
Gå över till annan överföringshastighet (steg 2)		80	EE	F0	03	87		02,03	ED
Request Upload		80	EE	F0	0A	35		00,00,00,00- ,00,FF,FF, FF,FF	99
Positive Response Request Upload		80	F0	EE	03	75		00,FF	D5
Transfer Data Request									
Overview		80	EE	F0	02	36	01 eller 21		97
Activities		80	EE	F0	06	36	02 eller 22	Datum	CS
Events & Faults		80	EE	F0	02	36	03 eller 23		99
Detailed Speed		80	EE	F0	02	36	04 eller 24		9A
Technical Data		80	EE	F0	02	36	05 eller 25		9B
Card download		80	EE	F0	02	36	06	Slot	CS

Meddelandestruktur		Max. 4 byte Startdel				Max. 255 byte Data			1 byte Kontrollsumma
IDE ->	<- VU	FMT	TGT	SRC	LEN	SID	DS_ / TRTP	DATA	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
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
Negativa svar									
Allmänt avvisande (<i>General reject</i>)		80	F0	EE	03	7F	Sid Req	10	CS
Tjänsten stöds ej (<i>Service not supported</i>)		80	F0	EE	03	7F	Sid Req	11	CS
Underfunktion stöds ej (<i>Sub function not supported</i>)		80	F0	EE	03	7F	Sid Req	12	CS
Fel meddelandelängd (<i>Incorrect Message Length</i>)		80	F0	EE	03	7F	Sid Req	13	CS
Fel omständigheter eller sekvensfel för begäran (<i>Conditions not correct or Request sequence error</i>)		80	F0	EE	03	7F	Sid Req	22	CS
Begäran utanför tillåtet intervall (<i>Request out of range</i>)		80	F0	EE	03	7F	Sid Req	31	CS
Överföring ej accepterad (<i>Upload not accepted</i>)		80	F0	EE	03	7F	Sid Req	50	CS
Svar dröjer (<i>Response pending</i>)		80	F0	EE	03	7F	Sid Req	78	CS
Data ej tillgängliga (<i>Data not available</i>)		80	F0	EE	03	7F	Sid Req	FA	CS"

(ii) Följande strecksatser ska läggas till i anmärkningarna efter tabellen:

— TRTP 21–25 används för begäran om dataöverföring från fordonsenhet enligt generation 2, medan TRTP 01–05 används för begäran om dataöverföring från fordonsenhet enligt generation 1, vilken kan accepteras av fordonsenheten endast inom ramen för förarkontroll som utförs med hjälp av ett kontrollkort i generation 1 av en kontrollmyndighet i ett tredjeland.

— TRTP 11–19 och 31–39 är reserverade för tillverkarspecifika begäranden om överföring."

(c) Punkt 2.2.2.9 ska ändras på följande sätt:

(i) DDP_011 ska ersättas med följande:

"DDP_011 IDE-enheten sänder Transfer Data Request för att specificera för fordonsenheten vilken typ av data som ska överföras. En parameter för begäran om överföring (TRTP) på en byte anger överföringstypen.

Det finns sex typer av dataöverföring. För dataöverföring från en fordonsenhet kan två olika TRTP-värden användas för varje överföringstyp:

Typ av dataöverföring	TRTP-värde för generation 1 vid dataöverföring från fordonsenhet	TRTP-värde för generation 2 vid dataöverföring från fordonsenhet
Overview (översikt)	01	21
Activities of a specified date (aktiviteter med avseende på ett särskilt datum).	02	22
Events and faults (händelser och fel)	03	23
Detailed speed (detaljerade hastighetsdata)	04	24
Technical data (tekniska data)	05	25

Typ av dataöverföring	TRTP-värde
Card download (överföring från kort)	06"

(ii) DDP_054 ska ersättas med följande:

"DDP_054 IDE-enheten måste begära översikten (TRTP 01 eller 21) under en överföringssession, eftersom det är det enda sättet att säkerställa att fordonsenhetens certifikat registreras i den överförda filen (och göra det möjligt att verifiera den digitala signaturen).

I det andra fallet (TRTP 02 eller 22) innehåller meddelandet *Transfer Data Request* en angivelse av den kalenderdag (format *TimeReal*) som ska överföras."

(d) I punkt 2.2.2.10 ska DDP_055 ersättas med följande:

"DDP_055 I det första fallet (TREP 01 eller 21) kommer fordonsenheten att sända data som hjälper IDE-användaren att välja vilka ytterligare data som han/hon önskar överföra. Informationen i detta meddelande är följande:

- Säkerhetsintyg.
- Fordonsidentifiering.
- Fordonsenhetens aktuella datum och tid.
- Tidigaste och senaste överföringsbart datum (data i fordonsenhet).
- Indikation av att det finns kort i fordonsenheten.
- Tidigare överföring till ett företag.
- Företagslås.
- Tidigare kontroller."

(e) I punkt 2.2.2.16 ska sista strecksatsen i DDP_018 ersättas med följande:

"— FA Data ej tillgängliga

Dataobjektet i en begäran om dataöverföring finns inte tillgängligt i fordonsenheten (t.ex.: inget kort har satts in, dataöverföring från fordonsenhet enligt generation 1 har begärts när förarkontrollen inte utförs av en kontrollmyndighet i ett tredjeland, ...)."

(f) Punkt 2.2.6.1 ska ändras på följande sätt:

(i) Första stycket i DDP_029 ska ersättas med följande:

"Datafältet i meddelandet *Positive Response Transfer Data – Overview* ska tillhandahålla följande data i följande ordning, med angivande av SID = 76 Hex, TREP = 01 eller 21 Hex och med passande delning och räkning av undermeddelanden:"

(ii) Rubriken "Datastruktur för generation 1" ska ersättas med följande:

"Datastruktur för generation 1 (TREP 01 Hex)".

(iii) Rubriken "Datastruktur för generation 2" ska ersättas med följande:

"Datastruktur för generation 2 (TREP 21 Hex)".

(g) Punkt 2.2.6.2 ska ändras på följande sätt:

(i) Första stycket i DDP_030 ska ersättas med följande:

"Datafältet i meddelandet *Positive Response Transfer Data – Activities* ska tillhandahålla följande data i följande ordning, med angivande av SID = 76 Hex, TREP = 02 eller 22 Hex och med passande delning och räkning av undermeddelanden:"

(ii) Rubriken "Datastruktur för generation 1" ska ersättas med följande:

"Datastruktur för generation 1 (TREP 02 Hex)".

(iii) Rubriken "Datastruktur för generation 2" ska ersättas med följande:

"Datastruktur för generation 2 (TREP 22 Hex)".

(iv) Raden `VuGNSSCDRecordArray` under rubriken "Datastruktur för generation 2 (TREP 22 Hex)" ska ersättas med följande:

`"VuGNSSADRecordArray"`

GNSS-positioner för fordonet om dess sammanlagda körtid uppnår en multipel av tre timmar. Om detta avsnitt är tomt sänds en startpost för uppställningen med `noOfRecords = 0`."

(h) Punkt 2.2.6.3 ska ändras på följande sätt:

(i) Första stycket i DDP_031 ska ersättas med följande:

"Datafältet i meddelandet *Positive Response Transfer Data – Events and Faults* ska tillhandahålla följande data i följande ordning med angivande av SID = 76 Hex, TREP = 03 eller 23 Hex och med passande delning och räkning av undermeddelanden:"

(ii) Rubriken "Datastruktur för generation 1" ska ersättas med följande:

"Datastruktur för generation 1 (TREP 03 Hex)".

(iii) Rubriken "Datastruktur för generation 2" ska ersättas med följande:

"Datastruktur för generation 2 (TREP 23 Hex)".

(iv) Raden `VuTimeAdjustmentGNSSRecordArray` under rubriken "Datastruktur för generation 2 (TREP 23 Hex)" ska tas bort.

(i) Punkt 2.2.6.4 ska ändras på följande sätt:

(i) Första stycket i DDP_032 ska ersättas med följande:

"Datafältet i meddelandet *Positive Response Transfer Data – Detailed Speed* ska tillhandahålla följande data i följande ordning med angivande av SID = 76 Hex, TREP = 04 eller 24 Hex och med passande delning och räkning av undermeddelanden:"

(ii) Rubriken "Datastruktur för generation 1" ska ersättas med följande:

"Datastruktur för generation 1 (TREP 04 Hex)".

(iii) Rubriken "Datastruktur för generation 2" ska ersättas med följande:

"Datastruktur för generation 2 (TREP 24 Hex)".

(j) Punkt 2.2.6.5 ska ändras på följande sätt:

(i) Första stycket i DDP_033 ska ersättas med följande:

"Datafältet i meddelandet *Positive Response Transfer – Technical Data* ska tillhandahålla följande data i följande ordning med angivande av SID = 76 Hex, TREP = 05 eller 25 Hex och med passande delning och räkning av undermeddelanden:"

(ii) Rubriken "Datastruktur för generation 1" ska ersättas med följande:

"Datastruktur för generation 1 (TREP 05 Hex)".

(iii) Rubriken "Datastruktur för generation 2" ska ersättas med följande:

"Datastruktur för generation 2 (TREP 25 Hex)".

(k) I punkt 3.3 ska DDP_035 ersättas med följande:

"DDP_035 Överföring från ett färdskrivarkort inbegriper följande steg:

- Överför kortets basinformation i elementfilerna (EF) ICC och IC. Denna information är valfri att överföra och säkras inte med en digital signatur.
- För första och andra generationens färdskrivarkort: överför elementfiler (EF) under Tachograph DF:
- Överför elementfilerna (EF) Card_Certificate och CA_Certificate. Denna information säkras inte med en digital signatur.

Överföring av dessa filer är obligatorisk vid varje överföringssession.

- Överför övriga elementfiler (EF) för tillämpningsdata (under Tachograph DF), med undantag för Card_Download. Denna information skyddas med en digital signatur, med hjälp av de gemensamma säkerhetsmekanismerna i del A i tillägg 11.
- Överföring av åtminstone elementfilerna (EF) Application_Identification och Identification är obligatorisk vid varje överföringssession.
- Vid överföring från ett förarkort är överföring av följande elementfiler (EF) också obligatorisk:
 - Events_Data,
 - Faults_Data,

- Driver_Activity_Data,
- Vehicles_Used,
- Places,
- Control_Activity_Data,
- Specific_Conditions,
- Endast för andra generationens färdskrivarkort, och med undantag för överföring från ett förarkort som är insatt i en fordonsenhet vid en förarkontroll som utförs med hjälp av ett kontrollkort i generation 1 av en kontrollmyndighet i ett tredjeland: överför elementfilerna (EF) under Tachograph_G2 DF:
 - Överför elementfilerna (EF) CardSignCertificate, CA_Certificate och Link_Certificate (om de finns). Denna information säkras inte med en digital signatur.
Överföring av dessa filer är obligatorisk vid varje överföringssession.
 - Överför övriga elementfiler (EF) för tillämpningsdata (under Tachograph_G2 DF), med undantag för Card_Download. Denna information skyddas med en digital signatur, med hjälp av de gemensamma säkerhetsmekanismerna i del B i tillägg 11.
 - Överföring av åtminstone elementfilerna (EF) Application_Identification och Identification är obligatorisk vid varje överföringssession.
 - Vid överföring från ett förarkort är överföring av följande elementfiler (EF) också obligatorisk:
 - Events_Data,
 - Faults_Data,
 - Driver_Activity_Data,
 - Vehicles_Used,
 - Places,
 - Control_Activity_Data,
 - Specific_Conditions,
 - VehicleUnits_Used,
 - GNSS Places.
 - Vid överföring från ett förarkort, uppdatera datumet för LastCardDownload i EF Card_Download i DF Tachograph och, i förekommande fall, DF Tachograph_G2.
 - Vid överföring från ett verkstadskort, återställ kalibreringsräknaren i EF Card_Download i DF Tachograph och, i förekommande fall, i DF Tachograph_G2.

