Den här texten är endast avsedd som ett dokumentationshjälpmedel och har ingen rättslig verkan. EU-institutionerna tar inget ansvar för innehållet. De autentiska versionerna av motsvarande rättsakter, inklusive ingresserna, publiceras i Europeiska unionens officiella tidning och finns i EUR-Lex. De officiella texterna är direkt tillgängliga via länkarna i det här dokumentet

►B

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

(Text av betydelse för EES)

(EUT L 139, 26.5.2016, s. 1)

Rättad genom:

►C1 Rättelse, EUT L 146, 3.6.2016, s. 31 (2016/799)

►C2 Rättelse, EUT L 27, 1.2.2017, s. 169 (2016/799)

▼B

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

(Text av betydelse för EES)

Artikel 1

Syfte och tillämpningsområde

1. I denna förordning fastställs de bestämmelser som krävs för en enhetlig tillämpning av följande aspekter beträffande färdskrivare:

a) Registrering av fordonets position vid vissa punkter under förarens dagliga arbetsperiod.

b) Fjärravläst tidig upptäckt av eventuell manipulering eller eventuellt missbruk av smarta färdskrivare.

c) Gränssnitt med intelligenta transportsystem.

d) Administrativa och tekniska krav på förfaranden för typgodkännande av färdskrivare, inklusive säkerhetsmekanismerna.

2. Konstruktion, provning, installation, besiktning, drift och reparation av smarta färdskrivare och deras komponenter ska uppfylla de tekniska krav som fastställs i bilaga 1 C 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 1 eller bilaga 1 B till rådets förordning (EEG) nr 3821/85 ([1]), enligt vad som är tillämpligt.

4. Enligt artikel 10d i direktiv 96/53/EG ska anordningen för fjärravläst tidig upptäckt även överföra viktuppgifter som tillhandahålls av interna ombordsystem för vägning, i syfte att tidigt upptäcka bedrägerier.

Artikel 2

Definitioner

I denna förordning ska definitionerna i artikel 2 i förordning (EU) nr 165/2014 gälla.

Dessutom gäller följande definitioner:

1. *digital färdskrivare* eller *första generations färdskrivare*: en digital färdskrivare som inte är en smart färdskrivare.

2. *extern GNSS-anordning*: en anordning som innehåller GNSS-mottagaren om fordonsenheten inte utgörs av en enda enhet, och även andra komponenter som behövs för att skydda kommunikationen av positionsdata till resten av fordonsenheten.

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

▼B

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 1 C till denna förordning, samt ritningar, fotografier och andra relevanta dokument.

4. *informationspaket*: informationsmappen, i elektronisk form eller på papper, tillsammans med alla andra handlingar som den typgodkännande myndigheten lägger till under sin tjänsteutövning, inklusive intyget om EG-typgodkännande av färdskrivaren eller en ingående komponent i slutet av typgodkännandeförfarandet.

5. *index till informationspaket*: ett dokument som förtecknar det numrerade innehållet i informationspaketet och som identifierar alla de relevanta delarna av detta paket. Dokumentets format ska särskilja de på varandra följande stadierna i förfarandet för EG-typgodkännande, inklusive datum för varje revidering och uppdatering av detta paket.

6. *anordning för fjärravläst tidig upptäckt*: den utrustning i fordonsenheten som används för att genomföra riktade vägkontroller.

7. *smart färdskrivare* eller *andra generations färdskrivare*: en digital färdskrivare som överensstämmer med artiklarna 8, 9 och 10 i förordning (EU) nr 165/2014 samt med bilaga 1 C till den här förordningen.

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

9. *typgodkännande myndighet*: den myndighet i en medlemsstat som är behörig att typgodkänna färdskrivare eller dess komponenter, att genomföra tillståndsförfarande och att utfärda och eventuellt även återkalla intyg om typgodkännande, som fungerar som kontaktpunkt för de typgodkännande myndigheterna i övriga medlemsstater och som säkerställer att tillverkare uppfyller sina skyldigheter när det gäller överensstämmelse med kraven i denna förordning.

Artikel 3

Lokaliseringstjänster

1. Tillverkare ska säkerställa att smarta färdskrivare är kompatibla med de tjänster för positionsbestämning som tillhandahålls av systemen Galileo och Egnos (*European Geostationary Navigation Overlay Service*).

2. Utöver de system som avses i punkt 1 får tillverkare även välja att säkerställa kompatibilitet med andra satellitnavigeringssystem.

▼B

Artikel 4

Förfarande för typgodkännande av en färdskrivare och av färdskrivarkomponenter

1. En tillverkare eller dennes företrädare ska lämna in en ansökan om typgodkännande av en färdskrivare eller någon av dess komponenter, eller grupper av komponenter, till de typgodkännande myndigheter som utses av varje medlemsstat. Den ska bestå av en informationsmapp med information om var och en av de berörda komponenterna, inklusive, i tillämpliga fall, de typgodkännandeintyg för andra komponenter som krävs för att fullborda färdskrivaren och alla andra relevanta handlingar.

2. En medlemsstat ska bevilja typgodkännande för varje färdskrivare, komponent eller grupp av komponenter som uppfyller de administrativa och tekniska krav som avses i artikel 1.2 eller 1.3, beroende på vad som är tillämpligt. I detta fall ska den typgodkännande myndigheten utfärda ett typgodkännandeintyg till sökanden, och intyget ska överensstämma med förlagan i bilaga II till denna förordning.

3. Den typgodkännande myndigheten får begära att tillverkaren eller dennes företrädare tillhandahåller alla slag av ytterligare information.

4. Tillverkaren eller dennes företrädare ska tillhandahålla så många färdskrivare eller färdskrivarkomponenter som krävs för att typgodkännandeförfarandet ska kunna genomföras på ett tillfredsställande sätt, och ställa dessa till förfogande för de typgodkännande myndigheterna, samt för de enheter som ansvarar för att utfärda de intyg som avses i artikel 12.3 i förordning (EU) nr 165/2014.

5. Om tillverkaren eller dennes företrädare ansöker om ett typgodkännande av vissa komponenter eller grupper av komponenter till en färdskrivare ska denne förse de typgodkännande myndigheterna med de andra redan typgodkända komponenter samt andra delar som krävs för att färdigställa den kompletta färdskrivaren, så att dessa myndigheter kan utföra de prov som krävs.

Artikel 5

Ändringar av typgodkännanden

1. Tillverkaren eller dennes företrädare ska utan dröjsmål informera de typgodkännande myndigheter som beviljade det ursprungliga typgodkännandet om varje ändring av färdskrivarens programvara eller maskinvara eller av de slags material som används för dess tillverkning, som registreras i informationspaketet, och lämna in en ansökan om ändring av typgodkännandet.

2. De typgodkännande myndigheterna får revidera eller utvidga ett befintligt typgodkännande, eller utfärda ett nytt typgodkännande med hänsyn till ändringarnas art och karaktär.

En ”revidering” ska göras om den typgodkännande myndigheten anser att ändringarna av färdskrivarens programvara eller maskinvara, eller av de slags material som används för dess tillverkning, är små. I sådana fall ska den typgodkännande myndigheten utfärda de reviderade dokumenten i informationspaketet och ange vilken slags ändringar som gjorts och datum för deras godkännande. En uppdaterad version av informationspaketet i konsoliderad form, tillsammans med en detaljerad beskrivning av de ändringar som gjorts, ska vara tillräcklig för att uppfylla detta krav.

▼B

En ”utvidgning” ska göras om den typgodkännande myndigheten anser att ändringarna av färdskrivarens programvara eller maskinvara, eller av de slags material som används för dess tillverkning, är betydande. I sådana fall får den begära att nya prov utförs och informera tillverkaren eller dennes företrädare om detta. Om dessa prov visar sig vara tillfredsställande ska den typgodkännande myndigheten utfärda ett reviderat typgodkännandeintyg som innehåller ett nummer som hänvisar till den beviljade utvidgningen. I typgodkännandeintyget ska skälet till utvidgningen och dess utfärdandedatum anges.

3. Indexet till informationspaketet ska visa datum för den senaste utvidgningen eller revideringen av typgodkännandet eller datum för den senaste konsolideringen av den uppdaterade versionen av typgodkännandet.

4. Ett nytt typgodkännande ska krävas när de begärda ändringarna av en typgodkänd färdskrivare eller dess komponenter skulle leda till utfärdande av ett nytt säkerhetsintyg eller intyg om driftskompatibilitet.

Artikel 6

Ikraftträdande

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

Den ska tillämpas från och med den 2 mars 2016.

Bilagorna ska dock tillämpas från och med den 2 mars 2019, med undantag för tillägg 16 som ska tillämpas från och med den 2 mars 2016.

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

▼B

BILAGA I C

Krav i fråga om konstruktion, provning, installation och besiktning

INLEDNING

1. DEFINITIONER

2. ALLMÄN BESKRIVNING AV FÄRDSKRIVAREN OCH DESS FUNKTIONER

2.1 Allmän beskrivning

2.2 Funktioner

2.3 Driftlägen

2.4 Säkerhet

3. KONSTRUKTIONS- OCH FUNKTIONSKRAV FÖR FÄRDSKRIVARE

3.1 Övervakning av insättning och uttag av kort

3.2 Mätning av hastighet, position och sträcka

3.2.1 Mätning av tillryggalagd vägsträcka

3.2.2 Hastighetsmätning

3.2.3 Positionsmätning

3.3 Tidmätning

3.4 Övervakning av föraraktiviteter

3.5 Övervakning av körningsstatus

3.6 Förarens angivelser

3.6.1 Angivelse av de platser där dagens arbetsperioder påbörjas och/eller avslutas

3.6.2 Manuell angivelse av föraraktiviteter och förarens samtycke avseende ITS-gränssnitt

3.6.3 Angivelse av särskilda omständigheter

3.7 Hantering av företagslås

3.8 Övervakning av kontrollaktiviteter

3.9 Upptäckt av händelser och/eller fel

3.9.1 Insättning av ett ogiltigt kort (händelse, ”Insertion of a non-valid card”)

3.9.2 Kortkonflikt (händelse, ”Card conflict”)

3.9.3 Överlappning av tider (händelse, ”Time overlap”)

3.9.4 Körning utan korrekt kort (händelse, ”Driving without an appropriate card”)

3.9.5 Insättning av kort vid körning (händelse, ”Card insertion while driving”)

3.9.6 Senaste kortsession ej korrekt avslutad (händelse, ”Last card session not correctly closed”)

3.9.7 Hastighetsöverträdelse (händelse, ”Over speeding”)

3.9.8 Avbrott i strömtillförsel (händelse, ”Power supply interruption”)

3.9.9 Fel i kommunikation med kommunikationsanordning för fjärravläsning (händelse, ”Communication error with the remote communication facility”)

3.9.10 Positionsinformation från GNSS-mottagare saknas (händelse, ”Absence of position information from GNSS receiver”)

▼B

3.9.11	Fel i kommunikation med extern GNSS-anordning (händelse, ”Communication error with the external GNSS facility”)
3.9.12	Fel i rörelsedata (händelse, ”Motion data error”)
3.9.13	Konflikt i fordonets rörelsedata (händelse, ”Vehicle motion conflict”)
3.9.14	Försök till säkerhetsöverträdelse (händelse, ”Security breach attempt”)
3.9.15	Tidskonflikt (händelse, ”Time conflict”)
3.9.16	Kortfel (”Card”)
3.9.17	Färdskrivarfel (”Recording equipment”)
3.10	Inbyggd provning och självprovning
3.11	Avläsning från dataminne
3.12	Registrering och lagring i dataminne
3.12.1	Data för identifiering av utrustning
3.12.1.1	Data för identifiering av fordonsenhet
3.12.1.2	Data för identifiering av rörelsesensor
3.12.1.3	Data för identifiering av globalt system för satellitnavigering (GNSS).
3.12.2	Nycklar och certifikat
3.12.3	Data om insättning och uttag av förarkort och verkstadskort
3.12.4	Data om föraraktiviteter
3.12.5	Platser och positioner där dagens arbetsperioder påbörjas eller avslutas och/eller där tre timmars sammanhängande körtid uppnås
3.12.6	Vägmätardata
3.12.7	Detaljerade hastighetsdata
3.12.8	Händelsedata
3.12.9	Data om fel
3.12.10	Kalibreringsdata
3.12.11	Data om tidsinställning
3.12.12	Data om kontrollaktiviteter
3.12.13	Data om företagslås
3.12.14	Överföringsdata
3.12.15	Data om särskilda omständigheter
3.12.16	Data om färdskrivarkort
3.13	Avläsning från färdskrivarkort
3.14	Registrering och lagring på färdskrivarkort
3.14.1	Registrering och lagring på första generationens färdskrivarkort
3.14.2	Registrering och lagring på andra generationens färdskrivarkort
3.15	Visning
3.15.1	Standardvisning
3.15.2	Visning av varningar

▼B

3.15.3	Åtkomst via meny
3.15.4	Visning av övrig information
3.16	Utskrift
3.17	Varningar
3.18	Överföring av data till externa media
3.19	Fjärrkommunikation vid riktade vägkontroller
3.20	Utdata till ytterligare externa anordningar
3.21	Kalibrering
3.22	Kalibreringskontroll på väg
3.23	Tidsinställning
3.24	Prestanda
3.25	Material
3.26	Märkningar
4.	KONSTRUKTIONS- OCH FUNKTIONSKRAV FÖR FÄRDSKRIVARKORT
4.1	Synliga data
4.2	Säkerhet
4.3	Standarder
4.4	Miljö- och elspecifikationer
4.5	Lagring av data
4.5.1	Elementfiler för identifiering och korthantering
4.5.2	Identifiering av smartkort
4.5.2.1	Identifiering av chip
4.5.2.2	DIR (finns endast på andra generationens färdskrivarkort)
4.5.2.3	ATR-information (under vissa förutsättningar, finns endast på andra generationens färdskrivarkort)
4.5.2.4	Information med utökad längd (under vissa förutsättningar, finns endast på andra generationens färdskrivarkort)
4.5.3	Förarkort
4.5.3.1	Färdskrivartillämpning (tillgänglig för första och andra generationens fordonsenheter)
4.5.3.1.1	Tillämpningsidentifiering
4.5.3.1.2	Nyckel och certifikat
4.5.3.1.3	Kortidentifiering
4.5.3.1.4	Identifiering av kortinnehavare
4.5.3.1.5	Överföring från kort
4.5.3.1.6	Information om körkort
4.5.3.1.7	Händelsedata
4.5.3.1.8	Data om fel
4.5.3.1.9	Data om föraraktiviteter

▼B

4.5.3.1.10	Data om använda fordon
4.5.3.1.11	Platser där dagens arbetsperioder påbörjas och/eller avslutas
4.5.3.1.12	Data om kortsessioner
4.5.3.1.13	Data om kontrollaktiviteter
4.5.3.1.14	Data om särskilda omständigheter
4.5.3.2	Färdskrivartillämpning i generation 2 (ej åtkomlig för första generationens fordonsenhet)
4.5.3.2.1	Tillämpningsidentifiering
4.5.3.2.2	Nycklar och certifikat
4.5.3.2.3	Kortidentifiering
4.5.3.2.4	Identifiering av kortinnehavare
4.5.3.2.5	Överföring från kort
4.5.3.2.6	Information om körkort
4.5.3.2.7	Händelsedata
4.5.3.2.8	Data om fel
4.5.3.2.9	Data om föraraktiviteter
4.5.3.2.10	Data om använda fordon
4.5.3.2.11	Platser och positioner där dagens arbetsperioder påbörjas och/eller avslutas
4.5.3.2.12	Data om kortsessioner
4.5.3.2.13	Data om kontrollaktiviteter
4.5.3.2.14	Data om särskilda omständigheter
4.5.3.2.15	Data om använda fordonsenheter
4.5.3.2.16	Data om platser avseende tre timmar sammanhängande körning
4.5.4	Verkstadskort
4.5.4.1	Färdskrivartillämpning (tillgänglig för första och andra generationens fordonsenheter)
4.5.4.1.1	Tillämpningsidentifiering
4.5.4.1.2	Nycklar och certifikat
4.5.4.1.3	Kortidentifiering
4.5.4.1.4	Identifiering av kortinnehavare
4.5.4.1.5	Överföring från kort
4.5.4.1.6	Data om kalibrering och tidsinställning
4.5.4.1.7	Data om händelser och fel
4.5.4.1.8	Data om föraraktiviteter
4.5.4.1.9	Data om använda fordon
4.5.4.1.10	Data om påbörjande och/eller avslutande av dagens arbetsperioder
4.5.4.1.11	Data om kortsessioner
4.5.4.1.12	Data om kontrollaktiviteter