— Vid överföring från ett verkstadskort ska EF Sensor_Installation_Data i DF Tachograph och, i förekommande fall, DF Tachograph_G2 inte överföras.”.

(l) I punkt 3.3.2 ska första stycket i DDP_037 ersättas med följande:

”Sekvensen för överföring av elementfilerna (EF) ICC, IC, Card_Certificate (eller CardSignCertificate för DF Tachograph_G2), CA_Certificate och Link_Certificate (endast för DF Tachograph_G2) är följande:”

(m) I punkt 3.3.3 ska tabellen ersättas med följande:

Kort	Riktning	IDE/IFD	Betydelse/anmärkningar
	⇐	Select File	
OK	⇒		
	⇐	Perform Hash of File	— Beräknar hashvärdet för data-innehållet i vald fil med hjälp av föreskriven hashalgoritm enligt del A eller B i tillägg 11. Detta kommando är inte ett ISO-kommando.
Beräkna filens hashvärde och lagra det tillfälligt.			
OK	⇒		
	⇐	Read Binary	Om filen innehåller mer data än vad som ryms i bufferten hos läsaren eller kortet måste kommandot upprepas tills den fullständiga filen har lästs.
Fildata OK	⇒	Lagra mottagna data till externt lagringsmedium.	Enligt 3.4. Data storage format
	⇐	PSO: COMPUTE DIGITAL SIGNATURE	
Utför kommandot PSO: Compute Digital Signature och använd det tillfälligt lagrade hashvärdet.			
Signatur OK	⇒	Foga data till tidigare lagrade data i externt lagringsmedium.	Enligt 3.4. Data storage format”

(n) I punkt 3.4.2 ska DDP_046 ersättas med följande:

"DDP_046 En signatur ska lagras som nästa TLV-objekt direkt efter det TLV-objekt som innehåller filens data.

Definition	Betydelse	Längd
FID (2 byte) '00'	Tagg för EF (FID) i DF Tachograph, eller för kortets basinformation	3 byte
FID (2 byte) '01'	Tagg för signatur för EF (FID) i DF Tachograph	3 byte
FID (2 byte) '02'	Tagg för EF (FID) i DF Tachograph_G2	3 byte
FID (2 byte) '03'	Tagg för signatur för EF (FID) i DF Tachograph_G2	3 byte
xx xx	Värdefältets längd	2 byte

Exempel på överförda data i en fil i ett externt lagringsmedium:

Tagg	Längd	Värde
00 02 00	00 11	— Data i EF ICC
C1 00 00	00 C2	— Data i EF Card_Certificate
		— ...
05 05 00	0A 2E	Data i EF Vehicles_Used (i DF Tachograph)
05 05 01	00 80	Signatur för EF Vehicles_Used (i DF Tachograph)
05 05 02	0A 2E	Data i EF Vehicles_Used (i DF Tachograph_G2)
05 05 03	xx xx	Signatur för EF Vehicles_Used (i DF Tachograph_G2)"

(o) I punkt 4 ska DDP_049 ersättas med följande:

"DDP_049 Förarkort i generation 1: Data ska överföras med hjälp av första generationens protokoll för dataöverföring, och överförda data ska ha samma format som data som överförs från första generationens fordonsenhet.

Förarkort i generation 2: Fordonsenheten ska sedan överföra hela kortet, fil efter fil, enligt det protokoll för överföring från kort som definieras i punkt 3, och vidareända alla data som mottagits från kortet till IDE-enheten i lämpligt TLV-filformat (se 3.4.2), inpackade i meddelandet *Positive Response Transfer Data*."

(34) Gäller inte den svenska språkversionen.

(35) Tillägg 9 ska ändras på följande sätt:

(a) I innehållsförteckningen ska punkt 6 ersättas med följande:

”6. PROVNING AV EXTERN KOMMUNIKATIONSANORDNING FÖR FJÄRRÄVLÄSNING”.

(b) Gäller inte den svenska språkversionen.

(c) I punkt 2 ska tabellen med funktionsprov för fordonsenheten ersättas med följande:

Nr	Prov	Beskrivning	Tillämpliga krav
1	Administrativ provning		
1.1	Dokumentation	Dokumentationens korrekthet	
1.2	Tillverkarens provresultat	Resultat från tillverkarens prov som utförts under integreringen Uppvisande av provningsdokumentation	88, 89, 91
2	Okulär besiktning		
2.1	Överensstämmelse med dokumentation		
2.2	Identifiering/märkningar		224–226
2.3	Material		219–223
2.4	Plombering		398, 401–405
2.5	Externa gränssnitt		
3	Funktionsprov		
3.1	Tillhandahållna funktioner		02, 03, 04, 05, 07, 382
3.2	Driftlägen		09–11*, 134, 135
3.3	Tillträdesrättigheter till data och funktioner		12*, 13*, 382, 383, 386–389
3.4	Övervakning av insättning och uttag av kort		15, 16, 17, 18, 19*, 20*, 134
3.5	Mätning av hastighet och sträcka		21–31
3.6	Tidsmätning (prov utförs vid 20 °C)		38–43
3.7	Övervakning av föraraktiviteter		44–53, 134
3.8	Övervakning av körningsstatus		54, 55, 134
3.9	Manuella angivelser		56–62
3.10	Hantering av företagslås		63–68
3.11	Övervakning av kontrollaktiviteter		69, 70
3.12	Upptäckt av händelser och/eller fel		71–88, 134

Nr	Prov	Beskrivning	Tillämpliga krav
3.13	Data för identifiering av utrustning		93*, 94*, 97, 100
3.14	Data om insättning och uttag av förarkort		102*–104*
3.15	Data om föraraktiviteter		105*–107*
3.16	Data om platser och positioner		108*–112*
3.17	Vägmätardata		113*–115*
3.18	Detaljerade hastighetsdata		116*
3.19	Händelsedata		117*
3.20	Data om fel		118*
3.21	Kalibreringsdata		119*–121*
3.22	Data om tidsinställning		124*, 125*
3.23	Data om kontrollaktiviteter		126*, 127*
3.24	Data om företagslås		128*
3.25	Data om överföringsaktiviteter		129*
3.26	Data om särskilda omständigheter		130*, 131*
3.27	Registrering och lagring på färdskrivarkort		136, 137, 138*, 139*, 141*, 142, 143 144, 145, 146*, 147*, 148*, 149, 150
3.28	Visning		90, 134 151–168 PIC_001, DIS_001
3.29	Utskrift		90, 134 169–181, PIC_001, PRT_001–PRT_014
3.30	Varning		134, 182–191 PIC_001
3.31	Överföring av data till externa media		90, 134, 192–196
3.32	Fjärravläsning vid riktade vägkontroller		197–199
3.33	Utdata till ytterligare externa anordningar		200, 201
3.34	Kalibrering		202–206*, 383, 384, 386–391
3.35	Kalibreringskontroll på väg		207–209
3.36	Tidsinställning		210–212*
3.37	Avsaknad av störningar från ytterligare funktioner		06, 425

Nr	Prov	Beskrivning	Tillämpliga krav
3.38	Gränssnitt för rörelsesensorer		02, 122
3.39	Extern GNSS-anordning		03, 123
3.40	Kontroll att fordonsenheten upptäcker, registrerar och lagrar den eller de händelser och/eller det eller de fel som definierats av fordonsenhetens tillverkare när en parad rörelsesensor reagerar på magnetfält som stör rörelseavkänningen		217
3.41	Chiffersvit och standardiserade domänparametrar		CSM_48, CSM_50
4	Miljöprovningar		
4.1	Temperatur	Kontrollera funktionalitet genom: Prov enligt ISO 16750-4, kapitel 5.1.1.2: Low temperature operation test (72 h vid – 20 °C) Detta prov hänvisar till IEC 60068-2-1: Environmental testing - Part 2-1: Tests - Test A: Cold Prov enligt ISO 16750-4: kapitel 5.1.2.2: High temperature operation test (72 h vid 70 °C) Detta prov hänvisar till IEC 60068-2-2: Basic environmental testing procedures; part 2: tests; tests B: dry heat Prov enligt ISO 16750-4: kapitel 5.3.2: Rapid change of temperature with specified transition duration (–20 °C/70 °C, 20 cykler, uppehållstid (<i>dwell time</i>) 2 timmar vid varje temperatur) En minskad uppsättning prov (bland dem som anges i del 3 i denna tabell) kan utföras vid den lägre temperaturen, den högre temperaturen och under temperaturcyklerna.	213
4.2	Luftfuktighet	Kontrollera att fordonsenheten tål en cyklisk fuktighet (värmeprov) genom IEC 60068-2-30, test Db, sex 24-timmarscykler, med en temperatur som varierar mellan +25 °C och +55 °C och en relativ luftfuktighet av 97 % vid +25 °C, motsvarande 93 % vid +55 °C.	214
4.3	Mekanik	1. Sinusformade vibrationer: Kontrollera att fordonsenheten tål sinusformade vibrationer med följande egenskaper: Konstant variation mellan 5 och 11 Hz: amplitud 10 mm. Konstant acceleration mellan 11 och 300 Hz: 5 g Detta krav kontrolleras genom IEC 68-2-6, test Fc, med en minsta provtid av 3 × 12 timmar (12 timmar per axel). I ISO 16750-3 krävs inget prov med sinusformade vibrationer för anordningar som är placerade i en fjädrad (<i>decoupled</i>) fordonshytt.	219

Nr	Prov	Beskrivning	Tillämpliga krav
		2. Slumpartade vibrationer: Prov enligt ISO 16750-3: kapitel 4.1.2.8: Test VIII: Commercial vehicle, decoupled vehicle cab Slumpartat vibrationsprov, 10–2 000 Hz, effektivvärde i höjdled $21,3 \text{ m/s}^2$, effektivvärde i längdled $11,8 \text{ m/s}^2$, effektivvärde i sidled $13,1 \text{ m/s}^2$, 3 axlar, 32 timmar per axel, inklusive temperaturcykel mellan -20°C och $+70^\circ\text{C}$. Detta prov hänvisar till IEC 60068-2-64: Environmental testing - Part 2-64: Tests - Test Fh: Vibration, broadband random and guidance 3. Stötar: Mekanisk stöt med 3 g, halvsinusformad, i enlighet med ISO 16750. Proven ovan ska utföras på olika exemplar av den utrustning som provas.	
4.4	Skydd mot vatten och främmande föremål	Prov enligt ISO 20653: Road vehicles – Degree of protection (IP code) – Protection of electrical equipment against foreign objects, water and access (inga ändrade parametrar), minimivärde IP 40	220, 221
4.5	Skydd mot överspänning	Kontrollera att fordonsenheten tål strömtillförsel enligt följande: 24 V-versioner: 34 V vid $+40^\circ\text{C}$, 1 timme 12 V-versioner: 17 V vid $+40^\circ\text{C}$, 1 timme (ISO 16750-2)	216
4.6	Skydd mot omkastade poler	Kontrollera att fordonsenheten tål en omkastning av strömtillförseln. (ISO 16750-2)	216
4.7	Skydd mot kortslutning	Kontrollera att in- och utsignaler är skyddade mot kortslutning i strömtillförsel och jord. (ISO 16750-2)	216
5	EMC-prov		
5.1	Utstrålning och känslighet	Överensstämmelse med förordning ECE R10	218
5.2	Elektrostatisk urladdning	Överensstämmelse med ISO 10605:2008 + Technical Corrigendum: 2010 + AMD1:2014: $\pm 4 \text{ kV}$ för kontakt och $\pm 8 \text{ kV}$ för urladdning till luft	218

Nr	Prov	Beskrivning	Tillämpliga krav
5.3	Känslighet för överförda transienter i strömtillförseln	För 24 V-versioner: överensstämmelse med ISO 7637-2 + ECE förordning nr 10 Rev. 3: puls 1a: $V_s = -450 \text{ V}$, $R_i = 50 \text{ Ohm}$ puls 2a: $V_s = +37 \text{ V}$, $R_i = 2 \text{ Ohm}$ puls 2b: $V_s = +20 \text{ V}$, $R_i = 0,05 \text{ Ohm}$ puls 3a: $V_s = -150 \text{ V}$, $R_i = 50 \text{ Ohm}$ puls 3b: $V_s = +150 \text{ V}$, $R_i = 50 \text{ Ohm}$ puls 4: $V_s = -16 \text{ V}$, $V_a = -12 \text{ V}$, $t_6 = 100 \text{ ms}$ puls 5: $V_s = +120 \text{ V}$, $R_i = 2,2 \text{ Ohm}$, $t_d = 250 \text{ ms}$ För 12 V-versioner: överensstämmelse med ISO 7637-1 + ECE förordning nr 10 Rev. 3: puls 1: $V_s = -75 \text{ V}$, $R_i = 10 \text{ Ohm}$ puls 2a: $V_s = +37 \text{ V}$, $R_i = 2 \text{ Ohm}$ puls 2b: $V_s = +10 \text{ V}$, $R_i = 0,05 \text{ Ohm}$ puls 3a: $V_s = -112 \text{ V}$, $R_i = 50 \text{ Ohm}$ puls 3b: $V_s = +75 \text{ V}$, $R_i = 50 \text{ Ohm}$ puls 4: $V_s = -6 \text{ V}$, $V_a = -5 \text{ V}$, $t_6 = 15 \text{ ms}$ puls 5: $V_s = +65 \text{ V}$, $R_i = 3 \text{ Ohm}$, $t_d = 100 \text{ ms}$ Puls 5 ska endast provas för de fordonsenheter som är avsedda att installeras i fordon för vilka inget externt gemensamt skydd mot laddningsdump (<i>load dump</i>) används. För förslag till laddningsdump, se ISO 16750-2, 4:e utgåvan, kapitel 4.6.4.	218"

(d) Punkt 6 ska ersättas med följande:

”6. PROVNING AV EXTERN KOMMUNIKATIONSANORDNING FÖR FJÄRRÄVLÄSNING

Nr	Prov	Beskrivning	Tillämpliga krav
1.	Administrativ provning		
1.1	Dokumentation	Dokumentationens korrekthet	
2.	Okulär besiktning		
2.1.	Överensstämmelse med dokumentation		
2.2.	Identifiering/märkningar		225, 226
2.3	Material		219–223
3.	Funktionsprov		
3.1	Fjärravläsning vid riktade vägkontroller		4, 197–199

Nr	Prov	Beskrivning	Tillämpliga krav
3.2	Registrering och lagring i dataminne		91
3.3	Kommunikation med fordonsenhet		Tillägg 14: DSC_66–DSC_70, DSC_71–DSC_76
4.	Miljöprovningar		
4.1	Temperatur	Kontrollera funktionalitet genom: Prov enligt ISO 16750-4, kapitel 5.1.1.2: Low temperature operation test (72 h vid – 20 °C) Detta prov hänvisar till IEC 60068-2-1: Environmental testing - Part 2-1: Tests - Test A: Cold Prov enligt ISO 16750-4: kapitel 5.1.2.2: High temperature operation test (72 h vid 70 °C) Detta prov hänvisar till IEC 60068-2-2: Basic environmental testing procedures; part 2: tests; tests B: dry heat Prov enligt ISO 16750-4: kapitel 5.3.2: Rapid change of temperature with specified transition duration (– 20 °C/70 °C, 20 cykler, uppehållstid (<i>dwell time</i>) 1 timme vid varje temperatur) En minskad uppsättning prov (bland dem som anges i del 3 i denna tabell) kan utföras vid den lägre temperaturen, den högre temperaturen och under temperaturcyklerna.	213
4.2	Skydd mot vatten och främmande föremål	Prov enligt ISO 20653: Road vehicles – Degree of protection (IP code) – Protection of electrical equipment against foreign objects, water and access (målvärde IP40)	220, 221
5	EMC-prov		
5.1	Utstrålning och känslighet	Överensstämmelse med förordning ECE R10	218
5.2	Elektrostatisk urladdning	Överensstämmelse med ISO 10605:2008 + Technical Corrigendum: 2010 + AMD1:2014: +/- 4 kV för kontakt och +/- 8 kV för urladdning till luft	218

Nr	Prov	Beskrivning	Tillämpliga krav
5.3	Känslighet för överförda transienter i strömtillförseln	För 24 V-versioner: överensstämmelse med ISO 7637-2 + ECE förordning nr 10 Rev. 3: puls 1a: $V_s = -450 \text{ V}$, $R_i = 50 \text{ Ohm}$ puls 2a: $V_s = +37 \text{ V}$, $R_i = 2 \text{ Ohm}$ puls 2b: $V_s = +20 \text{ V}$, $R_i = 0,05 \text{ Ohm}$ puls 3a: $V_s = -150 \text{ V}$, $R_i = 50 \text{ Ohm}$ puls 3b: $V_s = +150 \text{ V}$, $R_i = 50 \text{ Ohm}$ puls 4: $V_s = -16 \text{ V}$, $V_a = -12 \text{ V}$, $t_6 = 100 \text{ ms}$ puls 5: $V_s = +120 \text{ V}$, $R_i = 2,2 \text{ Ohm}$, $t_d = 250 \text{ ms}$ För 12 V-versioner: överensstämmelse med ISO 7637-1 + ECE förordning nr 10 Rev. 3: puls 1: $V_s = -75 \text{ V}$, $R_i = 10 \text{ Ohm}$ puls 2a: $V_s = +37 \text{ V}$, $R_i = 2 \text{ Ohm}$ puls 2b: $V_s = +10 \text{ V}$, $R_i = 0,05 \text{ Ohm}$ puls 3a: $V_s = -112 \text{ V}$, $R_i = 50 \text{ Ohm}$ puls 3b: $V_s = +75 \text{ V}$, $R_i = 50 \text{ Ohm}$ puls 4: $V_s = -6 \text{ V}$, $V_a = -5 \text{ V}$, $t_6 = 15 \text{ ms}$ puls 5: $V_s = +65 \text{ V}$, $R_i = 3 \text{ Ohm}$, $t_d = 100 \text{ ms}$ Puls 5 ska endast provas för de fordonsenheter som är avsedda att installeras i fordon för vilka inget externt gemensamt skydd mot laddningsdump (<i>load dump</i>) används. För förslag till laddningsdump, se ISO 16750-2, 4:e utgåvan, kapitel 4.6.4.	218"

(e) Tabellen i punkt 8 om provning av driftskompatibilitet ska ersättas med följande:

"Nr	Prov	Beskrivning
8.1 Prov av driftskompatibilitet mellan fordonsenheter och färdskrivarkort		
1	Ömsesidig autentisering	Kontrollera att den ömsesidiga autentiseringen mellan fordonsenheten och färdskrivarkortet fungerar normalt.
2	Skriv-/läsprov	Utför ett typiskt aktivitetsscenario på fordonsenheten. Scenariot ska anpassas till den typ av kort som provas och inbegripa skrivningar till så många elementfiler (EF) som möjligt på kortet. Kontrollera genom en överföring från fordonsenheten att alla motsvarande registreringar har gjorts korrekt. Kontrollera genom en överföring från kortet att alla motsvarande registreringar har gjorts korrekt. Verifiera genom dagsutskrifter att alla motsvarande registreringar kan läsas korrekt.

Nr	Prov	Beskrivning
8.2 Prov av driftskompatibilitet mellan fordonsenheter och rörelsesensorer		
1	Parning	Kontrollera att parningen mellan fordonsenheterna och rörelsesensorerna fungerar normalt.
2	Aktivitetsprov	Utför ett typiskt aktivitetsscenario på rörelsesensorn. Scenariet ska omfatta en normal aktivitet och skapa så många händelser eller fel som möjligt. Kontrollera genom en överföring från fordonsenheten att alla motsvarande registreringar har gjorts korrekt. Kontrollera genom en överföring från kortet att alla motsvarande registreringar har gjorts korrekt. Verifiera genom en dagsutskrift att alla motsvarande registreringar kan läsas korrekt.
8.3 Prov av driftskompatibilitet mellan fordonsenheter och externa GNSS-anordningar (i förekommande fall)		
1	Ömsesidig autentisering	Kontrollera att den ömsesidiga autentiseringen (kopplingen) mellan fordonsenheten och den externa GNSS-anordningen fungerar normalt.
2	Aktivitetsprov	Utför ett typiskt aktivitetsscenario på den externa GNSS-anordningen. Scenariet ska omfatta en normal aktivitet och skapa så många händelser eller fel som möjligt. Kontrollera genom en överföring från fordonsenheten att alla motsvarande registreringar har gjorts korrekt. Kontrollera genom en överföring från kortet att alla motsvarande registreringar har gjorts korrekt. Verifiera genom en dagsutskrift att alla motsvarande registreringar kan läsas korrekt.”

(36) Tillägg 11 ska ändras på följande sätt:

(a) I punkt 8.2.3 ska CSM_49 ersättas med följande:

”CSM_49 Fordonsenheter, färdskrivarkort och externa GNSS-anordningar ska stödja algoritmerna SHA-256, SHA-384 och SHA-512, såsom de specificeras i [SHS].”

(b) I punkt 9.1.2 ska första stycket i CSM_58 ersättas med följande:

”CSM_58 Varje gång Erca genererar ett nytt europeiskt rotnyckelpar ska man också skapa ett länkcertifikat för den nya europeiska öppna nyckeln och signera det med den föregående europeiska privata nyckeln. Giltighetstiden för länkcertifikatet ska vara 17 år plus 3 månader. Detta visas även i figur 1 i avsnitt 9.1.7.”

(c) I punkt 9.1.4 ska CSM_72 ersättas med följande:

”CSM_72 Två unika nyckelpar för elliptisk kryptering ska genereras för varje fordonsenhet och benämnas VU_MA och VU_Sign. Denna arbetsuppgift ska utföras av tillverkare av fordonsenheter. Varje gång ett nyckelpar genereras för en fordonsenhet ska den part som genererar nyckeln sända den öppna nyckeln till sin certifieringsinstans (MSCA) för att få ett motsvarande certifikat för fordonsenheten signerat av certifieringsinstansen. Den privata nyckeln får endast användas av fordonsenheten.”

(d) Punkt 9.1.5 ska ändras på följande sätt:

(i) CSM_83 ska ersättas med följande:

"CSM_83 Ett unikt nyckelpar för elliptisk kryptering, benämnt Card_MA, ska genereras för varje färdskrivarkort. Ytterligare ett unikt nyckelpar för elliptisk kryptering, benämnt Card_Sign, ska desutom genereras för varje förarkort och varje verkstadskort. Denna arbetsuppgift får utföras av tillverkare av kort eller användaranpassare av kort. Varje gång ett nyckelpar genereras för ett kort ska den part som genererar nyckeln sända den öppna nyckeln till sin certifieringsinstans (MSCA) för att få ett motsvarande certifikat för kortet signerat av certifieringsinstansen. Den privata nyckeln får endast användas av färdskrivarkortet."

(ii) CSM_88 ska ersättas med följande:

"CSM_88 Giltighetstiden för ett CARD_MA-certifikat ska vara följande:

- För förarkort: 5 år
- För företagskort: 5 år
- För kontrollkort: 2 år
- För verkstadskort: 1 år"

(iii) Följande text ska läggas till i CSM_91:

"— Endast för kontrollkort, företagskort och verkstadskort, och endast om korten utfärdas under de första tre månaderna av giltighetstiden för ett nytt EUR-certifikat: EUR-certifikatet som är två generationer äldre, om ett sådant finns.