▼B

4.5.4.1.13	Data om särskilda omständigheter
4.5.4.2	Färdskrivartillämpning i generation 2 (ej åtkomlig för första generationens fordonsenhet)
4.5.4.2.1	Tillämpningsidentifiering
4.5.4.2.2	Nycklar och certifikat
4.5.4.2.3	Kortidentifiering
4.5.4.2.4	Identifiering av kortinnehavare
4.5.4.2.5	Överföring från kort
4.5.4.2.6	Data om kalibrering och tidsinställning
4.5.4.2.7	Data om händelser och fel
4.5.4.2.8	Data om föraraktiviteter
4.5.4.2.9	Data om använda fordon
4.5.4.2.10	Data om påbörjande och/eller avslutande av dagens arbetsperioder
4.5.4.2.11	Data om kortsessioner
4.5.4.2.12	Data om kontrollaktiviteter
4.5.4.2.13	Data om använda fordonsenheter
4.5.4.2.14	Data om platser avseende tre timmar sammanhängande körning
4.5.4.2.15	Data om särskilda omständigheter
4.5.5	Kontrollkort
4.5.5.1	Färdskrivartillämpning (tillgänglig för första och andra generationens fordonsenheter)
4.5.5.1.1	Tillämpningsidentifiering
4.5.5.1.2	Nycklar och certifikat
4.5.5.1.3	Kortidentifiering
4.5.5.1.4	Identifiering av kortinnehavare
4.5.5.1.5	Data om kontrollaktiviteter
4.5.5.2	Färdskrivartillämpning G2 (ej åtkomlig för första generationens fordonsenhet)
4.5.5.2.1	Tillämpningsidentifiering
4.5.5.2.2	Nycklar och certifikat
4.5.5.2.3	Kortidentifiering
4.5.5.2.4	Identifiering av kortinnehavare
4.5.5.2.5	Data om kontrollaktiviteter
4.5.6	Företagskort
4.5.6.1	Färdskrivartillämpning (tillgänglig för första och andra generationens fordonsenheter)
4.5.6.1.1	Tillämpningsidentifiering
4.5.6.1.2	Nycklar och certifikat
4.5.6.1.3	Kortidentifiering

▼B

4.5.6.1.4 Identifiering av kortinnehavare

4.5.6.1.5 Data om företagsaktiviteter

4.5.6.2 Färdskrivartillämpning G2 (ej åtkomlig för första generationens fordonsenhet)

4.5.6.2.1 Tillämpningsidentifiering

4.5.6.2.2 Nycklar och certifikat

4.5.6.2.3 Kortidentifiering

4.5.6.2.4 Identifiering av kortinnehavare

4.5.6.2.5 Data om företagsaktiviteter

5. INSTALLATION AV FÄRDSKRIVARE

5.1 Installation

5.2 Installationsskylt

5.3 Plombering

6. KONTROLLER, BESIKTNINGAR OCH REPARATIONER

6.1 Godkännande av montörer, verkstäder och fordonstillverkare

6.2 Kontroll av nya eller reparerade komponenter

6.3 Installationsbesiktning

6.4 Periodiska besiktningar

6.5 Uppmätning av fel

6.6 Reparationer

7. UTFÄRDANDE AV KORT

8. TYPGODKÄNNANDE AV FÄRDSKRIVARE OCH FÄRDSKRIVARKORT

8.1 Allmänt

8.2 Säkerhetsintyg

8.3 Funktionsintyg

8.4 Intyg om driftskompatibilitet

8.5 Intyg om typgodkännande

8.6 Undantagsförfarande: första intyg om driftskompatibilitet för andra generationens färdskrivare och färdskrivarkort

INLEDNING

Den första generationens digitala färdskrivarsystem infördes den 1 maj 2006 och används sedan dess. Sådana system får användas till slutet av sin livscykel för inrikes transporter. För internationella transporter gäller i stället att alla fordon ska vara utrustade med en andra generationens smart färdskrivare som uppfyller kraven i denna kommissionsförordning senast 15 år efter förordningens ikraftträdande.

Denna bilaga innehåller krav på andra generationens färdskrivare och färdskrivarkort. Andra generationens färdskrivare ska från och med sin införandedag installeras i fordon som registreras för första gången, och andra generationens färdskrivarkort ska utfärdas.

I syfte att främja ett smidigt införande av andra generationens färdskrivarsystem

▼B

— ska andra generationens färdskrivarkort utformas så att de även kan användas i första generationens fordonsenheter,

— ska ingen begäran göras om att första generationens färdskrivarkort ska ersättas på införandedagen.

Detta gör det möjligt för förare att behålla sitt eget förarkort och använda det i båda systemen.

Andra generationens färdskrivare ska dock endast kalibreras med hjälp av andra generationens verkstadskort.

Denna bilaga innehåller samtliga krav som rör driftskompatibiliteten mellan första och andra generationens färdskrivarsystem.

Tillägg 15 innehåller ytterligare uppgifter om hur de två systemen ska hanteras parallellt.

Förteckning över tillägg

Tillägg 1: DATAKATALOG

Tillägg 2: SPECIFIKATION FÖR FÄRDSKRIVARKORT

Tillägg 3: PIKTOGRAM

Tillägg 4: UTSKRIFTER

Tillägg 5: BILDSKÄRM

Tillägg 6: FRONTANSLUTNING FÖR KALIBRERING OCH DATAÖVERFÖRING

Tillägg 7: PROTOKOLL FÖR DATAÖVERFÖRING

Tillägg 8: KALIBRERINGSPROTOKOLL

Tillägg 9: TYPGODKÄNNANDE: FÖRTECKNING ÖVER MINSTA NÖDVÄNDIGA UPPSÄTTNING PROV

Tillägg 10: SÄKERHETSKRAV

Tillägg 11: GEMENSAMMA SÄKERHETSMEKANISMER

Tillägg 12: POSITIONSBESTÄMNING BASERAD PÅ GNSS (GLOBAL NAVIGATION SATELLITE SYSTEM)

Tillägg 13: ITS-GRÄNSSNITT

Tillägg 14: FJÄRRKOMMUNIKATIONSFUNKTION

Tillägg 15: MIGRERING: PARALLELL HANTERING AV FLERA UTRUSTNINGSGENERATIONER

Tillägg 16: ADAPTER FÖR FORDONSKATEGORIERNA M1 OCH N1

1 DEFINITIONER

I denna bilaga används följande termer och definitioner:

a) Aktivering

Den fas där färdskrivaren blir helt klar för drift och alla dess funktioner, inklusive säkerhetsfunktionerna, aktiveras med hjälp av ett verkstadskort.

b) Autentisering

Funktion avsedd att upprätta och kontrollera en angiven identitet.

c) Autenticitet

Det faktum att information kommer från en part vars identitet går att kontrollera.

d) Inbyggd provning (BIT, *Built-In-Test*)

Provning som utförs på begäran från en användare eller extern utrustning.

▼B

e) Kalenderdag

Ett dygn som sträcker sig från kl. 00.00 till kl. 24.00. Alla kalenderdagar räknas enligt UTC-tid (*Universal Time Coordinated*).

f) Kalibrering (av en smart färdskrivare)

Uppdatering eller bekräftelse av de fordonsparametrar som ska lagras i dataminnet. Fordonsparametrarna omfattar fordonsidentifiering (VIN (identifieringsnummer), VRN (registreringsnummer) samt medlemsstat där fordonet är registrerat) och fordonets egenskaper (w, k, l, däcksdimension, inställning på den hastighetsbegränsande anordningen (i förekommande fall), aktuell UTC-tid, aktuell vägmätarställning). Under kalibreringen av färdskrivaren ska även alla befintliga plomberingar som är relevanta för typgodkännande lagras i dataminnet.

En uppdatering eller bekräftelse av enbart UTC-tid ska betraktas som en tidsinställning och inte som en kalibrering, under förutsättning att den inte strider mot krav 409.

Kalibrering av färdskrivare kräver att ett verkstadskort används.

g) Kortnummer

Ett nummer bestående av 16 alfanumeriska tecken med vars hjälp ett enskilt färdskrivarkort kan identifieras inom en medlemsstat. Kortnumret inbegriper ett löpnummer (i förekommande fall), ett ersättningsindex och ett förnyelseindex för kortet.

Ett enskilt kort kan därför identifieras med hjälp av den utfärdande medlemsstatens kod och kortnumret.

h) Löpnummer

Det 14:e alfanumeriska tecknet i ett kortnummer, används för att åtskilja de kort som utfärdats till ett företag, en verkstad eller en kontrollmyndighet som har rätt att få flera färdskrivarkort utfärdade. Det enskilda företaget eller den enskilda verkstaden eller kontrollmyndigheten kan identifieras med hjälp av de första 13 tecknen i kortnumret.

i) Förnyelseindex

Det 16:e alfanumeriska tecknet i ett kortnummer, ökar varje gång färdskrivarkortet förnyas.

j) Ersättningsindex

Det 15:e alfanumeriska tecknet i ett kortnummer, ökar varje gång färdskrivarkortet ersätts.

k) Fordonets karakteristiska koefficient

Den numeriska koefficient som anger värdet för den utsignal som skickas av den del av fordonet som utgör gränssnitt med färdskrivaren (växellådans utgående axel eller fordonets hjulaxel) medan fordonet tillryggalägger en sträcka av en kilometer under sådana standardiserade provningsförhållanden som definieras i krav 414. Den karakteristiska koefficienten uttrycks i impulser per kilometer (w = … imp/km).

l) Företagskort

Ett färdskrivarkort som utfärdas av myndigheterna i en medlemsstat till ett transportföretag som har behov av att framföra fordon utrustade med färdskrivare. Transportföretaget kan identifieras genom kortet, som också möjliggör visning, överföring och utskrift av de data som lagras i färdskrivaren och som är låsta av transportföretaget.

▼B

m) Färdskrivarens konstant

Den numeriska konstant som anger värdet för den ingående signal som krävs för att visa och registrera en tillryggalagd sträcka av en kilometer. Denna konstant ska uttryckas i impulser per kilometer (k = … imp/km).

n) Sammanhängande körtid (enligt färdskrivarens beräkning) ([1])

En viss förares aktuella sammanhängande körtid sedan slutet av förarens senaste period av tillgänglighet (AVAILABILITY) eller rast/vila (BREAK/REST) eller okända (UNKNOWN ([2])) period om minst 45 minuter (denna period kan ha delats upp i flera perioder i enlighet med Europaparlamentets och rådets förordning (EG) nr 561/2006 ([3])). Vid de berörda beräkningarna tas efter behov hänsyn till tidigare aktiviteter som lagrats på förarkortet. Om föraren inte har satt in sitt kort bygger de berörda beräkningarna på de registreringar i dataminnet som avser den innevarande period där inget kort varit insatt i den aktuella kortplatsen.

o) Kontrollkort

Ett färdskrivarkort som utfärdas av myndigheterna i en medlemsstat till en nationell behörig kontrollmyndighet. Kontrollorganet, och eventuellt även kontrolltjänstemannen, kan identifieras genom kortet, som också ger tillträde till de data som lagras i dataminnet eller i förarkorten, och eventuellt även i verkstadskorten, så att dessa kan avläsas, skrivas ut och/eller överföras.

Det ska även ge tillträde till funktionen för kalibreringskontroll på väg och till data genom fjärravläsaren.

p) Sammanlagd avbrottstid (enligt färdskrivarens beräkning) ([1])

Den sammanlagda tiden för avbrott från körtiden beräknas som en viss förares aktuella sammanlagda tidsperioder för tillgänglighet (AVAILABILITY) eller rast/vila (BREAK/REST) eller okända (UNKNOWN ([2])) tidsperioder om minst 15 minuter, sedan slutet av förarens senaste period av tillgänglighet (AVAILABILITY) eller rast/vila (BREAK/REST) eller okända (UNKNOWN ([3])) period om minst 45 minuter (denna period kan ha delats upp i flera perioder i enlighet med förordning (EG) nr 561/2006).

Vid de berörda beräkningarna tas efter behov hänsyn till tidigare aktiviteter som lagrats på förarkortet. Okända perioder av negativ varaktighet (okänd periods början > (dvs. är senare än) okänd periods slut) på grund av överlappningar i tid mellan två olika färdskrivare beaktas inte vid beräkningen.

([1]) Detta sätt att beräkna den sammanhängande körtiden och den sammanlagda avbrottstiden ger färdskrivaren underlag för varningen om sammanhängande körtid. Det påverkar inte den juridiska tolkning som ska göras av dessa tider. Alternativa sätt att beräkna den sammanhängande körtiden och den sammanlagda avbrottstiden får användas för att ersätta dessa definitioner om de blivit inaktuella genom uppdateringar av annan relevant lagstiftning.

([2]) Okända (UNKNOWN) perioder motsvarar perioder där förarkortet inte varit insatt och inga föraraktiviteter angivits manuellt.

([3]) Europaparlamentets och rådets förordning (EG) nr 561/2006 av den 15 mars 2006 om harmonisering av viss sociallagstiftning på vägtransportområdet och om ändring av rådets förordningar (EEG) nr 3821/85 och (EG) nr 2135/98 samt om upphävande av rådets förordning (EEG) nr 3820/85 (EUT L 102, 11.4.2006, s. 1).

▼B

Om föraren inte har satt in sitt kort bygger de berörda beräkningarna på de registreringar i dataminnet som avser den innevarande period där inget kort varit insatt i den aktuella kortplatsen.

q) Dataminne

En anordning för elektronisk datalagring som är inbyggd i färdskrivaren.

r) Digital signatur

Data som bifogas till, eller en kryptografisk omvandling av, ett datablock som gör det möjligt för mottagaren av datablocket att påvisa dess autenticitet och integritet.

s) Överföring

Kopiering och digital signering av samtliga eller en del av en uppsättning av datafiler som finns registrerade i fordonsenhetens dataminne eller i ett färdskrivarkorts minne, under förutsättning att denna process inte ändrar eller tar bort några lagrade data.

Tillverkare av fordonsenheter för smarta färdskrivare och tillverkare av utrustning som är konstruerad för och avsedd att överföra datafiler ska vidta alla rimliga åtgärder för att säkerställa att överföringen av dessa data kan utföras av transportföretag eller förare med minsta möjliga fördröjning.

Även om överföringen av detaljerade hastighetsdata inte är nödvändig för att fastställa överensstämmelsen med förordning (EG) nr 561/2006 kan den användas för andra ändamål, t.ex. i samband med olycksutredningar.

t) Förarkort

Ett färdskrivarkort som utfärdas av myndigheterna i en medlemsstat till ett viss förare. Föraren kan identifieras genom kortet, som också möjliggör lagring av data om föraraktiviteter.

u) Hjulens effektiva omkrets

Genomsnittsvärdet för de sträckor som tillryggalagts av de hjul som förflyttar fordonet (drivhjulen) under loppet av ett fullt varv. Uppmätning av dessa sträckor ska ske under sådana standardiserade provningsförhållanden som definieras i krav 414 och uttrycks i formen ”l = … mm”. Fordonstillverkare får ersätta uppmätningen av dessa sträckor med en teoretisk beräkning där axeltrycket för fordon utan last i körklart skick ([1]) beaktas. Metoderna för en sådan teoretisk beräkning är föremål för godkännande från en behörig myndighet i en medlemsstat och de kan endast användas innan färdskrivaren aktiveras.

v) Händelse

Onormalt driftsförhållande som upptäcks av den smarta färdskrivaren och som kan vara följden av ett försök till bedrägeri.

w) Extern GNSS-anordning

Anordning som innehåller GNSS-mottagaren om fordonsenheten inte utgörs av en enda enhet, och även andra komponenter som behövs för att skydda kommunikationen av positionsdata till resten av fordonsenheten.

([1]) Kommissionens förordning (EU) nr 1230/2012 av den 12 december 2012 om genomförande av Europaparlamentets och rådets förordning (EG) nr 661/2009 avseende krav för typgodkännande av vikter och mått för motorfordon och släpvagnar till dessa fordon och om ändring av Europaparlamentets och rådets direktiv 2007/46/EG (EUT L 353, 21.12.2012, s. 31), i sin senaste lydelse.

▼B

x) Fel

Onormalt driftsförhållande som upptäcks av den smarta färdskrivaren och som kan bero på att den inte fungerar riktigt eller inte fungerar alls.

y) GNSS-mottagare

En elektronisk anordning som tar emot och digitalt bearbetar signalerna från ett eller flera globala system för satellitnavigering (GNSS, *Global Navigation Satellite System*) för att tillhandahålla information om position, hastighet och tidpunkt.

z) Installation

Montering av en färdskrivare i ett fordon.

aa) Driftskompatibilitet

Kapacitet att utväxla data och dela information hos system och underliggande verksamhetsprocesser.

bb) Gränssnitt

En anordning mellan olika system, genom vilken systemen kan ansluta sig till varandra och samverka.

cc) Position

Fordonets geografiska koordinater vid en viss tidpunkt.

dd) Rörelsesensor

Den del av färdskrivaren som ger en signal som motsvarar fordonets hastighet och/eller tillryggalagda sträcka.

ee) Ogiltigt kort

Ett kort som upptäckts vara felaktigt, eller vars första autentisering misslyckats, vars första giltighetsdag ännu inte inträtt eller vars sista giltighetsdag har passerats.

ff) Öppen standard

En standard som fastställs i ett dokument med standardspecifikationer som är tillgängligt gratis eller till en obetydlig kostnad och som får mångfaldigas, spridas eller användas gratis eller mot en nominell avgift.

gg) Omfattas ej (*out of scope*)

Anger att användning av färdskrivare inte krävs enligt bestämmelserna i förordning (EG) nr 561/2006.

hh) Hastighetsöverträdelse

Överskridande av den tillåtna hastigheten för fordonet, definierat som en period om minst 60 sekunder under vilken fordonets uppmätta hastighet överskrider den gräns för inställning av anordningen för hastighetsbegränsning som anges i rådets direktiv 92/6/EEG ([1]), i sin senaste lydelse.

ii) Periodisk besiktning

Ett antal moment som utförs för att kontrollera att färdskrivaren fungerar väl, att dess inställningar motsvarar fordonets parametrar och att inga anordningar för att manipulera färdskrivaren är anslutna till färdskrivaren.

([1]) Rådets direktiv 92/6/EEG av den 10 februari 1992 om montering och användning av hastighetsbegränsande anordningar i vissa kategorier av motorfordon inom gemenskapen (EGT L 57, 2.3.1992, s. 27).

▼B

jj) Skrivare

Komponent i färdskrivaren som skriver ut lagrade data.

kk) Fjärrkommunikation för tidig upptäckt

Kommunikation mellan fordonsenhetens kommunikationsanordning för fjärravläst tidig upptäckt och fjärravläsaren för tidig upptäckt vid riktade vägkontroller, i syfte att på distans upptäcka möjlig manipulering eller möjligt missbruk av färdskrivare.

ll) Kommunikationsanordning för fjärravläsning

Den utrustning i fordonsenheten som används för att utföra riktade vägkontroller.

mm) Fjärravläsare (för tidig upptäckt)

Det system som används av kontrolltjänstemän för riktade vägkontroller.

nn) Förnyelse

Utfärdande av ett nytt färdskrivarkort när giltighetstiden för ett befintligt kort löper ut, eller när det fungerar felaktigt och har återlämnats till den utfärdande myndigheten. Förnyelse innebär alltid att det råder säkerhet om att två giltiga kort inte existerar samtidigt.

oo) Reparation

All reparation av en rörelsesensor eller av en fordonsenhet eller av en kabel som förutsätter att strömtillförseln bryts, att andra färdskrivarkomponenter kopplas bort eller att rörelsesensorn eller fordonsenheten öppnas.

pp) Ersättning av kort

Utfärdande av ett färdskrivarkort som ersättning för ett befintligt kort som har förklarats som förkommet eller stulet eller som inte fungerar på ett fullgott sätt, och som inte har återlämnats till den utfärdande myndigheten. Ersättning innebär alltid en risk för att två giltiga kort existerar samtidigt.

qq) Säkerhetscertifiering

Förfarandet hos ett certifieringsorgan som använder CC (*Common Criteria*) för att intyga att den färdskrivare (eller den komponent) eller det färdskrivarkort som undersöks uppfyller de säkerhetskrav som definieras i de aktuella skyddsprofilerna.

rr) Självprovning

Provningar som färdskrivaren regelbundet och automatiskt gör för att upptäcka fel.

ss) Tidmätning

En permanent digital registrering av datum och tidpunkt (UTC).

tt) Tidsinställning

En automatisk inställning av aktuell tidpunkt med regelbundna intervall och inom en maximal tolerans av en minut, eller en inställning som utförs vid kalibrering.

uu) Däcksdimension

Angivelse av däckens dimensioner (drivhjul) enligt rådets direktiv 92/23/EEG ([1]), i sin senaste lydelse.

([1]) Rådets direktiv 92/23/EEG av den 31 mars 1992 om däck och däckmontering på motorfordon och släpvagnar till dessa fordon (EGT L 129, 14.5.1992, s. 95).

▼B

vv) Fordonsidentifiering

Nummer för identifiering av fordonet: Fordonets registreringsnummer (VRN, *Vehicle Registration Number*) med angivelse av registrerande medlemsstat och fordonets identifieringsnummer (VIN, *Vehicle Identification Number*) ([1]).

ww) Vecka (för beräkning i färdskrivaren)

Period som sträcker sig från kl. 00.00 UTC på en måndag till kl. 24.00 UTC på en söndag.

xx) Verkstadskort

Ett färdskrivarkort som utfärdas av myndigheterna i en medlemsstat till utsedd personal hos en färdskrivartillverkare, en montör, en fordonstillverkare eller en verkstad som godkänts av medlemsstaten. Kortinnehavaren kan identifieras genom kortet, som också möjliggör provning, kalibrering och aktivering av färdskrivare och/eller dataöverföring från dessa.

yy) Adapter

En anordning vars avgivna signal ständigt är representativ för fordonets hastighet och tillryggalagda sträcka, men inte är den signal som används för den oberoende rörelsedetekteringen, och som

— endast installeras och används i fordon av typerna M1 och N1 (enligt definitionen i bilaga II till Europaparlamentets och rådets direktiv 2007/46/EG ([2]), i sin senaste lydelse) och som tagits i bruk första gången efter den 1 maj 2006,

— installeras där det inte är mekaniskt möjligt att installera någon annan typ av befintlig rörelsesensor som i övrigt överensstämmer med bestämmelserna i denna bilaga och dess tillägg 1–15,

— installeras mellan fordonsenheten och den plats där impulser för hastighet/tillryggalagd sträcka avges med integrerade sensorer eller alternativa gränssnitt,

— för fordonsenheten i fråga har samma funktion som om en rörelsesensor som överensstämmer med bestämmelserna i denna bilaga och dess tillägg 1–16 skulle vara kopplad till fordonsenheten.

Användning av en sådan adapter i de fordon som beskrivs ovan ska möjliggöra installation och korrekt användning av en fordonsenhet som uppfyller alla krav i denna bilaga.

För dessa fordon omfattar den smarta färdskrivaren kablar, en adapter och en fordonsenhet.

([1]) Rådets direktiv 76/114/EEG av den 18 december 1975 om tillnärmning av medlemsstaternas lagstiftning om föreskrivna skyltar och märkningar samt deras placering och fastsättningssätt på motorfordon och släpvagnar till dessa fordon (EGT L 24, 30.1.1976, s. 1).

([2]) Europaparlamentets och rådets direktiv 2007/46/EG av den 5 september 2007 om fastställande av en ram för godkännande av motorfordon och släpvagnar till dessa fordon samt av system, komponenter och separata tekniska enheter som är avsedda för sådana fordon (”Ramdirektiv”) (EUT L 263, 9.10.2007, s. 1).

▼B

zz) Dataintegritet

Exakthet och överensstämmelse hos lagrade data, indikerat genom frånvaron av varje förändring av data mellan två uppdateringar av en datapost. Integritet förutsätter att föreliggande data är en exakt kopia av originalversionen, dvs. att de inte har skadats när de skrevs till och lästes tillbaka från ett färdskrivarkort eller en IDE-enhet, eller vid överföring via vilken kommunikationskanal som helst.

aaa) Integritet för personuppgifter

De övergripande tekniska åtgärder som vidtagits för att säkerställa genomförandet av de principer som fastställs i Europaparlamentets och rådets direktiv 95/46/EG ([1]), och av de principer som fastställs i Europaparlamentets och rådets direktiv 2002/58/EG ([2]).

bbb) Smart färdskrivarsystem

Färdskrivaren, färdskrivarkorten och hela uppsättningen av direkt eller indirekt samverkande utrustning vid konstruktion, installation, användning, provning och kontroll, såsom kort, fjärravläsare och all annan utrustning för dataöverföring, dataanalys, kalibrering, generering, hantering och införande av säkerhetselement osv.

ccc) Införandedag

36 månader efter det att de detaljerade bestämmelser som avses i artikel 11 i Europaparlamentets och rådets förordning (EU) nr 165/2014 ([3]) har trätt i kraft.

Efter detta datum gäller för fordon som registreras för första gången att

— *de ska vara utrustade med en färdskrivare som är ansluten till en tjänst för positionsbestämning som är baserad på ett satellitnavigeringssystem,*

— *de ska kunna kommunicera data till behöriga kontrollmyndigheters riktade vägkontroller medan fordonet är i rörelse,*

— *de får vara utrustade med standardiserade gränssnitt som möjliggör att data som registrerats eller genererats av färdskrivare i driftläge kan användas av en extern anordning.*

ddd) Skyddsprofil

Ett dokument som ingår i certifieringsförfarandet enligt CC (*Common Criteria*) och som ger en tillämpningsoberoende specifikation avseende säkerhetskrav för informationsskydd (*information assurance*).

([1]) Europaparlamentets och rådets direktiv 95/46/EG av den 24 oktober 1995 om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter (EGT L 281, 23.11.1995, s. 31).

([2]) Europaparlamentets och rådets direktiv 2002/58/EG av den 12 juli 2002 om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation (direktiv om integritet och elektronisk kommunikation) (EGT L 201, 31.7.2002, s. 37).

([3]) Europaparlamentets och rådets förordning (EU) nr 165/2014 om färdskrivare vid vägtransporter, om upphävande av rådets förordning (EEG) nr 3821/85 om färdskrivare vid vägtransporter och om ändring av Europaparlamentets och rådets förordning (EG) nr 561/2006 om harmonisering av viss sociallagstiftning på vägtransportområdet (EUT L 60, 28.2.2014, s. 1).

▼B

eee) GNSS-precision

När det gäller färdskrivares positionsregistrering med hjälp av globala system för satellitnavigering (GNSS): HDOP-värdet (*Horizontal Dilution of Precision*), beräknat som det minsta av de HDOP-värden som samlas in från de tillgängliga GNSS-systemen.

2 ALLMÄN BESKRIVNING AV FÄRDSKRIVAREN OCH DESS FUNKTIONER

2.1 **Allmän beskrivning**

Syftet med en färdskrivare är att registrera, lagra, visa och skriva ut data om föraraktiviteter, och att tillhandahålla dessa som utdata.

Alla fordon som är utrustade med en färdskrivare som överensstämmer med bestämmelserna i denna bilaga måste vara försedda med en hastighetsmätare och en vägmätare. Dessa funktioner får inbegripas i färdskrivaren.

01) Färdskrivaren inbegriper kablar, en rörelsesensor och en fordonsenhet.

02) Gränssnittet mellan rörelsegivarna och fordonsenheterna ska uppfylla de krav som specificeras i tillägg 11.

03) Fordonsenheten ska anslutas till ett eller flera globala system för satellitnavigering, såsom anges i tillägg 12.

04) Fordonsenheten ska kommunicera med fjärravläsare, såsom anges i tillägg 14.

05) Fordonsenheten kan inbegripa ett ITS-gränssnitt, vilket specificeras i tillägg 13.

Färdskrivaren får anslutas till andra anordningar genom ytterligare gränssnitt och/eller genom det frivilliga ITS-gränssnittet.

06) En funktion eller en eller flera anordningar, oavsett om de är godkända eller inte, som inbegrips i eller ansluts till färdskrivaren ska inte påverka eller kunna påverka en korrekt och säker drift av färdskrivaren eller överensstämmelsen med bestämmelserna i denna förordning.

Användare av färdskrivaren identifierar sig för färdskrivaren med hjälp av färdskrivarkort.

07) Färdskrivaren ger selektiv rätt till åtkomst till data och funktioner enligt användartyp och/eller användaridentitet.

Färdskrivaren registrerar och lagrar data i sitt dataminne, i kommunikationsanordningen för fjärravläsning och på färdskrivarkort.

Detta görs i enlighet med Europaparlamentets och rådets direktiv 95/46/EG av den 24 oktober 1995 om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter ([1]) och Europaparlamentets och rådets direktiv 2002/58/EC av den 12 juli 2002 om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation ([2]), och i överensstämmelse med artikel 7 i förordning (EU) nr 165/2014.

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

▼B

2.2 **Funktioner**

08) Färdskrivaren ska inbegripa följande funktioner:

— Övervakning av insättning och uttag av kort.

— Mätning av hastighet, sträcka och position.

— Tidmätning.

— Övervakning av föraraktiviteter.

— Övervakning av körningsstatus.

— Följande manuella angivelser av föraren:

— Angivelse av de platser där dagens arbetsperioder påbörjas och/eller avslutas.

— Manuell angivelse av föraraktiviteter.

— Angivelse av särskilda omständigheter.

— Hantering av företagslås.

— Övervakning av kontrollaktiviteter.

— Upptäckt av händelser och/eller fel.

— Inbyggd provning och självprovning.

— Avläsning från dataminne.

— Registrering och lagring i dataminne.

— Avläsning från färdskrivarkort.

— Registrering och lagring på färdskrivarkort.

— Visning.

— Utskrift.

— Varning.

— Överföring av data till externa media.

— Fjärrkommunikation vid riktade vägkontroller.

— Utdata till ytterligare anordningar.

— Kalibrering.

— Kalibreringskontroll på väg.

— Tidsinställning.

2.3 **Driftlägen**

09) Färdskrivaren ska ha följande fyra driftlägen:

— Driftläge.

— Kontrolläge.

— Kalibreringsläge.

— Företagsläge.

10) Färdskrivaren ska använda nedanstående funktionslägen enligt de giltiga färdskrivarkort som är insatta i kortläsarna. När det gäller att fastställa funktionsläge är det ointressant vilken generation färdskrivarkortet tillhör, så länge det är giltigt. Ett verkstadskort av första generationen ska alltid anses som ogiltigt när det är insatt i en andra generationens fordonsenhet.

▼B

Funktionsläge		Förarens kortplats				
		Inget kort	Förarkort	Kontrollkort	Verkstadskort	Företagskort
Medförarens kortplats	Inget kort	Drift	Drift	Kontroll	Kalibrering	Företag
	Förarkort	Drift	Drift	Kontroll	Kalibrering	Företag
	Kontrollkort	Kontroll	Kontroll	Kontroll (*)	Drift	Drift
	Verkstadskort	Kalibrering	Kalibrering	Drift	Kalibrering (*)	Drift
	Företagskort	Företag	Företag	Drift	Drift	Företag (*)

(*) I dessa lägen ska färdskrivaren endast använda det färdskrivarkort som är insatt i förarens kortplats.

11) Färdskrivaren ska bortse från ogiltiga kort som är insatta, förutom att visning, utskrift eller överföring av data ska vara möjligt från kort vars giltighetstid har löpt ut.

12) Alla funktioner som förtecknas i avsnitt 2.2 ska fungera i alla funktionslägen, med följande undantag:

— Kalibreringsfunktionen är endast tillgänglig i kalibreringsläge.

— Funktionen för kalibreringskontroll på väg är endast tillgänglig i kontrolläge.

— Funktionen för hantering av företagslås är endast tillgänglig i företagsläge.

— Funktionen för övervakning av kontrollaktiviteter är aktiv endast i kontrolläge.

— Överföringsfunktionen är inte tillgänglig i driftläge (med undantag av det som bestäms i krav 193) utom vid överföring från ett förarkort när ingen annan korttyp är insatt i fordonsenheten.

13) Färdskrivaren ska kunna tillhandahålla alla data till bildskärm, skrivare eller externa gränssnitt, med följande undantag:

— I driftläge ska all personlig identifiering (efternamn och förnamn) som inte motsvarar det insatta färdskrivarkortet raderas och alla kortnummer som inte motsvarar det insatta färdskrivarkortet ska delvis raderas (vartannat tecken – från vänster till höger – ska raderas).

— I företagsläge ska data om föraren (kraven 102, 105 och 108) endast kunna tillhandahållas för perioder som inte är låsta eller som inte har låsts av ett annat företag (enligt identifiering genom de första 13 siffrorna i företagskortets nummer).

— När inget kort är insatt i färdskrivaren kan data om föraren tillhandahållas endast för den innevarande och de åtta föregående kalenderdagarna.

— Personuppgifter från fordonsenheten får inte tillhandahållas via fordonsenhetens ITS-gränssnitt med mindre än att den förare som personuppgifterna gäller samtycker och att detta kan kontrolleras.

▼B

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

2.4 **Säkerhet**

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 rörelsesensorn 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 färdskrivaren och den externa GNSS-anordningen, 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.

14) För att systemsäkerhet ska kunna uppnås ska följande komponenter uppfylla de säkerhetskrav som anges i deras skyddsprofiler, såsom krävs i tillägg 10:

— Fordonsenhet.

— Färdskrivarkort.

— Rörelsesensor.

— Extern GNSS-anordning (denna profil är endast nödvändig och tillämplig för varianten med extern GNSS-anordning).