Anmärkning till sista punkten: Exempel: under de första tre månaderna för certifikatet Erca (3) (se figur 1) ska korten innehålla certifikatet Erca (1). Detta behövs för att säkerställa att dessa kort kan användas för att överföra data från fordonsenheter med Erca (1) vars normala livstid på 15 år plus perioden på tre månader för dataöverföring löper ut under dessa månader. Se sista punkten i krav 13 i bilaga IC."

(e) Punkt 9.1.6 ska ändras på följande sätt:

(i) CSM_93 ska ersättas med följande:

"CSM_93 Ett unikt nyckelpar för elliptisk kryptering, benämnt EGF_MA, ska genereras för varje extern GNSS-anordning. Denna arbetsuppgift ska utföras av tillverkare av externa GNSS-anordningar. Varje gång ett nyckelpar för EGF_MA genereras ska den part som genererar nyckeln sända den öppna nyckeln till sin certifieringsinstans (MSCA) för att få ett motsvarande EGF_MA-certifikat signerat av certifieringsinstansen. Den privata nyckeln får endast användas av den externa GNSS-anordningen."

(ii) CSM_95 ska ersättas med följande:

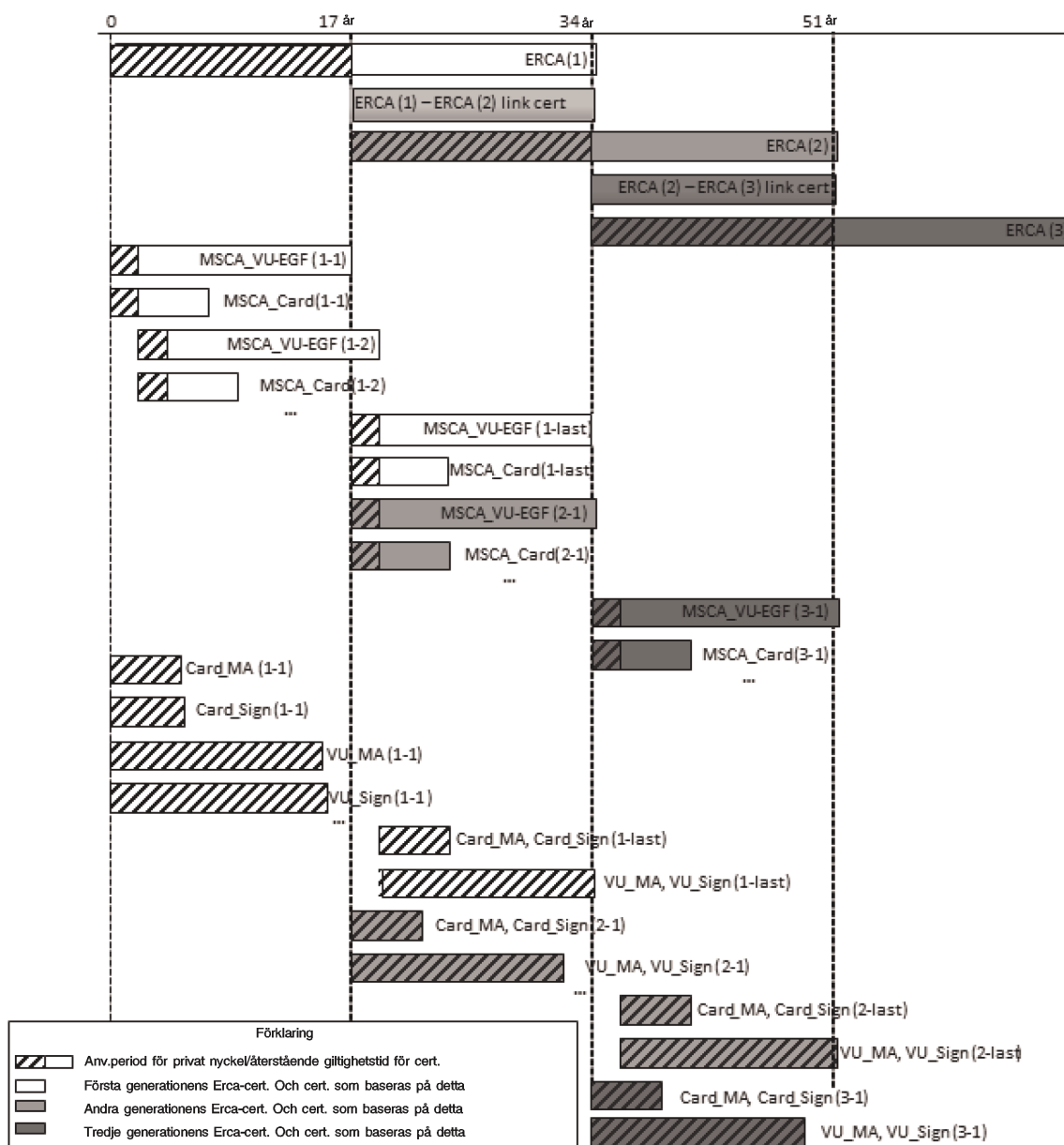
"CSM_95 En extern GNSS-anordning ska använda sitt EGF_MA-nyckelpar, bestående av en privat nyckel (EGF_MA.SK) och en öppen nyckel (EGF_MA.PK) endast för att utföra ömsesidig autentisering och överenskommelse om sessionsnyckel gentemot fordonsenheter såsom anges i avsnitt 11.4 i detta tillägg."

(f) Punkt 9.1.7 ska ändras på följande sätt:

(i) Figur 1 ska ersättas med följande:

”Figur 1

Utfärdande och användning av olika generationer av Erca-rotcertifikat, Erca-länkcertifikat, MSCA-certifikat och utrustningscertifikat



(ii) Anmärkning 6 till figur 1 ska ersättas med följande:

”6. För att spara plats visas skillnaden i fråga om giltighetsperiod mellan Card_MA- och Card_Sign-certifikaten endast för den första generationen.”

(g) Punkt 9.2.1.1 ska ändras på följande sätt:

(i) I CSM_106 ska första strecksatsen ersättas med följande:

— För 128-bits huvudnycklar för rörelsesensor: CV = 'B6 44 2C 45 0E F8 D3 62 0B 7A 8A 97 91 E4 5D 83'".

(ii) I CSM_107 ska första stycket ersättas med följande:

"Varje rörelsesensortillverkare ska generera en slumpmässig och unik parningsnyckel K_p för varje rörelsesensor, och ska överlämna varje parningsnyckel till sin certifieringsinstans (MSCA). Medlemsstatens certifieringsinstans (MSCA) ska kryptera varje parningsnyckel separat med rörelsesensornas huvudnyckel K_M och ska återsända den krypterade nyckeln till rörelsesensortillverkaren. För varje krypterad nyckel ska certifieringsinstansen meddela rörelsesensortillverkaren versionsnumret för tillhörande K_M ."

(iii) CSM_108 ska ersättas med följande:

"CSM_108 Varje rörelsesensortillverkare ska generera ett unikt serienummer för varje rörelsesensor, och ska överlämna alla serienummer till sin certifieringsinstans (MSCA). Medlemsstatens certifieringsinstans (MSCA) ska kryptera varje serienummer separat med identifieringsnyckeln K_{ID} och ska återsända det krypterade serienumret till rörelsesensortillverkaren. För varje krypterat serienummer ska certifieringsinstansen meddela rörelsesensortillverkaren versionsnumret för tillhörande K_{ID} ."

(h) Punkt 9.2.2.1 ska ändras på följande sätt:

(i) CSM_123 ska ersättas med följande:

"CSM_123 För varje fordonsenhet ska fordonsenhetstillverkaren skapa ett unikt serienummer och överlämna detta nummer till sin certifieringsinstans (MSCA) i en förfrågan om att få en uppsättning med två DSRC-nycklar som är specifika för fordonsenheten. Fordonsenhetens serienummer ska ha datatypen VuSerialNumber."

Anmärkning:

- Detta serienummer för fordonsenheten ska vara samma som elementet vuSerialNumber i VuIdentification (se tillägg 1) och CHR (*Certificate Holder Reference*) i fordonsenhetens certifikat.
- Fordonsenhetens serienummer kanske inte är känt när fordonsenhetens tillverkare begär de DSRC-nycklar som är specifika för fordonsenheten. I så fall ska fordonsenhetens tillverkare i stället överlämna den unika identifieringen av begäran om certifikat som tillverkaren använde vid begäran om fordonsenhetens certifikat (se CSM_153). Denna identifiering av begäran om certifikat ska därför vara samma som CHR (*Certificate Holder Reference*) i fordonsenhetens certifikat."

(ii) I CSM_124 ska informationskravet i steg 2 ersättas med följande:

"info = fordonsenhetens serienummer eller identifiering av begäran om certifikat, enligt vad som anges i CSM_123,"

(iii) CSM_128 ska ersättas med följande:

"CSM_128 MSCA ska föra ett register över alla fordonsenhetsspecifika DSRC-nycklar som den har genererat, tillsammans med deras versionsnummer och det serienummer för fordonsenheten eller den identifiering av begäran om certifikat som använts för att härleda dem."

(i) I punkt 9.3.1 ska första stycket i CSM_135 ersättas med följande:

"DER (Distinguished Encoding Rules) enligt [ISO 8825-1] ska användas för att koda dataobjekt inom certifikat. I tabell 4 visas den fullständiga kodningen av certifikat, inklusive alla byte för taggar och längder."

- (j) I punkt 9.3.2.3 ska CSM_141 ersättas med följande:

"CSM_141 Certifikatinnehavarens auktorisering (CHA) ska användas för att identifiera typen av certifikat. Den består av de sex byte som är mest signifikanta i färdskrivarens tillämpningsidentifierare (Application ID), konkatenerade med typen av utrustning för vilken certifikatet är avsett. För ett certifikat för fordonsenhet, förarkort eller verkstadskort används utrustningstypen också för att skilja mellan ett certifikat för ömsesidig autentisering och ett certifikat för att skapa digitala signaturer (se avsnitt 9.1 och datatyp EquipmentType i tillägg 1)."

- (k) I punkt 9.3.2.5 ska följande stycke läggas till i CSM_146:

"Anmärkning: För ett kortcertifikat ska värdet för CHR vara samma som värdet för cardExtendedSerialNumber i EF_ICC (se tillägg 2). För ett EGF-certifikat ska värdet för CHR vara samma som värdet för sensorGNSS-SerialNumber i EF_ICC (se tillägg 14). För ett certifikat fordonsenhet ska värdet för CHR vara samma som elementet vuSerialNumber i VuIdentification (se tillägg 1), såvida inte det tillverkarspecifika serienumret är okänt för tillverkaren när certifikatet begärs."

- (l) I punkt 9.3.2.6 ska CSM_148 ersättas med följande:

"CSM_148 Certifikatets första giltighetsdag anger startdatum och starttidpunkt för certifikatets giltighetsperiod."

- (m) Punkt 9.3.3 ska ändras på följande sätt:

- (i) I CSM_151 ska första stycket ersättas med följande:

"I samband med förfrågan om ett certifikat ska en MSCA skicka följande data till Erca:"

- (ii) CSM_153 ska ersättas med följande:

"CSM_153 En utrustningstillverkare ska översända följande data i en certifikatförfrågan till en MSCA, vilket gör det möjligt för denna MSCA att skapa certifikatinnehavarens referens (Certificate Holder Reference) för det nya utrustningscertifikatet:

— Om det är känt (se CSM_154): ett serienummer för utrustningen, som är unikt för tillverkaren, utrustningstypen och tillverkningsmånaden. I andra fall: en unik identifierare för certifikatförfrågan.

— Månad och år för tillverkning av utrustningen eller för certifikatförfrågan.

Tillverkaren ska säkerställa att dessa data är korrekta och att det certifikat som återsänds av MSCA installeras i den avsedda utrustningen."