3 KONSTRUKTIONS- OCH FUNKTIONSKRAV FÖR FÄRDSKRIVARE

3.1 **Övervakning av insättning och uttag av kort**

15) Färdskrivaren ska övervaka kortläsarna för att upptäcka insättningar och uttag av kort.

16) När kortet sätts in ska färdskrivaren känna av om kortet är ett giltigt färdskrivarkort och i så fall identifiera korttypen och kortgenerationen.

Om ett kort med samma kortnummer och ett högre förnyelseindex redan varit insatt i färdskrivaren ska kortet förklaras ogiltigt.

Om ett kort med samma kortnummer och förnyelseindex men ett högre ersättningsindex redan varit insatt i färdskrivaren ska kortet förklaras ogiltigt.

17) Första generationens färdskrivarkort ska anses ogiltiga av färdskrivaren efter det att möjligheten att använda första generationens färdskrivarkort har tagits bort av en verkstad, i enlighet med tillägg 15 (krav MIG003).

18) Första generationens verkstadskort som sätts in i andra generationens färdskrivare ska anses ogiltiga.

▼B

19) Färdskrivaren ska utformas så att färdskrivarkortet låses i sitt läge när det sätts in på korrekt sätt i kortläsaren.

20) Färdskrivarkortet ska gå att ta ut endast när fordonet är stillastående och efter det att relevanta data har lagrats på kortet. Kortet ska vara möjligt att ta ut endast genom en uttrycklig handling från användaren.

3.2 **Mätning av hastighet, position och sträcka**

21) Rörelsesensorn (eventuellt inbyggd i en adapter) är den huvudsakliga informationskällan för mätning av hastighet och sträcka.

22) Denna funktion ska kontinuerligt mäta och kunna tillhandahålla det vägmätarvärde som motsvarar den sammanlagda sträcka som fordonet har tillryggalagt, med hjälp av pulserna från rörelsesensorn.

23) Denna funktion ska kontinuerligt mäta och kunna tillhandahålla fordonets hastighet, med hjälp av pulserna från rörelsesensorn.

24) Funktionen för mätning av hastigheten ska dessutom tillhandahålla informationen oavsett om fordonet är i rörelse eller om det är stillastående. Fordonet ska anses vara i rörelse så snart som funktionen känner av mer än 1 imp/sek under minst fem sekunder från rörelsesensorn och i annat fall ska fordonet anses vara stillastående.

25) Anordningar som visar hastighet (hastighetsmätare) och sammanlagd tillryggalagd sträcka (vägmätare) som installerats i ett fordon som utrustats med en färdskrivare som överensstämmer med bestämmelserna i denna förordning ska uppfylla de krav i fråga om största tillåtna toleranser (se avsnitt 3.2.1 och 3.2.2) som anges i denna bilaga.

26) För att upptäcka manipulering av rörelsedata ska information från rörelsesensorn bekräftas av information om fordonets rörelse som genereras från GNSS-mottagaren, och frivilligt även från en eller flera andra källor som är oberoende av rörelsesensorn.

27) Denna funktion ska mäta fordonets position för att möjliggöra automatisk registrering av

— positioner där föraren och/eller medföraren påbörjar dagens arbetsperioder,

— positioner där förarens sammanhängande körtid uppgår till en multipel av tre timmar,

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

3.2.1 *Mätning av tillryggalagd vägsträcka*

28) Tillryggalagd sträcka får mätas och registreras antingen

— genom att körning framåt och bakåt slås samman, eller

— genom att endast körning framåt räknas.

29) Färdskrivaren ska mäta sträckor från 0 till 9 999 999,9 km.

▼B

30) Den uppmätta sträckan ska ligga inom följande toleranser (sträckor på minst 1 000 m):

— ±1 procent före installation.

— ±2 procent vid installation och periodisk besiktning.

— ±4 procent i drift.

31) Uppmätta sträckor ska ha en upplösning som är bättre än eller lika med 0,1 km.

3.2.2 *Hastighetsmätning*

32) Färdskrivaren ska mäta hastigheter från 0 till 220 km/h.

33) För att säkerställa en största tillåtna tolerans för visad hastighet av ± 6 km/h i drift, och med hänsyn till

— en tolerans av ± 2 km/h för variationer i indata (däckvariationer, …),

— en tolerans av ± 1 km/h för mätningar som gjorts vid montering eller periodisk besiktning,

ska färdskrivaren för hastigheter mellan 20 och 180 km/h, och för karakteristiska koefficienter hos fordonet på mellan 4 000 and 25 000 imp/km, mäta hastigheten med en tolerans av ± 1 km/h (vid konstant hastighet).

Anmärkning: Upplösningen för datalagringen ger en ytterligare tolerans av ± 0,5 km/h för hastigheter som lagras av färdskrivaren.

34) Hastigheten ska mätas korrekt inom de normala toleranserna inom två sekunder från det att en hastighetsändring har avslutats, när hastigheten har ändrats med upp till 2 m/s^2.

35) Uppmätta hastigheter ska ha en upplösning som är bättre än eller lika med 1 km/h.

3.2.3 *Positionsmätning*

36) Färdskrivaren ska mäta fordonets absoluta position med hjälp av GNSS-mottagaren.

37) Den absoluta positionen ska mätas som geografiska koordinater för latitud och longitud, uttryckta i grader och minuter och med en upplösning av 0,1 minut.

3.3 **Tidmätning**

38) Funktionen för tidmätning ska kontinuerligt mäta och digitalt tillhandahålla UTC-datum och UTC-tid.

39) UTC-datum och UTC-tid ska användas för datering i färdskrivarens alla funktioner (registrering, datautbyte) och för samtliga utskrifter som anges i tillägg 4 om utskrifter.

40) Det ska vara möjligt att justera den tid som visas på bildskärmen i steg om halva timmar så att lokal tid kan visas. Enbart negativa eller positiva multiplar av halva timmar ska tillåtas.

41) Tidsavvikelsen från UTC ska vara mindre än ±2 sekunder per dag under de förhållanden som gäller för typgodkännande, och utan någon tidsinställning.

▼B

42) Uppmätt tid ska ha en upplösning som är bättre än eller lika med 1 sekund.

43) Tidmätningen ska inte påverkas av externa avbrott av strömtillförseln som är kortare än 12 månader under de förhållanden som gäller för typgodkännande.

3.4 **Övervakning av föraraktiviteter**

44) Denna funktion ska ständigt och separat övervaka en förares och en medförares aktiviteter.

45) Förarens aktiviteter ska delas upp i körning (DRIVING), annat arbete (WORK), tillgänglighet (AVAILABILITY) och rast/vila (BREAK/REST).

46) Det ska vara möjligt för föraren och/eller medföraren att manuellt välja annat arbete (WORK), tillgänglighet (AVAILABILITY) eller rast/vila (BREAK/REST).

47) När fordonet befinner sig i rörelse ska körning (DRIVING) väljas automatiskt för föraren och tillgänglighet (AVAILABILITY) väljas automatiskt för medföraren.

48) När fordonet stannar ska annat arbete (WORK) väljas automatiskt för föraren.

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)).

50) Denna funktion ska tillhandahålla aktivitetsändringar till registreringsfunktionerna med en upplösning av en minut.

51) För en viss kalenderminut ska hela minuten betraktas som körning (DRIVING) om aktiviteten både inom den närmast föregående och den närmast efterkommande minuten har registrerats som körning (DRIVING).

52) För en viss kalenderminut som inte betraktas som körning (DRIVING) enligt krav 51 ska hela minuten betraktas som samma typ av aktivitet som den längsta sammanhängande aktiviteten inom den minuten (eller den senaste av lika långa aktiviteter).

53) Denna funktion ska dessutom ständigt övervaka förarens sammanhängande körtid och sammanlagda avbrottstid.

3.5 **Övervakning av körningsstatus**

54) Denna funktion ska ständigt och automatiskt övervaka körningens status.

55) Körningsstatus ”flera förare” (CREW) ska väljas när två giltiga förarkort sätts in i färdskrivaren, körningsstatus ”ensam förare” (SINGLE) ska väljas i alla andra fall.

3.6 **Förarens angivelser**

3.6.1 *Angivelse av de platser där dagens arbetsperioder påbörjas och/eller avslutas*

56) Denna funktion ska göra det möjligt att ange de platser där dagens arbetsperioder påbörjas och/eller avslutas för en förare och/eller en medförare.

▼B

57) Platser definieras som landet, och där så är tillämpligt regionen, och anges eller bekräftas manuellt.

58) När ett förarkort tas ut ska färdskrivaren uppmana (med)föraren att ange ”den plats där arbetsperioden avslutas”.

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

60) Det ska vara möjligt att mata in de platser där dagens arbetsperioder påbörjas och/eller avslutas genom kommandon i menyerna. Om mer än en sådan inmatning görs inom en kalenderminut ska endast den senast inmatade angivelsen av var dagens arbetsperioder påbörjas och/eller avslutas lagras i registret.

3.6.2 *Manuell angivelse av föraraktiviteter och förarens samtycke avseende ITS-gränssnitt*

61) När förarkortet (eller verkstadskortet) sätts in, och endast då, ska färdskrivaren tillåta manuell angivelse av aktiviteter. I samband med manuella angivelser ska aktiviteter anges i lokal tid och med lokala datum för den tidszon (UTC-tidsskillnad) som vid det tillfället är inställd för fordonsenheten.

När förarkortet (eller verkstadskortet) sätts in ska färdskrivaren påminna kortinnehavaren om

— datum och tidpunkt då kortet senast togs ut,

— den lokala tidsskillnad som för närvarande är inställd för fordonsenheten (frivilligt).

När ett visst förarkort eller verkstadskort som är okänt för fordonsenheten sätts in för första gången ska kortinnehavaren uppmanas att ge sitt samtycke till att personuppgifter som finns i färdskrivaren tillhandahålls via det frivilliga ITS-gränssnittet.

Förarens eller verkstadens samtycke kan när som helst aktiveras eller avaktiveras via menykommandon, förutsatt att förarrespektive verkstadskortet är insatt.

Det ska gå att mata in aktiviteter med följande begränsningar:

— Aktivitetstypen ska vara annat arbete (WORK), tillgänglighet (AVAILABILITY) eller rast/vila (BREAK/REST).

— Start- och sluttiden för varje aktivitet får endast ligga inom perioden från senaste uttag av kort till aktuell insättning.

— Aktiviteterna får inte överlappa varandra i tid.

Det ska vid behov gå att göra manuella angivelser första gången ett oanvänt förarkort (eller verkstadskort) sätts in.

▼B

Förfarandet för manuella angivelser av aktiviteter ska omfatta så många på varandra följande steg som krävs för att ange typen av aktivitet samt start- och sluttid för varje aktivitet. Föraren ska för varje del av perioden från senaste uttag av kort till aktuell insättning kunna välja att inte ange någon aktivitet.

I samband med manuella angivelser när kortet sätts in ska kortinnehavaren, om tillämpligt, ha möjlighet att ange

— den plats där en föregående arbetsperiod avslutades, kopplad till den relevanta tidpunkten (som därmed skriver över det som angavs när kortet senast togs ut),

— den plats där den innevarande arbetsperioden påbörjas, kopplad till den relevanta tidpunkten.

Om kortinnehavaren inte anger någon plats där arbetspasset påbörjas eller avslutas, i form av en manuell angivelse i samband med att kortet sätts in, ska detta betraktas som att kortinnehavarens arbetspass inte har ändrats sedan kortet senast togs ut. Nästa angivelse av en plats där en föregående arbetsperiod avslutades ska då skriva över den tillfälliga angivelsen som gjordes när kortet senast togs ut.

Om en plats anges ska den registreras på det relevanta färdskrivarkortet.

Manuella angivelser ska avbrytas om

— kortet tas ut, eller

— fordonet rör sig och kortet finns i förarens kortplats.

Avbrott får göras av andra skäl, t.ex. efter en viss period av inaktivitet från användarens sida. Om manuella angivelser avbryts ska färdskrivaren bekräfta alla fullständiga angivelser av plats och aktivitet (dvs. otvetydiga uppgifter om plats och tidpunkt eller om aktivitetstyp, start- och sluttidpunkt) som redan har gjorts.

Om ett andra förar- eller verkstadskort sätts in under pågående manuella angivelser av aktiviteter för ett tidigare insatt kort ska de manuella angivelserna för det första kortet avslutas innan manuella angivelser för det andra kortet påbörjas.

Kortinnehavaren ska ha möjlighet att göra manuella angivelser enligt följande minimiförfarande:

— Ange aktiviteter manuellt i kronologisk ordning för perioden från senaste uttag av kort till aktuell insättning.

— Starttiden för den första aktiviteten ska ställas in till tidpunkten då kortet togs ut. För varje efterföljande angivelse ska starttiden förinställas så att den följer omedelbart på sluttiden för föregående angivelse. Aktivitetstyp och sluttid ska anges för varje aktivitet.

▼B

Förfarandet avslutas när sluttiden för en manuellt angiven aktivitet är densamma som tidpunkten för insättning av kortet. Färdskrivaren kan därefter eventuellt göra det möjligt för kortinnehavaren att ändra de aktiviteter som angivits manuellt, innan de bekräftas genom ett särskilt kommando. Därefter ska sådana ändringar inte längre vara möjliga.

3.6.3 *Angivelse av särskilda omständigheter*

62) Färdskrivaren ska göra det möjligt för föraren att i realtid ange följande två särskilda omständigheter:

— ”omfattas ej” (OUT OF SCOPE) (början, slut).

— ”transport med färja/tåg” (FERRY/TRAIN CROSSING) (början, slut).

Transport med färja/tåg (FERRY/TRAIN CROSSING) får inte äga rum om en omständighet av typen ”omfattas ej” (OUT OF SCOPE) påbörjats.

En påbörjad omständighet av typen ”omfattas ej” (OUT OF SCOPE) måste automatiskt avslutas av färdskrivaren om ett förarkort sätts in eller tas ut.

En påbörjad omständighet av typen ”omfattas ej” (OUT OF SCOPE) ska förhindra följande händelser och varningar:

— Körning utan korrekt kort.

— Varningar i samband med sammanhängande körtid.

Startmarkeringen för ”transport med färja/tåg” (FERRY/TRAIN CROSSING) ska anges innan motorn stängs av på färjan eller tåget.

En inledd ”transport med färja/tåg” (FERRY/TRAIN CROSSING) måste avslutas när något av följande inträffar:

— Föraren avslutar manuellt ”transport med färja/tåg” (FERRY/TRAIN CROSSING).

— Föraren tar ut sitt kort.

En inledd ”transport med färja/tåg” (FERRY/TRAIN CROSSING) ska avslutas när den inte längre är giltig, på grundval av de regler som anges i förordning (EG) nr 561/2006.

3.7 **Hantering av företagslås**

63) Denna funktion ska göra det möjligt att hantera de lås som ett företag har för att begränsa andras tillgång till data i företagsläge.

64) Företagslås utgörs av tidpunkt/datum för start (låsning) och tidpunkt/datum för avslutande (öppning) som kopplas till det företag som identifieras med företagskortets nummer (vid låsning).

65) Låsning och öppning kan endast ske i realtid.

66) Öppning ska endast vara möjligt för det företag som låst (vilket anges genom de 13 första siffrorna i företagskortets nummer), eller

67) öppning ska ske automatiskt om ett annat företag låser.

▼B

68) Om ett företag låser och det föregående låset var för samma företag antas att det föregående låset inte har öppnats utan fortfarande är låst.

3.8 **Övervakning av kontrollaktiviteter**

69) Denna funktion ska övervaka kontrollaktiviteterna visning (DISPLAYING), utskrift (PRINTING), fordonsenhet (VU), överföring av data (DOWNLOADING) och kalibrering på väg (ROADSIDE CALIBRATION) då dessa sker i kontrollläge.

70) Denna funktion ska även övervaka kontroll av hastighetsöverträdelse (OVER SPEEDING CONTROL) i kontrolläge. En kontroll av hastighetsöverträdelse anses ha ägt rum när utskriften ”hastighetsöverträdelse” i kontrolläge har sänts till skrivaren eller till bildskärmen, eller när data om ”händelser och fel” har överförts från fordonsenhetens dataminne.

3.9 **Upptäckt av händelser och/eller fel**

71) Denna funktion ska upptäcka nedanstående händelser och/eller fel.

3.9.1 *Insättning av ett ogiltigt kort (händelse, ”Insertion of a non-valid card”)*

72) Denna händelse ska utlösas om ett ogiltigt kort sätts in, om ett redan ersatt förarkort sätts in och/eller när ett insatt giltigt kort upphör att gälla.

3.9.2 *Kortkonflikt (händelse, ”Card conflict”)*

73) Denna händelse ska utlösas om någon av de kombinationer av giltiga kort som är markerade med X i nedanstående tabell uppstår.