- (n) Punkt 10.2.1 ska ändras på följande sätt:

- (i) I CSM_157 ska texten före anmärkningarna till figur 4 ersättas med följande:

"Fordonsenheter ska använda det protokoll som visas i figur 4 för att verifiera ett färdskrivarkorts certifikatskedja. För varje certifikat som fordonsenheten läser från kortet ska den kontrollera att CHA-fältet (Certificate Holder Authorisation) är korrekt:

— Kortcertifikatets CHA-fält ska ange ett kortcertifikat för ömsesidig autentisering (se datatyp EquipmentType i tillägg 1).

— Card.CA-certifikatets CHA-fält ska ange en MSCA.

— Card.Link-certifikatets CHA-fält ska ange Erca.”

(ii) I CSM_159 ska följande mening läggas till:

”Även om lagring av andra typer av certifikat är frivillig ska en fordonsenhet obligatoriskt lagra ett nytt länkcertifikat som överlämnas av ett kort.”

(o) Punkt 10.2.2 ska ändras på följande sätt:

(i) I CSM_161 ska texten före figur 5 ersättas med följande:

”Färdskrivarkort ska använda det protokoll som visas i figur 5 för att verifiera en fordonsenhets certifikatskedja. För varje certifikat som överlämnas av fordonsenheten ska kortet kontrollera att CHA-fältet (*Certificate Holder Authorisation*) är korrekt:

— VU.Link-certifikatets CHA-fält ska ange Erca.

— VU.CA-certifikatets CHA-fält ska ange en MSCA.

— CHA-fältet i fordonsenhetens certifikat ska ange ett certifikat för fordonsenhet och ömsesidig autentisering (se datatyp *EquipmentType* i tillägg 1).”

(ii) CSM_165 ska ersättas med följande:

”CSM_165 Om kommandot MSE:SET AT lyckas ska kortet ställa in den angivna VU.PK för efterföljande användning vid fordonsautentisering, och ska tillfälligt lagra $\text{Comp(VU.PK}_{\text{eph}})$. Om två eller flera lyckade MSE:SET AT-kommandon sänds innan överenskommelse om sessionsnyckel genomförs, ska kortet lagra endast senast mottagna $\text{Comp(VU.PK}_{\text{eph}})$. Kortet ska återställa $\text{Comp(VU.PK}_{\text{eph}})$ efter att kommandot GENERAL AUTHENTICATE utförts med gott resultat.”

(p) Punkt 10.3 ska ändras på följande sätt:

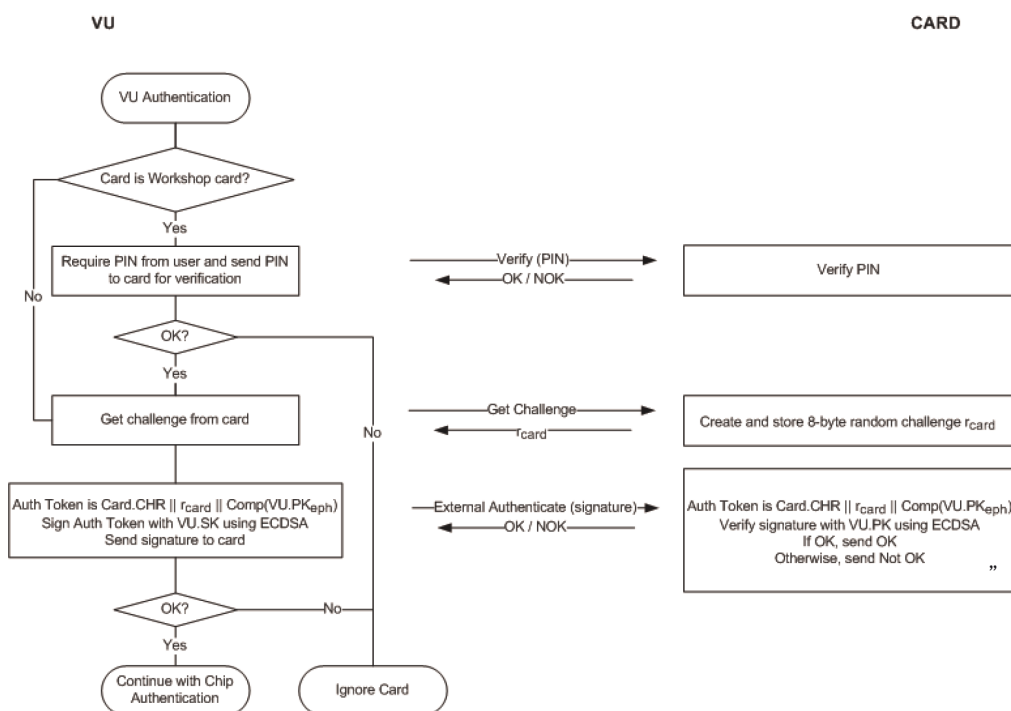
(i) Första stycket i CSM_170 ska ersättas med följande:

”Intill utmaningen från kortet ska fordonsenheten i signaturen inkludera den referens till certifikatinnehavaren som hämtas från kortcertifikatet.”

(ii) I CSM_171 ska figur 6 ersättas med följande:

”Figur 6

Protokoll för autentisering av fordonsenhet (VU)



(iii) CSM_174 ska ersättas med följande:

”CSM_174 Efter att ha mottagit fordonsenhetens signatur i ett EXTERNAL AUTHENTICATE-kommando, ska kortet

- beräkna token för autentiseringen genom att konkatenera Card.CHR, kortutmaningen rcard och identifieraren för fordonsenhetens tillfälliga öppna nyckel $\text{Comp(VU.PK}_{\text{eph}})$,
- kontrollera fordonsenhetens signatur med hjälp av ECDSA-algoritmen och den hashalgoritm som är länkad till nyckelstorleken för fordonsenhetens VU_MA-nyckelpar, enligt vad som anges i CSM_50, kombinerat med VU.PK och den beräknade token för autentiseringen.”

(q) I punkt 10.4 ska CSM_176 ändras på följande sätt:

(i) Punkt 2 ska ersättas med följande:

”2. Fordonsenheten översänder den öppna punkten (*public point*) $\text{VU.PK}_{\text{eph}}$ för sitt tillfälliga nyckelpar till kortet. Den öppna punkten ska omvandlas till en oktetsträng i enlighet med [TR-03111]. Det okomprimerade kodningsformatet ska användas. Såsom förklaras i CSM_164 har fordonsenheten genererat detta tillfälliga nyckelpar före verifieringen av fordonsenhetens certifikatskedja. Fordonsenheten översänder identifieraren av den tillfälliga öppna nyckeln $\text{Comp(VU.PK}_{\text{eph}})$ till kortet, och kortet lagrade den.”

(ii) Punkt 6 ska ersättas med följande:

”6. Med användning av K_{MAC} beräknar kortet en token för autentisering för identifieraren för fordonsenhetens tillfälliga punkt: $T_{\text{PICC}} = \text{CMAC}(K_{\text{MAC}}, \text{VU.PK}_{\text{eph}})$. Den öppna punkten ska ha det format som används av fordonsenheten (se punkt 2 ovan). Kortet översänder N_{PICC} och T_{PICC} till fordonsenheten.”

(r) I punkt 10.5.2 ska CSM_191 ersättas med följande:

"CSM_191 Alla dataobjekt som ska krypteras ska fyllas ut i enlighet med [ISO 7816-4] med användning av utfyllnadsindikator '01'. För beräkningen av MAC ska dataobjekt i dataenheten (APDU) fyllas ut i enlighet med [ISO 7816-4].

Anmärkning: Utfyllnad för säker meddelandehantering utförs alltid av skiktet för säker meddelandehantering, inte av CMAC- eller CBC-algoritmerna.

Sammanfattning och exempel

En kommando-APDU med tillämpad säker meddelandehantering kommer att ha följande struktur, beroende på respektive fall av oskyddat kommando (DO betyder dataobjekt):

Fall 1: CLA INS P1 P2 || Lc' || DO '8E' || Le

Fall 2: CLA INS P1 P2 || Lc' || DO '97' || DO '8E' || Le

Fall 3 (jämn INS-byte): CLA INS P1 P2 || Lc' || DO '81' || DO '8E' || Le

Fall 3 (udda INS-byte): CLA INS P1 P2 || Lc' || DO 'B3' || DO '8E' || Le

Fall 4 (jämn INS-byte): CLA INS P1 P2 || Lc' || DO '81' || DO '97' || DO '8E' || Le

Fall 4 (udda INS-byte): CLA INS P1 P2 || Lc' || DO 'B3' || DO '97' || DO '8E' || Le

där Le = '00' eller '00 00' beroende på om fält med kort längd eller fält med utökad längd används; se [ISO 7816-4].

En svars-APDU med tillämpad säker meddelandehantering kommer att ha följande struktur, beroende på respektive fall av oskyddat svar:

Fall 1 eller 3: DO '99' || DO '8E' || SW1SW2

Fall 2 eller 4 (jämn INS-byte) utan kryptering: DO '81' || DO '99' || DO '8E' || SW1SW2

Fall 2 eller 4 (jämn INS-byte) med kryptering: DO '87' || DO '99' || DO '8E' || SW1SW2

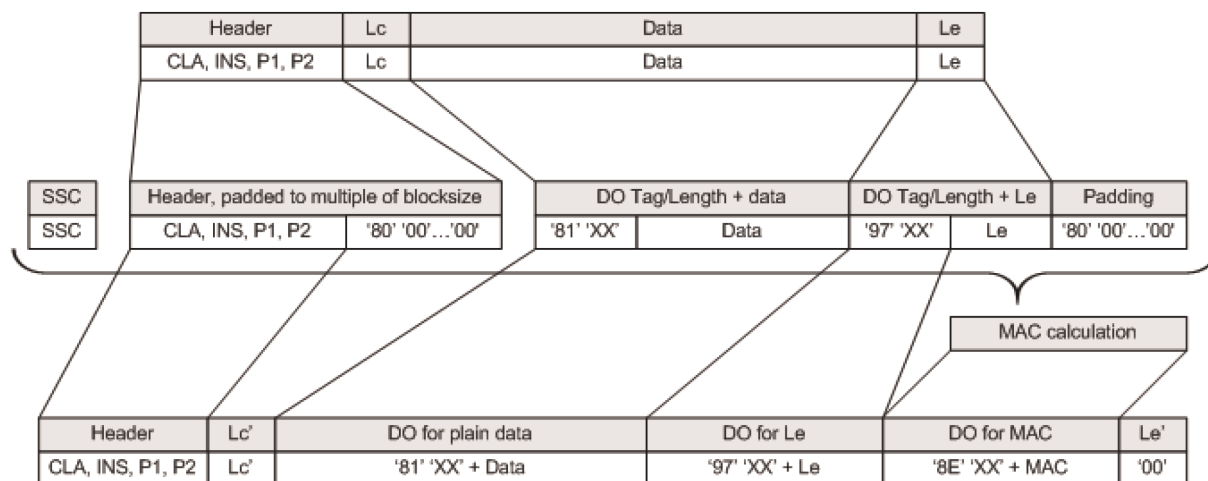
Fall 2 eller 4 (udda INS-byte) utan kryptering: DO 'B3' || DO '99' || DO '8E' || SW1SW2

Anmärkning: Fall 2 eller 4 (udda INS-byte) med kryptering används aldrig i kommunikationen mellan en fordonsenhet och ett kort.

Nedan visas tre exempel på APDU-omvandlingar för kommandon med jämn INS-kod. Figur 8 visar en autentiserad kommando-APDU i fall 4, figur 9 visar en autentiserad svars-APDU i fall 1/fall 3, och figur 10 visar en krypterad och autentiserad svars-APDU i fall 2/fall 4.

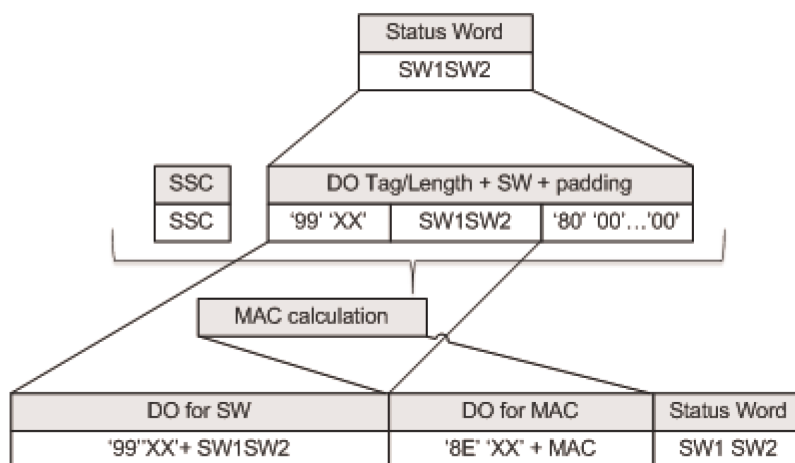
Figur 8

Omvandling av en autentiserad kommando-APDU i fall 4



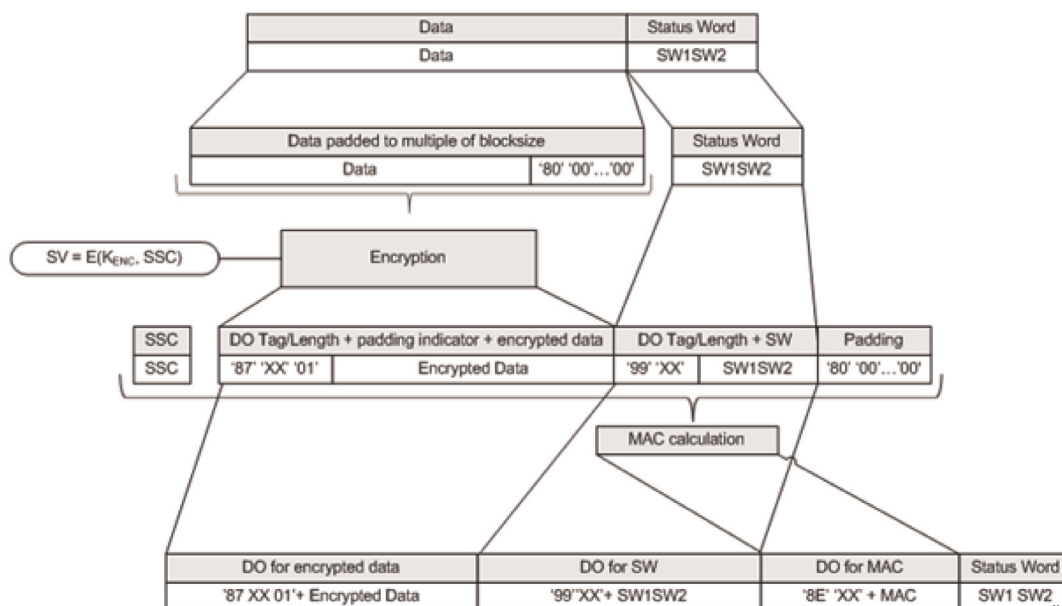
Figur 9

Omvandling av en autentiserad svars-APDU i fall 1/fall 3



Figur 10

Omvandling av en krypterad och autentiserad svars-APDU i fall 2/fall 4



(s) I punkt 10.5.3 ska CSM_193 ersättas med följande:

”CSM_193 Ett färdskrivarkort ska avbryta en pågående session med säker meddelandehantering om, och endast om, ett av följande villkor är uppfyllt:

- Det tar emot en kommando-APDU i klartext.
- Det upptäcker ett fel vid säker meddelandehantering i en kommando-APDU:
 - Ett förväntat dataobjekt för säker meddelandehantering saknas, dataobjektens ordningsföljd är felaktig, eller ett okänt dataobjekt är inkluderat.
 - Ett dataobjekt för säker meddelandehantering är felaktigt (exempel: MAC-värdet är felaktigt eller TLV-strukturen är felaktig).
- Det blir strömlöst eller återställt.
- Fordonsenheten startar processen för autentisering av fordonsenhet.
- Gränsen för antalet kommandon och tillhörande svar inom den aktuella sessionen har nåtts. För ett bestämt kort ska denna gräns fastställas av dess tillverkare, med beaktande av säkerhetskraven för den maskinvara som används, med ett högsta värde av 240 kommandon och tillhörande svar (med säker meddelandehantering) per session.”

(t) Punkt 11.3.2 ska ändras på följande sätt:

(i) Gäller inte den svenska språkversionen.

(ii) Gäller inte den svenska språkversionen.

(u) I punkt 11.3.3 ska första stycket i CSM_211 ersättas med följande:

”En fordonsenhet och en extern GNSS-anordning ska under normal drift använda det protokoll som visas i figur 11 för att verifiera den tidsmässiga giltigheten för det lagrade EGF_MA-certifikatet och för att bestämma den öppna nyckeln VU_MA för den påföljande autentiseringen av fordonsenheten. Ingen ytterligare ömsesidig verifiering av certifikatskedjorna ska äga rum under normal drift.”

(v) I punkt 12.3 ska tabell 6 ersättas med följande:

”Tabell 6

Antal byte med klartextdata och krypterade data per instruktion enligt definitioner i [ISO 16844-3]

Instruktion	Förfrågan/svar	Beskrivning av data	Antal byte med klartextdata enligt [ISO 16844-3]	Antal byte med klartextdata med användning av AES-nycklar	Antal byte med krypterade data vid användning av AES-nycklar med bitlängd		
					128	192	256
10	Förfrågan	Autentiseringsdata + filnummer	8	8	16	16	16
11	Svar	Autentiseringsdata + filinnehåll	16 eller 32, beroende på fil	16 eller 32, beroende på fil	32/48	32/48	32/48
41	Förfrågan	Rörelsesensorns serienummer	8	8	16	16	16
41	Svar	Parningsnyckel	16	16 / 24 / 32	16	32	32
42	Förfrågan	Sessionsnyckel	16	16 / 24 / 32	16	32	32
43	Förfrågan	Parningsinformation	24	24	32	32	32
50	Svar	Parningsinformation	24	24	32	32	32
70	Förfrågan	Autentiseringsdata	8	8	16	16	16
80	Svar	Rörelsesensorns räknarvärde + autentiseringsdata	8	8	16	16	16”

(w) I punkt 13.1 ska kravet om fordonsenhetens serienummer i CSM_224 ersättas med följande:

”Fordonsenhetens serienummer Fordonsenhetens serienummer eller identifiering av begäran om certifikat (datatyp VuSerialNumber eller CertificateRequestID) – se CSM_123.”

(x) I punkt 13.3 ska punkt 2 i CSM_228 ersättas med följande:

"2. Kontrollkortet ska använda den angivna DSRC-huvudnyckeln i kombination med fordonsenhetens serienummer eller identifieringen av begäran om certifikat i DSRC-säkerhetsdata för att härleda de fordonsenhetsspecifika DSRC-nycklarna $K_{VU_{DSRC_ENC}}$ och $K_{VU_{DSRC_MAC}}$, enligt vad som specificeras i CSM_124."

(y) Punkt 14.3 ska ändras på följande sätt:

(i) I CSM_234 ska texten före anmärkningarna till figur 13 ersättas med följande:

"En IDE-enhet kan själv utföra verifiering av en signatur för överförda data, eller den kan använda ett kontrollkort för detta ändamål. Om den använder ett kontrollkort ska verifiering av en signatur utföras såsom visas i Figure 13. För verifieringen av den tidsmässiga giltigheten hos ett certifikat som överlämnas av IDE-enheten ska kontrollkortet använda sin interna klocka, enligt vad som anges i CSM_167. Kontrollkortet ska uppdatera sin aktuella tid om den första giltighetsdagen för ett autentiskt certifikat som utgör 'giltig tidskälla' anger en tidpunkt som infaller senare än kortets aktuella tid. Kortet ska endast godta följande certifikat som en giltig tidskälla:

— Andra generationens Erca-länkcertifikat.

— Andra generationens MSCA-certifikat.

— Andra generationens VU_Sign- eller Card_Sign-certifikat som utfärdats av samma land som utfärdat kontrollkortets eget kortcertifikat.

Om den själv utför verifiering av en signatur, ska IDE-enheten verifiera autenticiteten och giltigheten hos alla certifikat i certifikatskedjan i datafilen, och den ska verifiera signaturen för data i enlighet med det signaturschema som definieras i [DSS]. I båda fallen är det nödvändigt, för varje certifikat som läses från datafilen, att kontrollera att CHA-fältet (*Certificate Holder Authorisation*) är korrekt:

— CHA-fältet i EQT-certifikatet ska ange ett certifikat för fordonsenhet eller ett kortcertifikat (i förekommande fall) för signering (se datatyp EquipmentType i tillägg 1).

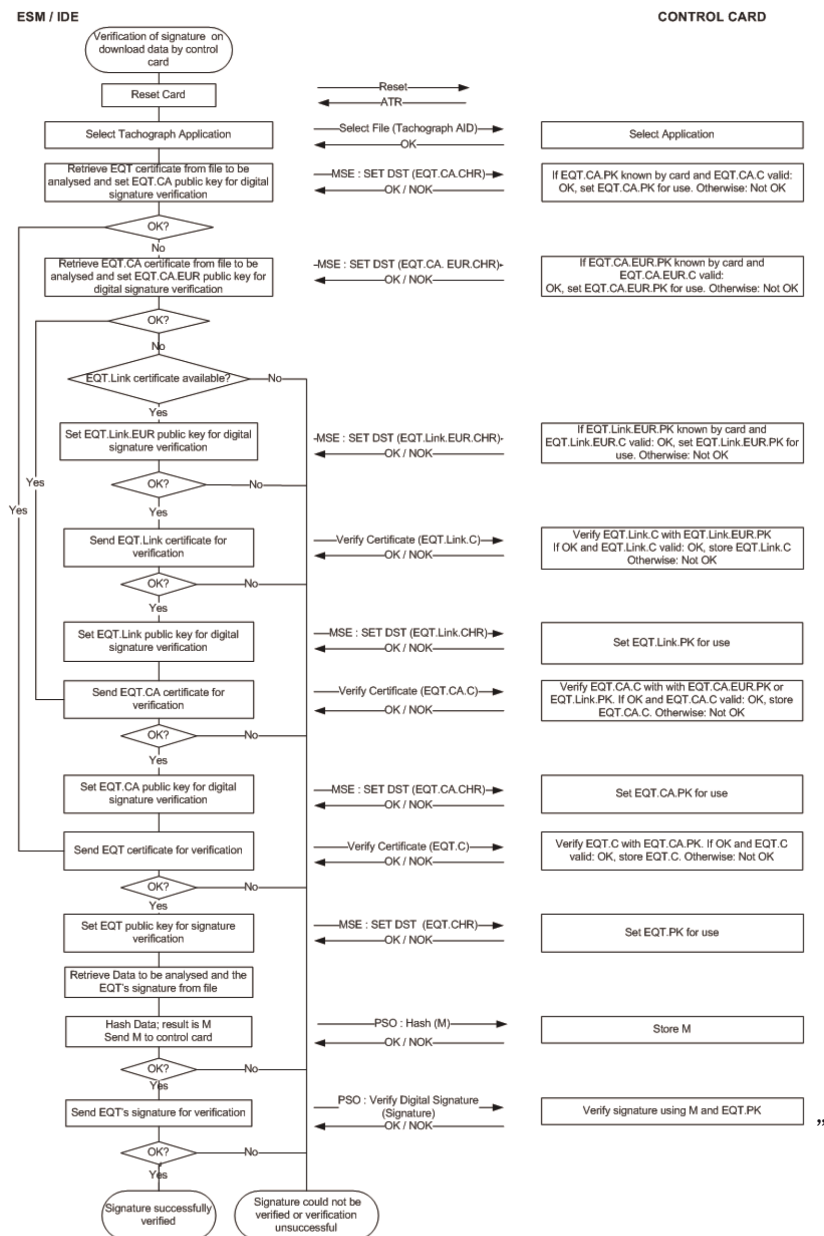
— EQT.CA-certifikatets CHA-fält ska ange en MSCA.