Kortkonflikt		Förarens kortplats				
		Inget kort	Förarkort	Kontrollkort	Verkstadskort	Företagskort
Medförarens kortplats	Inget kort					
	Förarkort				X	
	Kontrollkort			X	X	X
	Verkstadskort		X	X	X	X
	Företagskort			X	X	X

3.9.3 *Överlappning av tider (händelse, ”Time overlap”)*

74) Denna funktion ska utlösas när datum/tidpunkt för det senaste uttaget av ett förarkort, såsom det läses från detta kort, är senare än aktuellt datum/tidpunkt i den färdskrivare i vilken kortet sätts in.

3.9.4 *Körning utan korrekt kort (händelse, ”Driving without an appropriate card”)*

75) Denna händelse ska utlösas när någon av de giltiga kombinationer av färdskrivarkort som är markerade med X i nedanstående tabell uppstår, när föraraktiviteten ändras till körning (DRIVING) eller vid ändring av funktionsläge när föraraktiviteten är körning (DRIVING).

▼B

Körning utan korrekt kort (*Driving without an appropriate card*)		Förarens kortplats				
		Inget (eller ogiltigt) kort	Förarkort	Kontrollkort	Verkstadskort	Företagskort
Medförarens kortplats	Inget (eller ogiltigt) kort	X		X		X
	Förarkort	X		X	X	X
	Kontrollkort	X	X	X	X	X
	Verkstadskort	X	X	X		X
	Företagskort	X	X	X	X	X

3.9.5 *Insättning av kort vid körning (händelse, ”Card insertion while driving”)*

76) Denna händelse ska utlösas om ett färdskrivarkort sätts in i en kortplats när föraraktiviteten är körning (DRIVING).

3.9.6 *Senaste kortsession ej korrekt avslutad (händelse, ”Last card session not correctly closed”)*

77) Denna händelse ska utlösas om färdskrivaren vid insättning av ett kort upptäcker att föregående kortsession, trots bestämmelserna i punkt 3.1, inte har avslutats korrekt (kortet har tagits ut innan alla relevanta data har lagrats på kortet). Denna händelse gäller endast förarkort och verkstadskort.

3.9.7 *Hastighetsöverträdelse (händelse, ”Over speeding”)*

78) Denna händelse ska utlösas vid varje hastighetsöverträdelse.

3.9.8 *Avbrott i strömtillförsel (händelse, ”Power supply interruption”)*

79) Denna händelse ska utlösas när kalibrerings- eller kontrolläget inte är inställt om strömtillförseln till rörelsesensorn och/eller fordonsenheten är avbruten under mer än 200 millisekunder. Tröskelvärdet för avbrott ska fastställas av tillverkaren. Sänkt strömtillförsel på grund av att fordonets motor startas ska inte utlösa denna händelse.

3.9.9 *Fel i kommunikation med kommunikationsanordning för fjärravläsning (händelse, ”Communication error with the remote communication facility”)*

80) Denna händelse ska utlösas **när kalibreringsläget inte är inställt** om kommunikationsanordningen för fjärravläsning inte kvitterar att den lyckats ta emot data för fjärrkommunikation som sänts från fordonsenheten vid mer än tre försök.

3.9.10 *Positionsinformation från GNSS-mottagare saknas (händelse, ”Absence of position information from GNSS receiver”)*

81) Denna händelse ska utlösas **när kalibreringsläget inte är inställt** om positionsinformation från GNSS-mottagaren (intern eller extern) saknas under mer än tre timmars sammanlagd körtid.

3.9.11 *Fel i kommunikation med extern GNSS-anordning (händelse, ”Communication error with the external GNSS facility”)*

82) Denna händelse ska utlösas **när kalibreringsläget inte är inställt** om kommunikationen mellan den externa GNSS-anordningen och fordonsenheten är avbruten under mer än 20 sammanhängande minuter när fordonet är i rörelse.

▼B

3.9.12 *Fel i rörelsedata (händelse, ”Motion data error”)*

83) Denna händelse ska utlösas **när kalibreringsläget inte är inställt** vid avbrott av det normala dataflödet mellan rörelsesensorn och fordonsenheten och/eller vid integritetsfel eller autentiseringsfel under utväxling av data mellan rörelsesensorn och fordonsenheten.

3.9.13 *Konflikt i fordonets rörelsedata (händelse, ”Vehicle motion conflict”)*

84) Denna händelse ska utlösas **när kalibreringsläget inte är inställt** om den rörelseinformation som beräknas utifrån rörelsesensorn motsägs av rörelseinformation som beräknas utifrån GNSS-mottagaren eller utifrån den externa GNSS-anordningen och, frivilligt, utifrån andra oberoende källor, såsom anges i tillägg 12. Denna händelse ska inte utlösas under transport med färja/tåg, under omständigheten ”omfattas ej” eller när positionsinformation från GNSS-mottagaren inte är tillgänglig.

3.9.14 *Försök till säkerhetsöverträdelse (händelse, ”Security breach attempt”)*

85) Denna händelse ska utlösas vid varje övrig händelse som påverkar säkerheten i rörelsesensorn och/eller fordonsenheten och/eller den externa GNSS-anordningen, såsom krävs i tillägg 10, när kalibreringsläget inte är inställt.

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 tidmätningsfunktion och den tid som har sitt ursprung i GNSS-mottagaren. Denna händelse registreras tillsammans 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 de föregående 30 dagarna. Den automatiska tidsinställningen ska dock göras när positionsinformation från GNSS-mottagaren är tillgänglig igen.

3.9.16 *Kortfel (”Card”)*

87) Detta fel ska utlösas om ett fel på ett färdskrivarkort uppstår under drift.

3.9.17 *Färdskrivarfel (”Recording equipment”)*

88) Detta fel ska utlösas vid något av följande fel om kalibreringsläget inte är inställt:

— Internt fel i fordonsenheten.

— Skrivarfel.

— Bildskärmsfel.

— Överföringsfel.

— Sensorfel.

— Fel i GNSS-mottagare eller extern GNSS-anordning.

— Fel i kommunikationsanordning för fjärravläsning.

▼B

3.10 **Inbyggd provning och självprovning**

89) Färdskrivaren ska upptäcka fel genom självprovning och inbyggd provning, i enlighet med nedanstående tabell.

Enhet som provas	Självprovning	Inbyggd provning
Programvara		Integritet
Dataminne	Åtkomst	Tillträde, dataintegritet
Kortläsare	Åtkomst	Åtkomst
Knappsats		Manuell kontroll
Skrivare	(Bestäms av tillverkare)	Utskrift
Bildskärm		Visuell kontroll
Överföring (utförs endast vid överföring)	Korrekt drift	
Sensor	Korrekt drift	Korrekt drift
Kommunikationsanordning för fjärravläsning	Korrekt drift	Korrekt drift
GNSS-anordning	Korrekt drift	Korrekt drift

3.11 **Avläsning från dataminne**

90) Färdskrivaren ska kunna läsa alla data som finns lagrade i dess dataminne.

3.12 **Registrering och lagring i dataminne**

Under denna punkt gäller följande:

— ”365 dagar”: 365 kalenderdagar av genomsnittlig föraraktivitet i ett fordon. Genomsnittlig aktivitet per dag i ett fordon: Minst sex förare eller medförare, sex cykler med insättning och uttag av kort och 256 aktivitetsändringar. ”365 dagar” inbegriper därför åtminstone 2 190 (med)förare, 2 190 cykler med insättning och uttag av kort och 93 440 aktivitetsändringar.

— Genomsnittligt antal positioner per dag: Minst sex positioner där en arbetsperiod påbörjas, sex positioner där förarens sammanhängande körtid uppgår till en multipel av tre timmar och sex positioner där en arbetsperiod avslutas, vilket innebär att ”365 dagar” inbegriper minst 6 570 positioner.

— Tider registreras med en upplösning av en (1) minut, om inte annat anges.

— Vägmätarvärden registreras med en upplösning av en (1) kilometer.

— Hastigheter registreras med en upplösning av en (1) km/h.

— Positioner (latitud och longitud) registreras i grader och minuter med en upplösning av 0,1 minut, och med tillhörande GNSS-precision och låsningstid (*acquisition time*).

▼B

91) Data som finns lagrade i dataminnet ska inte påverkas av externa avbrott av strömtillförseln som är kortare än 12 månader under de förhållanden som gäller för typgodkännande. Dessutom får data som lagras i den externa kommunikationsanordningen för fjärravläsning, såsom definieras i tillägg 14, inte påverkas av ett avbrott i strömtillförseln som är kortare än 28 dagar.

92) Färdskrivaren ska i sitt dataminne direkt eller indirekt kunna registrera och lagra nedanstående information.

3.12.1 *Data för identifiering av utrustning*

3.12.1.1 Data för identifiering av fordonsenhet

93) Det ska gå att lagra följande data för identifiering av fordonsenheten i färdskrivarens dataminne:

— Tillverkarens namn.

— Tillverkarens adress.

— Artikelnummer.

— Serienummer.

— Generation.

— Förmåga att hantera första generationens färdskrivarkort.

— Programvarans versionsnummer.

— Datum för installation av programvaruversionen.

— Utrustningens tillverkningsår.

— Typgodkännandenummer.

94) Tillverkaren av fordonsenheten registrerar och lagrar data för identifiering av fordonsenheten en gång för alla, utom när det gäller programvarudata och typgodkännandenummer, som får ändras om programvaran uppgraderas, och förmågan att hantera första generationens färdskrivarkort.

3.12.1.2 Data för identifiering av rörelsesensor

95) Det ska gå att lagra följande identifieringsdata i rörelsesensorns minne:

— Tillverkarens namn.

— Serienummer.

— Typgodkännandenummer.

— Inbyggd identifiering av säkerhetskomponent (t.ex. artikelnummer för internt chip eller intern processor).

— Identifiering av operativsystem (t.ex. programvarans versionsnummer).

96) Tillverkaren av rörelsesensorn registrerar och lagrar data för identifiering av rörelsesensorn en gång för alla i rörelsesensorn.

97) Färdskrivaren ska i sitt dataminne kunna registrera och lagra nedanstående data med avseende på de senaste 20 parningarna med rörelsesensorer (om flera parningar utförs under en kalenderdag gäller detta endast den första och den sista parningen det dygnet).

▼B

Följande data ska registreras för var och en av dessa parningar:

— Data för identifiering av rörelsesensorn.

— Serienummer.

— Typgodkännandenummer.

— Data om rörelsesensorns parning.

— Datum för parning.

3.12.1.3 Data för identifiering av globalt system för satellitnavigering (GNSS).

98) Det ska gå att lagra följande identifieringsdata i den externa GNSS-anordningens minne:

— Tillverkarens namn.

— Serienummer.

— Typgodkännandenummer.

— Inbyggd identifiering av säkerhetskomponent (t.ex. artikelnummer för internt chip eller intern processor).

— Identifiering av operativsystem (t.ex. programvarans versionsnummer).

99) Tillverkaren av den externa GNSS-anordningen registrerar och lagrar data för identifiering en gång för alla i den externa GNSS-anordningen.

100) Färdskrivaren ska i sitt dataminne kunna registrera och lagra nedanstående data med avseende på de senaste 20 kopplingarna med externa GNSS-anordningar (om flera kopplingar utförs under en kalenderdag gäller detta endast den första och den sista kopplingen det dygnet).

Följande data ska registreras för var och en av dessa kopplingar:

— Data för identifiering av den externa GNSS-anordningen.

— Serienummer.

— Typgodkännandenummer.

— Data om den externa GNSS-anordningens koppling.

— Datum för koppling.

3.12.2 *Nycklar och certifikat*

101) Färdskrivaren ska kunna lagra ett antal kryptografiska nycklar och certifikat, såsom anges i tillägg 11 del A och del B.

3.12.3 *Data om insättning och uttag av förarkort och verkstadskort*

102) För varje cykel med insättning och uttag av förarkort eller verkstadskort i utrustningen ska färdskrivaren registrera och lagra följande data i sitt dataminne:

— Kortinnehavarens efternamn och förnamn såsom de lagrats på kortet.

— Kortnummer, utfärdande medlemsstat och sista giltighetsdag såsom de lagrats på kortet.

— Kortets generation.

▼B

— Datum och tidpunkt för insättning.

— Vägmätarvärde när kortet sattes in.

— Den kortplats som kortet sätts in i.

— Datum och tidpunkt för uttag.

— Vägmätarvärde när kortet togs ut.

— Följande information om det föregående fordon som föraren använt, såsom den lagrats på kortet:

  — Fordonets registreringsnummer (VRN) och registrerande medlemsstat.

  — Fordonsenhetens generation (när sådan finns tillgänglig).

  — Datum och tidpunkt när kortet togs ut.

— En markering som visar om innehavaren vid insättningen av kortet har angivit aktiviteter manuellt.

103) Det ska gå att lagra dessa data i dataminnet i minst 365 dagar.

104) När lagringskapaciteten har utnyttjats till fullo ska nya data ersätta de data som är äldst.

3.12.4 *Data om föraraktiviteter*

105) Färdskrivaren ska, när föraren och/eller medföraren ändrar aktivitet, och/eller när körningsstatusen ändras, och/eller när ett förarkort eller verkstadskort sätts in eller tas ut, registrera och lagra följande i sitt dataminne:

— Körningsstatus (flera förare (CREW), ensam förare (SINGLE)).

— Kortplats (förare (DRIVER), medförare (CO-DRIVER)).

— Kortstatus (insatt (INSERTED), ej insatt (NOT INSERTED)).

— Aktivitet (körning (DRIVING), tillgänglighet (AVAILABILITY), annat arbete (WORK), rast/vila (BREAK/REST)).

— Datum och tidpunkt för ändringen.

”Insatt” (INSERTED) innebär att ett giltigt förarkort eller verkstadskort är insatt i kortplatsen. ”Ej insatt” (NOT INSERTED) innebär motsatsen, dvs. att något giltigt förarkort eller verkstadskort inte är insatt i kortplatsen (exempelvis är ett företagskort eller inget kort insatt).

Aktivitetsdata som en förare har angivit manuellt registreras inte i dataminnet.

106) Det ska gå att lagra data om föraraktiviteter för minst 365 dagar i dataminnet.

107) När lagringskapaciteten har utnyttjats till fullo ska nya data ersätta de data som är äldst.

▼B

3.12.5 *Platser och positioner där dagens arbetsperioder påbörjas eller avslutas och/eller där tre timmars sammanhängande 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 förarens sammanhängande körtid uppgår till en multipel av tre timmar.

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

109) När fordonets position inte är tillgänglig via GNSS-mottagaren vid dessa tillfällen ska färdskrivaren använda den senaste tillgängliga positionen och tillhörande datum och tidpunkt.

110) Färdskrivaren ska registrera och lagra följande i sitt dataminne, tillsammans med varje plats eller position:

— (Med)förarens kortnummer och medlemsstat som utfärdat kortet.

— Kortets generation.

— Datum och tidpunkt för angivelsen.

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

— Aktuell GNSS-precision, samt datum och tidpunkt i förekommande fall.

— Fordonets vägmätarställning.

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

112) När lagringskapaciteten har utnyttjats till fullo ska nya data ersätta de data som är äldst.

3.12.6 *Vägmätardata*

113) Färdskrivaren ska vid midnatt varje kalenderdag registrera fordonets vägmätarställning och motsvarande datum i sitt dataminne.

114) Det ska gå att lagra vägmätarvärden vid midnatt i minst 365 dagar.

115) När lagringskapaciteten har utnyttjats till fullo ska nya data ersätta de data som är äldst.

3.12.7 *Detaljerade hastighetsdata*

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 har körts.

3.12.8 *Händelsedata*

För de data som avses i denna punkt ska tidpunkten registreras med en upplösning av en (1) sekund.

117) Färdskrivaren ska i sitt dataminne registrera och lagra nedanstående data för varje händelse som upptäcks i enlighet med nedanstående lagringsregler.