— EQT.Link-certifikatets CHA-fält ska ange Erca."

(ii) Figur 13 ska ersättas med följande:

”Figur 13

Protokoll för verifiering av signaturen för en överförd datafil



(37) Tillägg 12 ska ändras på följande sätt:

(a) Punkt 3 ska ändras på följande sätt:

(i) I GNS_4 ska andra stycket efter figur 2 ersättas med följande:

"Positionens upplösning baseras på formatet för den RMC-sats som beskrivs ovan. Den första delen av fälten 3) och 5) används för att representera antalet grader. Resterande tecken används för att representera antalet minuter med tre decimaler. Upplösningen är därmed 1/1 000 av en minut eller 1/60 000 av en grad (eftersom en minut är 1/60 grad)."

(ii) GNS_5 ska ersättas med följande:

"GNS_5 Fordonsenheten ska lagra positionsinformationen för latitud och longitud i sin databas med en upplösning på 1/10 minut eller 1/600 grad, såsom beskrivs i tillägg 1 för datatypen GeoCoordinates.

Kommandot GSA (*GPS DOP and active satellites*) kan användas av fordonsenheten för att bestämma och registrera signalens tillgänglighet och precision. Särskilt används HDOP (*Horizontal Dilution of Precision*) för att ge en indikering om precisionsnivån för registrerade lokaliseringssuppgifter (se avsnitt 4.2.2). Fordonsenheten kommer att lagra HDOP-värdet, beräknat som det minsta av de HDOP-värden som samlas in från de tillgängliga GNSS-systemen.

GNSS-identiteten anger motsvarande NMEA-identitet för varje GNSS-konstellation och SBAS (*Satellite-Based Augmentation System*).

Figur 3

GSA-satsens struktur

1 2 3 4 14 15 16 17 18
↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓

\$<GNSS-identitet>GSA,a,a,x,x,x,x,x,x,x,x,x,x,x,x,x,x,x,x*hh

1) Val av läge (*selection mode*)

2) Läge (*mode*)

3) Identitet för satellit 1 som används för fix

4) Identitet för satellit 2 som används för fix

...

14) Identitet för satellit 12 som används för fix

15) PDOP

16) HDOP

17) VDOP

18) Kontrollsumma „

(iii) GNS_6 ska ersättas med följande:

"GNS_6 GSA-satsen ska lagras med postnummer '02' till '06'."

(b) Punkt 4.2.1 ska ändras på följande sätt:

(i) GNS_16 ska ersättas med följande:

"GNS_16 Kommunikationsprotokollet stöder inte fält med utökad längd."

(ii) GNS_18 ska ersättas med följande:

"GNS_18 När det gäller funktionerna 1) (insamling och distribuering av GNSS-data), 2) (insamling av konfigurationsdata för den externa GNSS-anordningen) och 3) (styrprotokoll) ska den skyddade GNSS-transceiveren simulera ett smartkort med en filsystemsarkitektur som består av en huvudfil (MF, Master File), en dedikerad fil (DF, Dedicated File) med tillämpningsidentifierare såsom anges i avsnitt 6.2 i tillägg 1 ('FF 44 54 45 47 4D'), tre elementfiler (EF, Elementary File) som innehåller certifikat och en enda elementfil (EF.EGF) med filidentifieraren '2F2F' såsom beskrivs i tabell 1."

(iii) GNS_20 ska ersättas med följande:

"GNS_20 Den skyddade GNSS-transceiveren ska använda ett minne för att lagra data och kunna utföra minst 20 miljoner läs/skrivcykler.". Bortsett från denna aspekt avgör tillverkarna hur den skyddade GNSS-transceiveren utformas och realiseras.

Mapping av postnummer och data visas i tabell 1. Notera att det finns fem GSA-satser för GNSS-konstellationerna och SBAS (*Satellite-Based Augmentation System*)."

(c) I punkt 4.2.2 ska punkt 5 i GNS_23 ersättas med följande:

"5. Fordonsenhetens processor kontrollerar mottagna data genom att hämta information (t.ex. latitud och tid) från RMC-satsen enligt NMEA. RMC-satsen enligt NMEA omfattar denna information om positionen är giltig. Om positionen inte är giltig finns det ännu inte några lokaliseringsuppgifter och den kan inte användas för att registrera fordonets position. Om positionen är giltig hämtar fordonsenhetens processor även HDOP-värdena från GSA-satserna enligt NMEA och beräknar minimivärdet från de tillgängliga satellitsystemen (dvs. när en fix är tillgänglig)."

(d) I punkt 4.4.1 ska GNS_28 ersättas med följande:

"GNS_28 Om fordonsenheten inte klarar att kommunicera med den kopplade externa GNSS-anordningen under mer än 20 minuter ska fordonsenheten internt generera och registrera en händelse med typen EventFaultType och värdet '0E'H (Fel i kommunikation med extern GNSS-anordning) och med den aktuella tidpunkten som tidsstämpel. Händelsen uppstår endast om följande två villkor är uppfyllda: a) den smarta färdskrivaren är inte i kalibreringsläge och b) fordonet är i rörelse. Under dessa omständigheter utlöses ett kommunikationsfel när fordonsenhetens skyddade transceiver inte tar emot något svarsmeddelande efter ett sådant meddelande om begäran som beskrivs i avsnitt 4.2."

(e) I punkt 4.4.2 ska GNS_29 ersättas med följande:

"GNS_29 Om den externa GNSS-anordningen har öppnats fysiskt ska den skyddade GNSS-transceiveren radera hela sitt minne, inklusive krypteringsuppgifter. Fordonsenheten ska påvisa manipulering om svaret har status '6690', enligt vad som beskrivs i GNS_25 och GNS_26. Fordonsenheten ska sedan generera en händelse med typen EventFaultType och värdet '19'H (GNSS-manipulering upptäckt). Alternativt kan den externa GNSS-anordningen sluta att svara på alla begäranden."

(f) I punkt 4.4.3 ska GNS_30 ersättas med följande:

"GNS_30 Om den skyddade GNSS-transceiveren inte tar emot data från GNSS-mottagaren under mer än tre sammanhängande timmar ska den skyddade GNSS-transceiveren generera ett svarsmeddelande till kommandot READ RECORD, med postnummer (RECORD) lika med '01' och med ett datafält på 12 byte som alla har värdet 0xFF. När fordonsenheten tar emot svarsmeddelandet med detta värde i datafältet ska fordonsenheten generera och registrera en händelse med typen EventFaultType och värdet '0D'H (Positionsinformation från GNSS-mottagare saknas), med den aktuella tiden som tidsstämpel, men endast om följande två villkor är uppfyllda: a) den smarta färdskrivaren är inte i kalibreringsläge och b) fordonet är i rörelse."

(g) I punkt 4.4.4 ska texten i GNS_31 fram till figur 4 ersättas med följande:

"Om fordonsenheten upptäcker att EGF-certifikatet som används för ömsesidig autentisering inte längre är giltigt ska fordonsenheten generera och registrera en händelse med typen EventFaultType och värdet '1B'H (*Certifikat för extern GNSS-anordning har löpt ut*), med den aktuella tiden som tidsstämpel. Fordonsenheten ska fortfarande använda mottagna positionsdata från GNSS."

(h) I punkt 5.2.1 ska GNS_34 ersättas med följande:

"GNS_34 Om fordonsenheten inte tar emot data från GNSS-mottagaren under mer än tre sammanhängande timmar ska fordonsenheten generera och registrera en händelse med typen EventFaultType och värdet '0D'H (*Positionsinformation från GNSS-mottagare saknas*), med den aktuella tiden som tidsstämpel, men endast om följande två villkor är uppfyllda: a) den smarta färdskrivaren är inte i kalibreringsläge och b) fordonet är i rörelse."

(i) Gäller inte den svenska språkversionen.

(38) Tillägg 13 ska ändras på följande sätt:

(a) I punkt 2 ska fjärde stycket ersättas med följande:

"Förtydligande: I detta tillägg specificeras inte följande:

- Drift och hantering i samband med insamling av *data* i fordonsenheten (dessa ska specificeras på annat ställe i *förordningen* eller följa av produktens utformning).
- Överlämningsform för insamlade data gentemot tillämpningen som finns i den externa anordningen.
- Bestämmelser om datasäkerhet utöver den som tillhandahålls av Bluetooth® (t.ex. kryptering) och som rör innehållet i *data* (dessa ska specificeras på annat ställe i *förordningen*, nämligen i tillägg 11 om gemensamma säkerhetsmekanismer).
- De Bluetooth®-protokoll som används av ITS-gränssnittet."

(b) I punkt 4.2 ska tredje stycket ersättas med följande:

"När en extern anordning för första gången kommer inom fordonsenhetens räckvidd kan parningsprocessen enligt Bluetooth® inledas (se även bilaga 2). Enheterna utväxlar sina adresser, namn och profiler samt sin gemensamma hemliga nyckel, vilket innebär att de kan länka ihop sig på nytt när de befinner sig i varandras närhet. När detta steg är slutfört betraktas den externa anordningen som pålitlig och godkänd för att initiera begäran om att överföra data från färdskrivaren. Det finns inga planer på att lägga till krypteringsmekanismer utöver dem som tillhandahålls genom Bluetooth®. Om ytterligare säkerhetsmekanismer ändå behövs kommer dessa att utformas i enlighet med tillägg 11 om gemensamma säkerhetsmekanismer."

(c) Punkt 4.3 ska ändras på följande sätt:

(i) Första stycket ska ersättas med följande:

"Fordonsenheten ska av säkerhetsskäl kräva ett system för PIN-kodsauktorisering som är separerat från Bluetooth-parningen. Varje fordonsenhet ska kunna generera PIN-koder för autentiseringsändamål med minst fyra siffror. Varje gång en extern anordning parar sig med fordonsenheten ska den tillhandahålla rätt PIN-kod innan data tas emot."

(ii) Gäller inte den svenska språkversionen.

(d) I punkt 4.4 ska andra stycket efter rubriken "Datafält" ersättas med följande:

"Om de data som ska behandlas är större än det utrymme som finns tillgängligt i ett meddelande delas det upp i flera undermeddelanden. Varje undermeddelande ska ha samma startdel (*header*) och SID, men innehåller en räknare på 2 byte (CC, *Counter Current*, och CM, *Counter Max*) för att ange undermeddelandets ordningsnummer. Den mottagande anordningen kvitterar varje undermeddelande för att ge en möjlighet att felkontrollera och avbryta. Den mottagande anordningen kan godta undermeddelandet, be att det överförs igen, begära att den avsändande anordningen startar om eller avbryta överföringen."

(e) Bilaga 1 ska ändras på följande sätt:

(i) Rubriken ska ersättas med följande:

"1) FÖRTECKNING ÖVER TILLGÄNGLIGA DATA GENOM ITS-GRÄNSSNITTET".

(ii) Följande rad ska föras in i tabellen i punkt 3, efter raden "Positionsinformation från GNSS-mottagare saknas":

"Fel i kommunikation med extern GNSS-anordning"	— Den långvarigaste händelsen för vart och ett av de senaste tio dygn där händelsen inträffat — De fem långvarigaste händelserna under de senaste 365 dygna	— Datum och tidpunkt för händelsens början — Datum och tidpunkt för händelsens slut — Korttyp, kortnummer, utfärdande medlemsstat och generation för ett eventuellt kort som var insatt vid händelsens början och/eller slut — Antal liknande händelser samma dag"
---	--	---

(iii) I punkt 5 ska följande strecksats läggas till:

"— Fel i ITS-gränssnitt (i förekommande fall)."