▼B

Händelse	Lagringsregler	Data som ska registreras per händelse
Insättning av ett ogiltigt kort (*Insertion of a non-valid card*)	— De senaste tio händelserna	— Datum och tidpunkt för händelsen — Korttyp, kortnummer, utfärdande medlemsstat och generation för det kort som orsakat händelsen — Antal liknande händelser samma dag
Kortkonflikt (*Card conflict*)	— De senaste tio händelserna	— Datum och tidpunkt för händelsens början — Datum och tidpunkt för händelsens slut — Korttyp, kortnummer, utfärdande medlemsstat och generation för de två kort som orsakat konflikten
Körning utan korrekt kort (*Driving without an appropriate card*)	— Den långvarigaste händelsen för vart och ett av de senaste tio dygn där händelsen inträffat — De fem långvarigaste händelserna under de senaste 365 dygnen	— 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
Insättning av kort under körning (*Card insertion while driving*)	— Den senaste händelsen för vart och ett av de senaste tio dygn där händelsen inträffat	— Datum och tidpunkt för händelsen — Korttyp, kortnummer, utfärdande medlemsstat och generation — Antal liknande händelser samma dag

Senaste kortsession ej korrekt avslutad (*Last card session not correctly closed*)	— De senaste tio händelserna	— Datum och tidpunkt för insättning av kort
		— Korttyp, kortnummer, utfärdande medlemsstat och generation
		— Data om senaste session enligt avläsning från kortet:
		  — Datum och tidpunkt för insättning av kort
		  — Fordonets registreringsnummer, registrerande medlemsstat och fordonsenhetens generation

Hastighetsöverträdelse (*Over speeding*) (1)	— Den mest allvarliga händelsen för vart och ett av de senaste tio dygn där händelsen inträffat (dvs. den med högsta medelhastighet) — De fem mest allvarliga händelserna under de senaste 365 dygnen — Den första händelsen som inträffat efter den senaste kalibreringen	— Datum och tidpunkt för händelsens början — Datum och tidpunkt för händelsens slut — Högsta hastighet som uppmätts under händelsen — Aritmetisk medelhastighet som uppmätts under händelsen — Korttyp, kortnummer, utfärdande medlemsstat och generation för förarkortet (i förekommande fall) — Antal liknande händelser samma dag

▼B

Händelse	Lagringsregler	Data som ska registreras per händelse
Avbrott i strömtillförseln (*Power supply interruption*) (2)	— Den långvarigaste händelsen för vart och ett av de senaste tio dygn där händelsen inträffat — De fem långvarigaste händelserna under de senaste 365 dygnen	— 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
Fel i kommunikation med kommunikationsanordning för fjärravläsning (*Communication error with the remote communication facility*)	— Den långvarigaste händelsen för vart och ett av de senaste tio dygn där händelsen inträffat — De fem långvarigaste händelserna under de senaste 365 dygnen	— 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
Positionsinformation från GNSS-mottagare saknas (*Absence of position information from GNSS receiver*)	— Den långvarigaste händelsen för vart och ett av de senaste tio dygn där händelsen inträffat — De fem långvarigaste händelserna under de senaste 365 dygnen	— 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
Fel i rörelsedata (*Motion data error*)	— Den långvarigaste händelsen för vart och ett av de senaste tio dygn där händelsen inträffat — De fem långvarigaste händelserna under de senaste 365 dygnen	— 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
Konflikt i fordonets rörelsedata (*Vehicle motion conflict*)	— Den långvarigaste händelsen för vart och ett av de senaste tio dygn där händelsen inträffat — De fem långvarigaste händelserna under de senaste 365 dygnen	— 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
Försök till säkerhetsöverträdelse (*Security breach attempt*)	— De tio senaste händelserna per händelsetyp	— Datum och tidpunkt för händelsens början — Datum och tidpunkt för händelsens slut (om det är relevant) — Korttyp, kortnummer, utfärdande medlemsstat och generation för ett eventuellt kort som var insatt vid händelsens början och/eller slut — Händelsetyp

▼B

Händelse	Lagringsregler	Data som ska registreras per händelse
Tidskonflikt (*Time conflict*)	— Den långvarigaste händelsen för vart och ett av de senaste tio dygn där händelsen inträffat — De fem långvarigaste händelserna under de senaste 365 dygnen	— Datum och tidpunkt enligt färdskrivaren — Aktuellt UTC-datum och aktuell UTC-tid — Korttyp, kortnummer, utfärdande medlemsstat och generation för ett eventuellt kort som var insatt vid händelsens början och/eller slut — Antal liknande händelser samma dag

(1) Färdskrivaren ska även registrera och lagra följande i sitt dataminne:

— Datum och tidpunkt för den senaste kontrollen av hastighetsöverträdelse.

— Datum och tidpunkt för den första hastighetsöverträdelsen efter denna kontroll av hastighetsöverträdelse.

— Antalet händelser av typen hastighetsöverträdelse sedan den senaste kontrollen av hastighetsöverträdelse.

(2) Dessa data kan endast registreras när strömtillförseln återställs, och tidpunkter får anges på minuten när.

3.12.9 *Data om fel*

För de data som avses i denna punkt ska tidpunkten registreras med en upplösning av en (1) sekund.

118) Färdskrivaren ska i sitt dataminne försöka registrera och lagra nedanstående data för varje fel som upptäcks i enlighet med nedanstående lagringsregler.

Fel	Lagringsregler	Data som ska registreras per fel
Kortfel	— De tio senaste förarkortsfelen	— Datum och tidpunkt för felets början — Datum och tidpunkt för felets slut — Korttyp, kortnummer, utfärdande medlemsstat och generation
Färdskrivarfel	— De tio senaste felen för varje typ av fel — Det första felet efter den senaste kalibreringen	— Datum och tidpunkt för felets början — Datum och tidpunkt för felets slut — Typ av fel — Korttyp, kortnummer, utfärdande medlemsstat och generation för ett eventuellt kort som var insatt vid felets början och/eller slut

3.12.10 *Kalibreringsdata*

119) Färdskrivaren ska registrera och lagra data med avseende på följande i sitt dataminne:

— Kända kalibreringsparametrar vid aktivering.

▼B

— Första kalibrering efter aktivering.

— Första kalibrering i det nuvarande fordonet (enligt fordonets identifieringsnummer (VIN)).

— De 20 senaste kalibreringarna (om flera kalibreringar görs under en kalenderdag gäller detta endast den första och den sista kalibreringen det dygnet).

120) Följande data ska registreras för var och en av dessa kalibreringar:

— Syfte med kalibreringen (aktivering, första installation, installation, periodisk besiktning).

— Verkstadens namn och adress.

— Verkstadskortets nummer, medlemsstat som utfärdat kortet och kortets sista giltighetsdag.

— Fordonsidentifiering.

— Uppdaterade eller bekräftade parametrar (w, k, l, däcksdimension, den hastighetsbegränsande anordningens inställning, vägmätare (gamla och nya värden), datum och tidpunkt (gamla och nya värden).

— Typer och identifierare för samtliga befintliga plomberingar.

121) Färdskrivaren ska dessutom registrera eventuell förmåga att hantera första generationens färdskrivarkort (dvs. om denna funktion fortfarande är aktiverad eller inte) och lagra detta i sitt dataminne.

122) Rörelsesensorn ska registrera följande data om installationen av rörelsesensorn och lagra dem i sitt minne:

— Första parning med en fordonsenhet (VU) (datum, tidpunkt, fordonsenhetens typgodkännandenummer och serienummer).

— Senaste parning med en fordonsenhet (VU) (datum, tidpunkt, fordonsenhetens typgodkännandenummer och serienummer).

123) Den externa GNSS-anordningen ska registrera följande data om installationen av den externa GNSS-anordningen och lagra dem i sitt minne:

— Första koppling med en fordonsenhet (VU) (datum, tidpunkt, fordonsenhetens typgodkännandenummer och serienummer).

— Senaste koppling med en fordonsenhet (VU) (datum, tidpunkt, fordonsenhetens typgodkännandenummer och serienummer).

3.12.11 *Data om tidsinställning*

124) Färdskrivaren ska registrera data som är relevanta för tidsinställningar som utförts i kalibreringsläge, men inte vid en normal kalibrering (se def. f) och lagra dem i sitt dataminne:

— Senaste tidsinställning.

— De fem mest omfattande tidsinställningarna.

125) Följande data ska registreras för var och en av dessa tidsinställningar:

— Datum och tidpunkt, gammalt värde.

— Datum och tidpunkt, nytt värde.

— Verkstadens namn och adress.

— Verkstadskortets nummer, utfärdande medlemsstat, generation och sista giltighetsdag.

▼B

3.12.12 *Data om kontrollaktiviteter*

126) Färdskrivaren ska i sitt dataminne registrera och lagra följande data med avseende på de senaste 20 kontrollaktiviteterna:

— Datum och tidpunkt för kontrollen.

— Kontrollkortets nummer, utfärdande medlemsstat och generation.

— Kontrolltyp (visning och/eller utskrift och/eller överföring av data från fordonsenhet och/eller överföring av data från kort och/eller kalibreringskontroll på väg).

127) Vid överföring ska även datum för tidigaste och senaste överförda dagar registreras.

3.12.13 *Data om företagslås*

128) Färdskrivaren ska i sitt dataminne registrera och lagra följande data med avseende på de 255 senaste företagslåsen:

— Datum och tidpunkt för låsning.

— Datum och tidpunkt för öppning.

— Företagskortets nummer, utfärdande medlemsstat och generation.

— Företagets namn och adress.

Data som tidigare varit låsta genom ett lås som har raderats från minnet på grund av ovanstående gräns ska betraktas som olåsta.

3.12.14 *Överföringsdata*

129) Färdskrivaren ska i sitt dataminne registrera och lagra följande data med avseende på senaste dataöverföring till externa media i företags- eller kalibreringsläge:

— Datum och tidpunkt för överföringen.

— Företagskortets eller verkstadskortets nummer, utfärdande medlemsstat och generation.

— Företagets eller verkstadens namn.

3.12.15 *Data om särskilda omständigheter*

130) Färdskrivaren ska i sitt dataminne registrera följande data med avseende på särskilda omständigheter:

— Datum och tidpunkt för angivelsen.

— Typ av särskild omständighet.

131) Det ska gå att lagra data om särskilda omständigheter i dataminnet i minst 365 dygn (under förutsättning att det i genomsnitt påbörjas och avslutas en omständighet per dygn). När lagringskapaciteten har utnyttjats till fullo ska nya data ersätta de data som är äldst.

3.12.16 *Data om färdskrivarkort*

132) Färdskrivaren ska kunna lagra följande data med avseende på de olika färdskrivarkort som använts i fordonsenheten:

— Färdskrivarkortets kortnummer och serienummer.

— Färdskrivarkortets tillverkare.

▼B

— Färdskrivarkortets typ.

— Färdskrivarkortets version.

133) Det ska gå att lagra minst 88 sådana poster i färdskrivaren.

3.13 **Avläsning från färdskrivarkort**

134) Färdskrivaren ska i förekommande fall kunna avläsa nödvändiga data från första och andra generationens färdskrivarkort för att

— identifiera korttyp, kortinnehavare, fordon som använts tidigare, datum och tidpunkt för senaste uttag av kort och den aktivitet som valdes vid det tillfället,

— kontrollera att den senaste kortsessionen avslutades korrekt,

— beräkna förarens sammanhängande körtid, sammanlagda avbrottstid och sammanlagda körtider under föregående och innevarande vecka,

— skriva ut begärda utskrifter med avseende på de data som registrerats på ett förarkort,

— överföra data från ett förarkort till externa media.

Detta krav gäller första generationens färdskrivarkort endast så länge som möjligheten att använda dem inte har tagits bort av en verkstad.

135) Vid avläsningsfel ska färdskrivaren pröva samma läskommando igen, högst tre gånger, och om detta misslyckas ska den förklara kortet felaktigt och ogiltigt.

3.14 **Registrering och lagring på färdskrivarkort**

3.14.1 *Registrering och lagring på första generationens färdskrivarkort*

136) Förutsatt att möjligheten att använda första generationens färdskrivarkort inte har tagits bort av en verkstad ska färdskrivaren registrera och lagra data på exakt samma sätt som en första generationens färdskrivare.

137) Färdskrivaren ska ställa in data om kortsessionen på förarkortet eller verkstadskortet omedelbart efter det att kortet satts in.

138) Färdskrivaren ska uppdatera de data som lagrats på giltiga förar-, verkstads- företags- och/eller kontrollkort med alla nödvändiga data för den period då kortet är insatt och som avser kortinnehavaren. De data som lagras på dessa kort specificeras i kapitel 4.

139) Färdskrivaren ska uppdatera de data om föraraktivitet och platser (i enlighet med avsnitt 4.5.3.1.9 och 4.5.3.1.11) som finns lagrade på giltiga förar- och/eller verkstadskort med de data om aktivitet och platser som kortinnehavaren anger manuellt.

140) Inga händelser som inte finns definierade för första generationens färdskrivare får lagras på förar- och verkstadskorten.

▼B

141) Uppdateringen av data på färdskrivarkort ska, vid behov och med hänsyn till kortets faktiska lagringskapacitet, ske på så sätt att senaste data ersätter äldsta data.

142) Vid skrivfel ska färdskrivaren pröva samma skrivkommando igen, högst tre gånger, och om detta misslyckas ska den förklara kortet felaktigt och ogiltigt.

143) Innan ett förarkort kan tas ut från färdskrivaren, och efter det att alla relevanta data har lagrats på kortet, ska färdskrivaren nollställa data om kortsession.

3.14.2 *Registrering och lagring på andra generationens färdskrivarkort*

144) Andra generationens färdskrivarkort ska innehålla två olika korttillämpningar: den första ska vara exakt samma som TACHO-tillämpningen i första generationens färdskrivarkort, den andra ska vara tillämpningen TACHO_G2, såsom den specificeras i kapitel 4 och tillägg 2.

145) Färdskrivaren ska ställa in data om kortsessionen på förarkortet eller verkstadskortet omedelbart efter det att kortet satts in.

146) Färdskrivaren ska uppdatera de data – för båda två kortapplikationerna – som lagrats på giltiga förar-, verkstads-, företags- och/eller kontrollkort med alla nödvändiga data för den period då kortet är insatt och som avser kortinnehavaren. De data som lagras på dessa kort specificeras i kapitel 4.

147) Färdskrivaren ska uppdatera de data om föraraktivitet, platser och positioner (i enlighet med avsnitt 4.5.3.1.9, 4.5.3.1.11, 4.5.3.2.9 och 4.5.3.2.11) som finns lagrade på giltiga förar- och/eller verkstadskort med de data om aktivitet och platser som kortinnehavaren anger manuellt.

148) Uppdateringen av data på färdskrivarkort ska, vid behov och med hänsyn till kortets faktiska lagringskapacitet, ske på så sätt att senaste data ersätter äldsta data.

149) Vid skrivfel ska färdskrivaren pröva samma skrivkommando igen, högst tre gånger, och om detta misslyckas ska den förklara kortet felaktigt och ogiltigt.

150) Innan ett förarkort kan tas ut från färdskrivaren, och efter det att alla relevanta data – för båda två kortapplikationerna – har lagrats på kortet, ska färdskrivaren nollställa data om kortsession.

3.15 **Visning**

151) Bildskärmen ska innefatta minst 20 tecken.

152) Minsta teckenstorlek ska vara en höjd på 5 mm och en bredd på 3,5 mm.

153) Bildskärmen ska stödja de tecken som anges i tillägg 1 kapitel 4 om teckenmängder. Förenklade tecken får användas (t.ex. får tecken med accent visas utan accent, och gemener får ersättas med versaler).

▼B

154) Bildskärmen ska vara försedd med lämplig belysning som inte bländar.

155) Tecknen ska vara synliga på färdskrivarens utsida.

156) Färdskrivaren ska kunna visa följande:

— Standarddata.

— Data om varningar.

— Data om tillträde till meny.

— Övriga data som användaren vill se.

Färdskrivaren får visa ytterligare information, förutsatt att den lätt går att skilja från den information som krävs ovan.

157) Färdskrivarens bildskärm ska visa de piktogram eller kombinationer av piktogram som förtecknas i tillägg 3. Den får även visa ytterligare piktogram eller kombinationer av piktogram om de lätt går att skilja från ovan nämnda piktogram eller kombinationer av piktogram.

158) Bildskärmen ska alltid vara på (ON) när fordonet är i rörelse.

159) Färdskrivaren får inbegripa en manuell eller automatisk anordning för att slå av (OFF) bildskärmen när fordonet inte är i rörelse.

Bildskärmsformatet specificeras i tillägg 5.

3.15.1 *Standardvisning*

160) När ingen annan information behöver visas ska färdskrivaren som standard automatiskt visa följande:

— Lokaltiden (UTC-tid + tidsskillnad som föraren ställer in).

— Funktionsläge.

— Förarens och medförarens innevarande aktiviteter.

— Information om föraren:

— Om förarens innevarande aktivitet är körning (DRIVING): förarens aktuella sammanhängande körtid och innevarande sammanlagda avbrottstid.

— Om förarens innevarande aktivitet inte är körning (DRIVING): den aktuella varaktigheten för denna aktivitet (sedan den valdes) och förarens innevarande sammanlagda avbrottstid.

161) Visningen av data för varje förare ska vara klar, enkel och otvetydig. Om informationen om föraren och medföraren inte kan visas samtidigt ska färdskrivaren som standard visa informationen om föraren och göra det möjligt för användaren att visa informationen om medföraren.

162) Om bildskärmens bredd inte gör det möjligt att som standard visa funktionsläget ska färdskrivaren snabbt visa det nya funktionsläget när det ändras.

▼B

163) Färdskrivaren ska snabbt visa kortinnehavarens namn då kortet sätts in.

164) När en omständighet av typen ”omfattas ej” (OUT OF SCOPE) eller ”transport med färja/tåg” (FERRY/TRAIN CROSSING) påbörjas måste bildskärmen som standard med hjälp av relevant piktogram visa att den särskilda omständigheten har påbörjats (förarens innevarande aktivitet behöver inte visas samtidigt).

3.15.2 *Visning av varningar*

165) Färdskrivaren ska visa varningsinformation främst med hjälp av piktogrammen i tillägg 3, som vid behov ska kompletteras med ytterligare numeriskt kodad information. En textbaserad beskrivning av varningen får också visas på det språk som föraren väljer.

3.15.3 *Åtkomst via meny*

166) Färdskrivaren ska tillhandahålla nödvändiga kommandon genom en lämplig menystruktur.

3.15.4 *Visning av övrig information*

167) Det ska vara möjligt att specifikt och på begäran visa följande:

— UTC-datum och UTC-tid samt lokal tidsskillnad.

— Innehållet i de sex utskrifterna i samma format som utskrifterna själva.

— Förarens sammanhängande körtid och sammanlagda avbrottstid.

— Medförarens sammanhängande körtid och sammanlagda avbrottstid.

— Förarens sammanlagda körtid för föregående och innevarande vecka.

— Medförarens sammanlagda körtid för föregående och innevarande vecka.

Frivilligt:

— Den aktuella varaktigheten för medförarens aktivitet (sedan den valdes).

— Förarens sammanlagda körtid för innevarande vecka.

— Medförarens sammanlagda körtid för den innevarande arbetsperioden.

— Förarens sammanlagda körtid för den innevarande arbetsperioden.

168) Innehållet i utskrifterna ska visas i en följd, rad för rad. Om bildskärmens bredd är mindre än 24 tecken ska användaren få komplett information på lämpligt sätt (flera rader, rullning, …).

De utskriftsrader som är avsedda för handskriven information behöver inte visas.

▼B

3.16 **Utskrift**

169) Det ska gå att skriva ut information från färdskrivarens dataminne och/eller från färdskrivarkorten i enlighet med följande sju utskrifter:

— Dagsutskrift från kort av föraraktiviteter.

— Dagsutskrift från fordonsenhet av föraraktiviteter.

— Utskrift från kort av händelser och fel.

— Utskrift från fordonsenhet av händelser och fel.

— Utskrift av tekniska data.

— Utskrift av hastighetsöverträdelse.

— Datahistorik avseende färdskrivarkort för en viss fordonsenhet (se avsnitt 3.12.16).

Format och innehåll i dessa utskrifter anges i detalj i tillägg 4.

Ytterligare data får förekomma i slutet av utskrifterna.

Färdskrivaren får ge ytterligare utskrifter, om de är lätta att skilja från de sju ovan nämnda utskrifterna.

170) ”Dagsutskrift från kort av föraraktiviteter” och ”Utskrift från kort av händelser och fel” ska endast finnas tillgängliga om ett förarkort eller ett verkstadskort är insatt i färdskrivaren. De relevanta data som finns på det berörda kortet ska uppdateras av färdskrivaren innan utskriften inleds.

171) För att tillhandahålla ”Dagsutskrift från kort av föraraktiviteter” eller ”Utskrift från kort av händelser och fel” ska färdskrivaren

— antingen automatiskt välja förarkortet eller verkstadskortet om endast ett sådant kort är insatt,

— eller tillhandahålla ett kommando för val av vilket kort som ska användas, eller välja kortet i förarens kortplats, om två kort (förar- och/eller verkstadskort) är insatta i färdskrivaren.

172) Skrivaren ska kunna skriva ut 24 tecken per rad.

173) Minsta teckenstorlek ska vara en höjd på 2,1 mm och en bredd på 1,5 mm.

174) Skrivaren ska stödja de tecken som anges i tillägg 1 kapitel 4 om teckenmängder.

175) Skrivarna ska vara utformade så att de tillhandahåller dessa utskrifter med en skärpa som sannolikt förhindrar tvetydighet när utskriften läses.

176) Utskrifternas storlek och uppgifterna i dem ska inte ändras vid normal luftfuktighet (10–90 procent) och temperatur.

177) Det typgodkända papper som används i färdskrivaren ska vara försett med giltigt typgodkännandemärke och angivelse av de typ(er) av färdskrivare där det får användas.

▼B

178) Utskrifterna ska vara klart läsbara och identifierbara under minst två år under normala lagringsvillkor, med avseende på ljusintensitet, luftfuktighet och temperatur.

179) Utskrifterna ska åtminstone uppfylla de provningsspecifikationer som definieras i tillägg 9.

180) Det ska även gå att lägga till handskrivna anmärkningar, t.ex. förarens namnteckning, i dessa handlingar.

181) Om papperet tar slut vid utskrift ska färdskrivaren, när papperet har fyllts på, börja om från början i utskriften eller fortsätta utskriften med en otvetydig hänvisning till den del som tidigare skrivits ut.

3.17 **Varningar**

182) Färdskrivaren ska varna föraren när den upptäcker en händelse eller ett fel.

183) En varning om avbrott i strömtillförsel får uppskjutas till det att strömtillförseln återställts.

184) Färdskrivaren ska varna föraren 15 minuter före och vid den tidpunkt då längsta tillåtna sammanhängande körtid överskrids.

185) Varningarna ska vara visuella. Ljudvarningar får också ges utöver de visuella varningarna.

186) Användaren ska tydligt kunna urskilja de visuella varningarna, som ska vara placerade i förarens synfält och vara tydligt läsbara både dag och natt.

187) De visuella varningarna får byggas in i färdskrivaren och/eller vara avskilda från den.

188) I det senare fallet ska färdskrivaren vara försedd med symbolen ”T”.

189) Varningarna ska vara minst 30 sekunder långa, om inte användaren kvitterar dem genom att trycka på en eller flera särskilda knappar på färdskrivaren. Den första kvitteringen får inte radera ut den visning av orsaken till varningen som avses i nästa punkt.

190) Orsaken till varningen ska visas på färdskrivaren och vara synlig tills det att användaren kvitterar den med hjälp av en särskild knapp eller ett särskilt kommando i färdskrivaren.

191) Ytterligare varningar får ges, förutsatt att det inte finns någon risk för att föraren blandar ihop dem med varningarna ovan.

3.18 **Överföring av data till externa media**

192) Det ska på begäran gå att överföra data från färdskrivarens dataminne eller från ett förarkort till externa lagringsmedia via en kalibrerings-/överföringsanslutning. De data som finns på det berörda kortet ska uppdateras av färdskrivaren innan överföringen inleds.

▼B

193) Dessutom får färdskrivaren i alla funktionslägen, som tillvalsfunktion, kunna överföra data på annat valfritt sätt till ett företag som har autentiserats genom denna kanal. I detta fall ska alla tillträdesrättigheter till data i företagsläge tillämpas på denna överföring.

194) Överföringen får inte ändra eller ta bort några lagrade data.

195) Det elektriska gränssnittet för kalibrerings-/överföringsanslutningen specificeras i tillägg 6.

196) Överföringsprotokoll specificeras i tillägg 7.

3.19 **Fjärrkommunikation vid riktade vägkontroller**

197) När tändningen är påslagen ska fordonsenheten var 60:e sekund lagra de senaste data som krävs för riktade vägkontroller i kommunikationsanordningen för fjärravläsning. Dessa data ska krypteras och signeras såsom anges i tillägg 11 och tillägg 14.

198) Data som ska kontrolleras på distans ska vara tillgängliga för fjärravläsare via trådlös kommunikation, såsom anges i tillägg 14.

199) Data som krävs för riktade vägkontroller ska avse följande:

— Senaste försök till säkerhetsöverträdelse.

— Längsta avbrott i strömtillförsel.

— Sensorfel.

— Fel i rörelsedata.

— Konflikt i fordonets rörelsedata.

— Körning utan giltigt kort.

— Insättning av kort under körning.

— Data om tidsinställning.

— Kalibreringsdata, inklusive datum för de två senast lagrade kalibreringsposterna.

— Fordonets registreringsnummer.

— Hastighet som registrerats av färdskrivaren.

3.20 **Utdata till ytterligare externa anordningar**

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

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

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

— Dessa data är utvalda bland befintliga data från färdskrivarens datakatalog (tillägg 1).

▼B

— 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 meddela förarens samtycke till andra externa anordningar.

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

201) För att säkerställa bakåtkompatibilitet får färdskrivare även fortsättningsvis utrustas med det gränssnitt för seriell anslutning som specificeras i bilaga 1B till förordning EEG nr 3821/85, i sin senaste lydelse. Förarens samtycke krävs dock även här om personuppgifter ska sändas.

3.21 **Kalibrering**

202) Kalibreringsfunktionen ska göra det möjligt att

— automatiskt para rörelsesensorn med fordonsenheten,

— automatiskt koppla den externa GNSS-anordningen med fordonsenheten (i förekommande fall),

— digitalt anpassa färdskrivarens konstant (k) till fordonets karakteristiska koefficient (w),

— ställa in aktuell tidpunkt inom giltighetstiden för det insatta verkstadskortet,

— ändra aktuellt vägmätarvärde,

— uppdatera de data för identifiering av rörelsesensor som finns lagrade i dataminnet,

— uppdatera de data för identifiering av extern GNSS-anordning som finns lagrade i dataminnet,

▼B

— uppdatera typer och identifierare för samtliga befintliga plomberingar,

— uppdatera eller bekräfta andra parametrar som färdskrivaren känner till: fordonsidentifiering, w, l, däcksdimension, samt hastighetsbegränsande anordning (i förekommande fall).

203) Kalibreringsfunktionen ska dessutom kunna ta bort möjligheten att använda första generationens färdskrivarkort i färdskrivaren, förutsatt att de villkor som anges i tillägg 15 uppfylls.

204) Parningen av rörelsesensorn med fordonsenheten ska minst bestå av följande:

— Uppdatering av de data om installation av rörelsesensor som finns i rörelsesensorn (efter behov).

— Kopiering från rörelsesensorn till fordonsenhetens dataminne av nödvändiga data för identifiering av rörelsesensorn.

205) Kopplingen av den externa GNSS-anordningen med fordonsenheten ska minst bestå av följande:

— Uppdatering av de data om installation av extern GNSS-anordning som finns i den externa GNSS-anordningen (efter behov).

— Kopiering från den externa GNSS-anordningen till fordonsenhetens dataminne av nödvändiga data för identifiering av den externa GNSS-anordningen, inklusive dess serienummer.

Efter kopplingen ska positionsinformationen från GNSS kontrolleras.

206) Kalibreringsfunktionen ska kunna mata in nödvändiga data genom kalibrerings-/överföringsanslutningen i enlighet med det kalibreringsprotokoll som definieras i tillägg 8. Kalibreringsfunktionen får också mata in nödvändiga data på andra sätt.

3.22 **Kalibreringskontroll på väg**

207) Funktionen för kalibreringskontroll på väg ska, direkt på begäran, möjliggöra avläsning av serienummer för den rörelsesensor (eventuellt inbyggd i adapter) och den externa GNSS-anordning (i förekommande fall) som är ansluten till fordonsenheten.

208) Denna avläsning ska åtminstone vara möjlig att utföra via menykommandon på fordonsenhetens bildskärm.

209) Funktionen för kalibreringskontroll på väg ska även möjliggöra kontroll av val av in-/utläge för signal på den in-/utlinje för kalibrering som specificeras i tillägg 6 via K-line-gränssnittet. Detta ska ske via ECUAdjustmentSession, såsom anges i tillägg 8 avsnitt 7 om kontroll av provpulser och funktionsenhet för kontroll av in-/utdata.

3.23 **Tidsinställning**

210) Funktionen för tidsinställning ska göra det möjligt att automatiskt ställa in aktuell tidpunkt. I färdskrivaren används två källor för tidsinställning: 1) fordonsenhetens interna klocka, 2) GNSS-mottagaren.

▼B

211) Tidsinställningen av fordonsenhetens interna klocka ska ske automatiskt med högst tolv timmars intervall. Om denna tidsperiod löper ut och 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. En händelse av typen tidskonflikt ska utlösas om den aktuella tiden avviker mer än en (1) minut från den tidsinformation som tillhandahålls av GNSS-mottagaren.

212) Funktionen för tidsinställning ska också möjliggöra externt utlöst inställning av aktuell tid i kalibreringsläge.

3.24 **Prestanda**

213) Fordonsenheten ska vara helt funktionsduglig vid temperaturer från – 20 °C till + 70 °C, den externa GNSS-anordningen från – 20 °C till + 70 °C och rörelsesensorn från – 40 °C till + 135 °C. Innehållet i dataminnet ska bevaras vid temperaturer ned till – 40 °C.

214) Färdskrivaren ska vara helt funktionsduglig vid en luftfuktighet från 10 % till 90 %.

215) De plomberingar som används i den smarta färdskrivaren ska klara de förhållanden som gäller för de färdskrivarkomponenter där plomberingarna är anbringade.

216) Färdskrivaren ska skyddas mot överspänning, omkastning av polerna i dess strömtillförsel och kortslutning.

217) Rörelsesensorer ska antingen

— reagera på ett magnetfält som stör avkänningen av fordonets rörelse (i så fall ska fordonsenheten registrera och lagra ett sensorfel (krav 88)), eller

— ha ett sensorelement som är skyddat eller immunt mot magnetfält.

218) Färdskrivaren och den externa GNSS-anordningen ska uppfylla kraven i den internationella förordningen UN ECE R10 och ska vara skyddade mot elektrostatiska urladdningar och transienter.

3.25 **Material**

219) Färdskrivarens samtliga beståndsdelar ska vara tillverkade av material med tillräcklig stabilitet och mekanisk hållfasthet samt med stabila elektriska och magnetiska egenskaper.

220) Vid normala driftsförhållanden ska samtliga inre delar av färdskrivaren vara skyddade mot fukt och damm.

221) Fordonsenheten och den externa GNSS-anordningen ska uppfylla kriterierna för skyddsklass IP 40 och rörelsesensorn ska uppfylla kriterierna för skyddsklass IP 64, i enlighet med standard IEC 60529:1989, inklusive A1:1999 och A2:2013.

222) Färdskrivaren ska uppfylla tillämpliga tekniska specifikationer med avseende på ergonomisk utformning.

▼B

223) Färdskrivaren ska skyddas mot oavsiktlig skada.

3.26 **Märkningar**

224) Om färdskrivaren visar fordonets vägmätarvärde och hastighet ska följande uppgifter visas på dess bildskärm:

— Intill den siffra som vägmätaren visar: enheten för sträcka, förkortat till ”km”.

— Intill den siffra som hastighetsmätaren visar: ”km/h”.

Färdskrivaren får också ställas om till att visa hastigheten i ”miles per hour”, varvid enheten för hastighet ska visas med förkortningen ”mph”. Färdskrivaren får också ställas om till att visa sträckan i ”miles”, varvid enheten för sträcka ska visas med förkortningen ”mi”.

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

— Färdskrivartillverkarens namn och adress.

— Tillverkarens artikelnummer och tillverkningsår för färdskrivaren.

— Färdskrivarens serienummer.

— Typgodkännandemärke för färdskrivartypen.

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 färdskrivarens artikelnummer.

4 KONSTRUKTIONS- OCH FUNKTIONSKRAV FÖR FÄRDSKRIVARKORT

4.1 **Synliga data**

Framsidan ska innehålla följande:

227) Korttypen, skriven med versaler på det eller de officiella språken i den medlemsstat som utfärdar kortet (på svenska ”FÖRARKORT”, ”KONTROLLKORT”, ”VERKSTADSKORT” eller ”FÖRETAGSKORT”).

228) Namnet på den medlemsstat som utfärdar kortet (frivilligt).

229) Nationalitetsbeteckningen för den medlemsstat som utfärdar kortet, inlagd i vitt i en blå rektangel och omgiven av tolv gula stjärnor. Nationalitetsbeteckningarna ska vara följande:

B	Belgien	LV	Lettland
BG	Bulgarien	L	Luxemburg
CZ	Tjeckien	LT	Litauen
CY	Cypern	M	Malta
DK	Danmark	NL	Nederländerna
D	Tyskland	A	Österrike
EST	Estland	PL	Polen

▼B

GR	Grekland	P RO SK SLO	Portugal Rumänien Slovakien Slovenien
E	Spanien	FIN	Finland
F HR H	Frankrike Kroatien Ungern	S	Sverige
IRL	Irland	UK	Förenade kungariket
I	Italien		

230) De uppgifter som är särskiljande för kortet, numrerade enligt nedanstående.