(f) ASN.1-specifikationerna i bilaga 3 ska ändras på följande sätt:

(i) Följande rader ska införas som raderna 206a–206e efter rad 206:

```

206a
206b   DriverID ::= SEQUENCE{
206c     issuingMemberState OCTET STRING (SIZE(3)),
206d     cardNumber OCTET STRING (SIZE(16))
206e   };

```

(ii) Raderna 262–264 ska ersättas med följande:

```

262   driveRecognize BIT STRING ('00'B UNION '01'B),
263   driverCardDriver1 BIT STRING ('00'B UNION '01'B),
264   driverCardDriver2 BIT STRING ('00'B UNION '01'B), ";

```

(iii) Rad 275 ska ersättas med följande:

```
"275    outOfScopeCondition BIT STRING ('00'B UNION '01'B),";
```

(iv) Raderna 288–310 ska ersättas med följande:

```
"288    driver1WorkingState BIT STRING ('000'B UNION '001'B UNION '010'B UNION
289    '011'B UNION '100'B UNION '101'B ...),
290    driver2WorkingState BIT STRING ('000'B UNION '001'B UNION '010'B UNION
291    '011'B UNION '100'B UNION '101'B ...),
292
293    driver1TimeRelatedStates BIT STRING ('0000'B UNION '0001'B
294    UNION '0010'B UNION '0011'B UNION '0100'B UNION '0101'B UNION
295    '0110'B UNION '0111'B UNION '1000'B UNION '1001'B UNION '1010'B
296    UNION '1011'B UNION '1100'B UNION '1101'B ...),
297
298
299    driver2TimeRelatedStates BIT STRING ('0000'B UNION '0001'B
300    UNION '0010'B UNION '0011'B UNION '0100'B UNION '0101'B UNION
301    '0110'B UNION '0111'B UNION '1000'B UNION '1001'B UNION '1010'B
302    UNION '1011'B UNION '1100'B UNION '1101'B ...),
303
304
305
306    overSpeed BIT STRING ('00 'B UNION '01 'B),
307    driver1Identification DriverID,
308    driver2Identification DriverID,
309
310"
```

(v) Raderna 362 och 363 ska ersättas med följande:

```
"362    driver1MaximumDailyDrivingTime BIT STRING (SIZE(4)),
363    driver2MaximumDailyDrivingTime BIT STRING (SIZE(4)),";
```

(vi) Följande rader ska införas som raderna 410a och 410b efter rad 410:

```
"410a    comErrorWithExternalGNSSFacility
410b    CommunicationErrorWithTheExternalGNSSFacility,";
```

(vii) Följande rader ska införas som raderna 539a–539j efter rad 539:

```
"539a    CommunicationErrorWithTheExternalGNSSFacility ::= SEQUENCE{
539b    beginDate GeneralizedTime,
539c    endDate GeneralizedTime,
539d    cardsType SEQUENCE OF UTF8String,
539e    cardsNumber SEQUENCE OF INTEGER,
539f    issuingMemberState SEQUENCE OF NationAlpha,
539g    cardsGeneration SEQUENCE OF INTEGER,
539h    numberOfSimilarEvent INTEGER
539i    }
539j";
```

(39) Tillägg 14 ska ändras på följande sätt:

(a) Punkt 5.5 i innehållsförteckningen ska ersättas med följande:

"5.5 Stöd för direktiv (EU) 2015/719 490".

(b) Gäller inte den svenska språkversionen.

(c) Punkt 5.1 ska ändras på följande sätt:

(i) I DSC_19 ska tolfte strecksatsen ersättas med följande:

"— Antennen till fordonsenhetens DSRC-modul ska placeras på en plats där den ger en optimal DSRC-kommunikation mellan fordonet och antennen vid vägkanten, när läsaren är placerad 15 meter framför fordonet och på två meters höjd och riktad mot vindrutans horisontella och vertikala mittpunkt. För lätta fordon är det lämpligt med en installation på vindrutans övre del. För alla andra fordon ska DSRC-antennen installeras antingen nära vindrutans nedre del eller nära dess övre del."

(ii) I DSC_22 ska första stycket ersättas med följande:

"Antennens formfaktor är inte definierad utan ska baseras på ett kommersiellt beslut, så länge som fordonsenhetens monterade DSRC-modul uppfyller kraven i avsnitt 5 nedan. Antennen ska vara placerad enligt vad som fastställs i DSC_19 och effektivt stödja de användningsfall som beskrivs i avsnitten 4.1.2 och 4.1.3."

(d) Gäller inte den svenska språkversionen.

"7 REDCR > DSRC-VU Sends GET.request for data of other Attribute (if appropriate)"

(e) I punkt 5.4.4 ASN.1-modulens definition i DCS_40 ändras på följande sätt:

(i) Första raden i sekvensen för TachographPayload ska ersättas med följande:

"tp15638VehicleRegistrationPlate LPN - Vehicle Registration Plate as per EN 15509¹"

(ii) Följande text ska läggas till som fotnot ¹:

"1. Om en LPN (fordonets registreringsskylt) innehåller en alfabetsindikator (*AlphabetIndicator*) med värdet *LatinAlphabetNo2* eller *latinCyrillicAlphabet* mappas specialtecknen i fjärravläsaren genom tillämpning av särskilda regler i enlighet med bilaga E till ISO/DIS 14 906,2."

(iii) Superskript "2" ska tas bort från den rad där den aktuella postens tidsstämpel (*timestamp of current record*) definieras.

(iv) ASN.1-modulens definition av RtmTransferAck ska ersättas med följande:

```
"RtmTransferAck ::= INTEGER {  
    Ok (1),  
    NoK (2)  
} (1..255)";
```

(f) I punkt 5.4.5 ska RTM12 i tabell 14.3 ersättas med följande:

"RTM12 Sensorfel (Sensor Fault)	Fordonsenheten ska generera ett heltalsvärde för dataelement RTM12. Fordonsenheten ska tilldela variabeln sensor-fault något av följande värden: — 1 om en händelse av typen sensorfel ('35'H <i>Sensor fault</i>) har registrerats under de senaste tio dagarna. — 2 om en händelse av typen fel i GNSS-mottagare (<i>GNSS receiver fault</i>, antingen intern eller extern med värdet "36"H respektive '37'H) har registrerats under de senaste tio dagarna. — 3 om en händelse av typen fel i kommunikation med extern GNSS-anordning ('0E'H <i>Communication error with the external GNSS facility</i>) har registrerats under de senaste tio dagarna. — 4 om både sensorfel (<i>Sensor Fault</i>) och fel i GNSS-mottagare (<i>GNSS receiver fault</i>) har registrerats under de senaste tio dagarna. — 5 om både sensorfel (<i>Sensor Fault</i>) och fel i kommunikation med extern GNSS-anordning (<i>Communication error with the external GNSS facility</i>) har registrerats under de senaste tio dagarna. — 6 om både fel i GNSS-mottagare (<i>GNSS receiver fault</i>) och fel i kommunikation med extern GNSS-anordning (<i>Communication error with the external GNSS facility</i>) har registrerats under de senaste tio dagarna. — 7 om samtliga tre sensorfel har registrerats under de senaste tio dagarna. I annat fall ('ELSE'): Värdet ska sättas till 0 om inga händelser har registrerats under de senaste tio dagarna.	– En oktett för sensorfel i enlighet med datakatalog.	sensorFault INTEGER (0..255) ;;
--	---	--	--

(g) I punkt 5.4.6 ska DSC_43 ersättas med följande:

'DSC_43 Data ska kodas med hjälp av PER (Packed Encoding Rules) UNALIGNED, bortsett från TachographPayload och OwsPayload;', vilka ska kodas med hjälp av OER (Octet Encoding Rules) som är definierad i ISO/IEC 8825-7, Rec. ITU-T X.696.'

(h) I punkt 5.4.7, fjärde kolumnen i tabell 14.9 ska texten i den cell som beskriver Rtm-ContextMark; ersättas med följande:

'Objektidentifierare för den standard, del och version som stöds. Exempel: ISO (1), standard (0), TARV (15638), del 9 (9), version 1 (1).

Första oktetten (objektidentifieraren) är 06H. Andra oktetten (dess längd) är 06H. Efterföljande 6 oktetter kodar objektidentifieraren i exemplet.'

(i) Gäller inte den svenska språkversionen.

(j) I punkt 5.6.1 ska punkt a i DSC_68 ersättas med följande:

'a) För att olika leverantörer ska kunna kontrakteras att leverera fordonsenheten och fordonsenhetens DSRC-modul, och även olika partier av DSRC-moduler, ska anslutningen mellan fordonsenheten och dess externa DSRC-modul följa en öppen standard. Fordonsenheten ska anslutas till dess DSRC-modul via antingen.'

(k) I punkt 5.7.1 ska DSC_77 ersättas med följande:

'DSC_77 Redan skyddade data ska tillhandahållas av fordonsenhetens säkerhetsmodul till fordonsenhetens DSRC-modul. Fordonsenhetens säkerhetsmodul ska kontrollera att de data som registreras i fordonsenhetens DSRC-modul har registrerats på korrekt sätt. Registrering och rapportering av eventuella fel vid överföringen av data från fordonsenheten till minnet i fordonsenhetens DSRC-modul ska registreras med typen EventFaultType och värdet "0C"H (fel i kommunikation med kommunikationsanordning för fjärravläsning) tillsammans med en tidsstämpel.'

(40) Tillägg 15 ska ändras på följande sätt:

(a) Första stycket i punkt 2.2 ska ersättas med följande:

"Det är underförstått att första generationens färdskrivarkort är driftskompatibla med första generationens fordonsenheter (i enlighet med bilaga IB till förordning (EEG) nr 3821/85, medan andra generationens färdskrivarkort är driftskompatibla med andra generationens fordonsenheter i enlighet med bilaga IC till den här förordningen. Dessutom gäller följande krav:"

(b) I punkt 2.4.1 ska MIG_11 ändras på följande sätt:

(i) Första strecksatsen ska ersättas med följande:

"— Icke signerade elementfiler (EF) IC och ICC (frivilligt)."

(ii) Tredje strecksatsen ska ersättas med följande:

"— Andra elementfiler (EF) med tillämpningsdata (under DF Tachograph) som krävs av första generationens protokoll för överföring från kort. Denna information ska skyddas med en digital signatur, i enlighet med den första generationens säkerhetsmekanismer.

En sådan överföring ska inte omfatta elementfiler (EF) med tillämpningsdata som endast finns på andra generationens förarkort (och verkstadskort) (elementfiler med tillämpningsdata under DF Tachograph_G2)."

(c) I punkt 2.4.3 ska MIG_014 och MIG_015 ersättas med följande:

"MIG_014 Med undantag för förarkontroll som utförs av kontrollmyndigheter i tredjeländer ska data överföras från andra generationens fordonsenheter med hjälp av andra generationens säkerhetsmekanismer och det dataöverföringsprotokoll som anges i tillägg 7 till denna bilaga.

MIG_015 För förarkontroll som utförs av kontrollmyndigheter i tredjeländer kan det också vara möjligt att överföra data från andra generationens fordonsenheter med hjälp av första generationens säkerhetsmekanismer. Överförda data ska då ha samma format som data som överförs från en första generationens fordonsenhet. Denna förmåga kan väljas genom kommandon i menyerna."

BILAGA II

Bilaga II till förordning (EU) 2016/799 ska ändras på följande sätt:

1. I kapitel I ska punkt 1 b ersättas med följande:

”b) Ett typgodkännandenummer som motsvarar numret på det typgodkännandeintyg som utfärdats för prototypen till färdskrivaren, diagrambladet eller färdskrivarkortet, placerat i rektangelns omedelbara närhet.”

2. Gäller inte den svenska språkversionen.

3. Gäller inte den svenska språkversionen.