	Förarkort	Kontrollkort	Företagskort eller verkstadskort
1.	Förarens efternamn	Kontrollorganets namn	Företagets eller verkstadens namn
2.	Förarens förnamn	Kontrollantens (kontrolltjänstemannens) efternamn (i förekommande fall)	Innehavarens efternamn (i förekommande fall)
3.	Förarens födelsedatum	Kontrollantens (kontrolltjänstemannens) förnamn (i förekommande fall)	Innehavarens förnamn (i förekommande fall)
4.a	Kortets första giltighetsdag		
4.b	Kortets sista giltighetsdag		
4.c	Namn på utfärdande myndighet (får tryckas på baksidan)		
4.d	Ett annat nummer än det som anges under punkt 5, för administrativa ändamål (frivilligt)		
5.a	Körkortsnummer (den dag då förarkortet utfärdas)	—	—
5.b	Kortnummer		
6.	Fotografi av föraren	Fotografi av kontrollanten (kontrolltjänstemannen) (frivilligt)	Fotografi av montören (frivilligt)
7.	Innehavarens namnteckning (frivilligt)		
8.	Innehavarens normala bosättningsort eller postadress (frivilligt)	Kontrollorganets postadress	Företagets eller verkstadens postadress

231) Datum ska skrivas i formatet ”dd/mm/yyyy” eller ”dd.mm.yyyy” (dag, månad, år).

Baksidan ska innehålla följande:

232) En förklaring av de numrerade punkterna på kortets framsida.

▼B

233) Med särskilt skriftligt samtycke från innehavaren får information som inte har samband med administreringen av kortet läggas till, vilken inte på något sätt påverkar modellens användning som färdskrivarkort.

234) Färdskrivarkorten ska tryckas i följande dominerande bakgrundsfärger:

— Förarkort: vitt.

— Kontrollkort: blått.

— Verkstadskort: rött.

— Företagskort: gult.

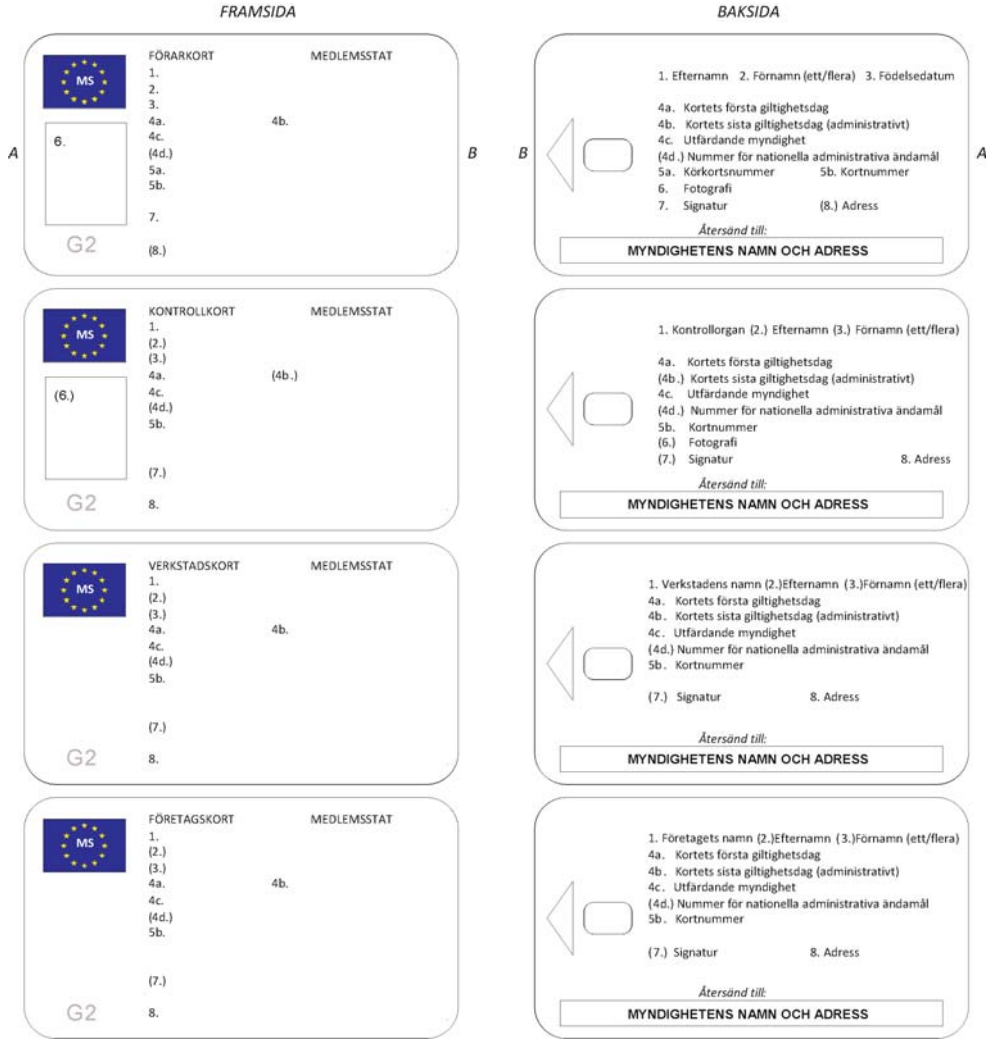
235) Färdskrivarkorten ska åtminstone ha följande skyddsfunktioner mot förfalskning och manipulering:

— En säkerhetsmönstrad bakgrund med fint guilloche-mönster och iristryck.

— Vid fotografiet ska den säkerhetsmönstrade bakgrunden och fotografiet överlappa varandra.

— Minst en tvåfärgad mikrotextrad.

GEMENSKAPSMODELL FÖR FÄRDSKRIVARKORT



▼B

236) Medlemsstaterna får efter samråd med kommissionen lägga till färger eller markeringar, såsom nationella symboler eller säkerhetsfunktioner, utan att det påverkar tillämpningen av andra bestämmelser i denna bilaga.

237) Sådana tillfälliga kort som avses i artikel 26.4 i förordning (EU) nr 165/2014 ska överensstämma med bestämmelserna i denna bilaga.

4.2 **Säkerhet**

Systemsäkerheten är avsedd att skydda integriteten och autenticiteten hos data som utväxlas mellan korten och färdskrivaren, skydda integriteten och autenticiteten hos data som överförs från korten, möjliggöra vissa skrivoperationer till korten endast från färdskrivaren, dekryptera vissa data, utesluta risken för förfalskningar av data som lagras på korten, förhindra manipulering och upptäcka alla sådana försök.

238) För att systemsäkerhet ska kunna uppnås ska färdskrivarkorten uppfylla de säkerhetskrav som definieras i tilläggen 10 och 11.

239) Färdskrivarkorten ska vara läsbara för annan utrustning, t.ex. persondatorer.

4.3 **Standarder**

240) Färdskrivarkorten ska uppfylla följande standarder:

— ISO/IEC 7810 *Identification cards – Physical characteristics*.

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

— *Part 1: Physical characteristics*.

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

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

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

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

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

— Färdskrivarkorten ska provas i enlighet med ISO/IEC 10373-3:2010 *Identification cards – Test methods – Part 3: Integrated circuit cards with contacts and related interface devices*.

4.4 **Miljö- och elspecifikationer**

241) Färdskrivarkorten ska fungera korrekt under alla klimatförhållanden som vanligtvis förekommer inom gemenskapens territorium och vid temperaturer mellan – 25 °C och + 70 °C, med tillfälliga toppar på upp till + 85 °C, varvid ”tillfälliga” innebär högst fyra timmar per gång och högst 100 gånger under kortets livstid.

242) Färdskrivarkorten ska fungera korrekt vid en luftfuktighet mellan 10 % och 90 %.

▼B

243) Färdskrivarkorten ska fungera korrekt under en femårsperiod om de används i enlighet med miljö- och elspecifikationerna.

244) Färdskrivarkorten ska uppfylla ECE R10 i fråga om elektromagnetisk kompatibilitet och vara skyddade mot elektrostatiska urladdningar.

4.5 **Lagring av data**

Under denna punkt gäller följande:

— Tider registreras med en upplösning av en (1) minut, om inte annat anges.

— Vägmätarvärden registreras med en upplösning av en (1) kilometer.

— Hastigheter registreras med en upplösning av en (1) km/h.

— Positioner (latitud och longitud) registreras i grader och minuter med en upplösning av 0,1 minut.

Färdskrivarkortens funktioner, kommandon och logiska strukturer, vilka uppfyller kraven för lagring av data, specificeras i tillägg 2.

Om inget annat anges ska datalagringen på färdskrivarkorten organiseras på så sätt att nya data ersätter de data som är äldst om den planerade minnesstorleken för de aktuella posterna har utnyttjats till fullo.

245) Under denna punkt anges minsta lagringskapacitet för de olika tillämpningarnas datafiler. Färdskrivarkorten ska kunna ange dessa datafilers faktiska lagringskapacitet till färdskrivaren.

246) Eventuella ytterligare data som kan lagras på färdskrivarkorten i samband med andra tillämpningar på kortet ska lagras i enlighet med Europaparlamentets och rådets direktiv 95/46/EG och Europaparlamentets och rådets direktiv 2002/58/EC, och i överensstämmelse med artikel 7 i förordning (EU) nr 165/2014.

247) Varje huvudfil (MF, *Master File*) på ett färdskrivarkort ska innehålla upp till fem elementfiler (EF, *Elementary File*) för korthantering, tillämpnings- och chipidentifiering, och två dedikerade filer (DF, *Dedicated File*):

— DF Tachograph, som innehåller den tillämpning som är åtkomlig för första generationens fordonsenheter, och som också finns i första generationens färdskrivarkort.

— DF Tachograph_G2, som innehåller den tillämpning som endast är åtkomlig för andra generationens fordonsenheter, och som endast finns i andra generationens färdskrivarkort.

Alla uppgifter om färdskrivarkortens struktur finns i tillägg 2.

4.5.1 *Elementfiler för identifiering och korthantering*

4.5.2 *Identifiering av smartkort*

248) Det ska gå att lagra följande identifieringsdata för smartkort på färdskrivarkortet:

— Klockstopp (*clockstop*).

▼B

— Kortets serienummer (inbegripet tillverkningsuppgifter).

— Kortets typgodkännandenummer.

— Identifiering av kortanpassare (*card personaliser*).

— Identifiering av inbäddare (*embedder*).

— Identifiering av integrerad krets (IC).

4.5.2.1 Identifiering av chip

249) Det ska gå att lagra följande identifieringsdata för integrerade kretsar (IC) på färdskrivarkortet:

— Den integrerade kretsens serienummer.

— Tillverkningsuppgifter för den integrerade kretsen.

4.5.2.2 DIR (finns endast på andra generationens färdskrivarkort)

250) Det ska gå att lagra de dataobjekt för tillämpningsidentifierare som anges i tillägg 2 på färdskrivarkortet.

4.5.2.3 ATR-information (under vissa förutsättningar, finns endast på andra generationens färdskrivarkort)

251) Det ska gå att lagra följande dataobjekt med information om utökad längd på färdskrivarkortet:

— Om färdskrivarkortet stöder fält med utökad längd: det dataobjekt med information om utökad längd som anges i tillägg 2.

4.5.2.4 Information med utökad längd (under vissa förutsättningar, finns endast på andra generationens färdskrivarkort)

252) Det ska gå att lagra följande dataobjekt med utökad längd på färdskrivarkortet:

— Om färdskrivarkortet stöder fält med utökad längd: de dataobjekt med utökad längd som anges i tillägg 2.

4.5.3 *Förarkort*

4.5.3.1 Färdskrivartillämpning (tillgänglig för första och andra generationens fordonsenheter)

4.5.3.1.1 Tillämpningsidentifiering

253) Det ska gå att lagra följande data för tillämpningsidentifiering på förarkortet:

— Identifiering av färdskrivartillämpning.

— Identifiering av typ av färdskrivarkort.

4.5.3.1.2 Nyckel och certifikat

254) Det ska gå att lagra ett antal kryptografiska nycklar och certifikat på förarkortet, såsom anges i tillägg 11 del A.

▼B

4.5.3.1.3 Kortidentifiering

255) Det ska gå att lagra följande data för kortidentifiering på förarkortet:

— Kortnummer.

— Utfärdande medlemsstat, utfärdande myndighet, utfärdandedatum.

— Kortets första och sista giltighetsdag.

4.5.3.1.4 Identifiering av kortinnehavare

256) Det ska gå att lagra följande identifieringsdata för kortinnehavare på förarkortet:

— Innehavarens efternamn.

— Innehavarens förnamn.

— Födelsedatum.

— Valt språk.

4.5.3.1.5 Överföring från kort

257) Det ska gå att lagra följande data om överföring från kort på förarkortet:

— Datum och tidpunkt för den senaste överföringen från kortet (för andra ändamål än kontrolländamål).

258) Det ska gå att lagra en (1) sådan post på förarkortet.

4.5.3.1.6 Information om körkort

259) Det ska gå att lagra följande körkortsdata på förarkortet:

— Utfärdande medlemsstat, utfärdande myndighet.

— Körkortsnummer (den dag då kortet utfärdas).

4.5.3.1.7 Händelsedata

För de data som avses i denna punkt ska tidpunkten lagras med en upplösning av en (1) sekund.

260) Det ska gå att på förarkortet lagra data om följande händelser som upptäckts av färdskrivaren när kortet var insatt:

— Överlappning av tider (om detta kort är orsaken till händelsen).

— Insättning av kort under körning (om händelsen gäller detta kort).

— Senaste kortsession ej korrekt avslutad (om händelsen gäller detta kort).

— Avbrott i strömtillförseln.

— Fel i rörelsedata.

— Försök till säkerhetsöverträdelse.

261) Det ska gå att lagra följande data om dessa händelser på förarkortet:

— Händelsekod.

— Datum och tidpunkt för händelsens början (eller för insättning av kort om händelsen pågick vid den tidpunkten).

▼B

— Datum och tidpunkt för händelsens slut (eller för uttag av kort om händelsen pågick vid den tidpunkten).

— Registreringsnummer (VRN) och registrerande medlemsstat för det fordon där händelsen ägde rum.

Anmärkning: När det gäller händelsen ”överlappning av tider” ska

— datum och tidpunkt för händelsens början motsvara datum och tidpunkt för uttag av kortet i föregående fordon,

— datum och tidpunkt för händelsens slut motsvara datum och tidpunkt för insättning av kortet i nuvarande fordon,

— fordonsdata motsvara det nuvarande fordonet, som ger upphov till händelsen.

Anmärkning: När det gäller händelsen ”senaste kortsession ej korrekt avslutad” ska

— datum och tidpunkt för händelsens början motsvara datum och tidpunkt för insättning av kortet för den session som inte avslutats korrekt,

— datum och tidpunkt för händelsens slut motsvara datum och tidpunkt för insättning av kortet för den session då händelsen upptäcks (innevarande session),

— fordonsdata motsvara det fordon där sessionen inte avslutades korrekt.

262) På förarkortet ska det gå att lagra data för de sex senaste händelserna av varje typ (dvs. 36 händelser).

4.5.3.1.8 Data om fel

För de data som avses i denna punkt ska tidpunkten registreras med en upplösning av en (1) sekund.

263) Det ska gå att på förarkortet lagra data om följande fel som upptäckts av färdskrivaren när kortet var insatt:

— Kortfel (om detta kort är orsak till felet).

— Färdskrivarfel.

264) Det ska gå att lagra följande data om dessa fel på förarkortet:

— Felkod.

— Datum och tidpunkt för felets början (eller för insättning av kort om felet pågick vid den tidpunkten).

— Datum och tidpunkt för felets slut (eller för uttag av kort om felet pågick vid den tidpunkten).

— Registreringsnummer (VRN) och registrerande medlemsstat för det fordon där felet ägde rum.

265) På förarkortet ska det gå att lagra data om de tolv senaste felen av varje typ (dvs. 24 fel).

▼B

4.5.3.1.9 Data om föraraktiviteter

266) Det ska gå att lagra följande data på förarkortet för varje kalenderdag då kortet har använts eller för vilken föraren har angivit aktiviteter manuellt:

— Datum.

— En daglig närvaroräknare (ökas med ett för varje sådan kalenderdag).

— Den sammanlagda sträcka som föraren har tillryggalagt den dagen.

— Förarstatus kl. 00.00.

— Följande data när föraren har ändrat aktivitet och/eller har ändrat körningsstatus och/eller har satt in eller tagit ut sitt kort:

— Körningsstatus (flera förare (CREW), ensam förare (SINGLE)).

— Kortplats (förare (DRIVER), medförare (CO-DRIVER)).

— Kortstatus (insatt (INSERTED), ej insatt (NOT INSERTED)).

— Aktivitet (körning (DRIVING), tillgänglighet (AVAILABILITY), annat arbete (WORK), rast/vila (BREAK/REST)).

— Tidpunkt för ändringen.

267) Det ska gå att lagra data om föraraktiviteter för minst 28 dagar i förarkortets minne (en förares genomsnittliga aktivitet är fastställd till 93 aktivitetsändringar per dygn).

268) De data som är förtecknade under krav 261, 264 och 266 ska lagras på ett sätt som möjliggör att aktiviteter tas fram i den ordning de har ägt rum, även om tiderna överlappar varandra.

4.5.3.1.10 Data om använda fordon

269) Det ska gå att lagra följande data på förarkortet för varje kalenderdag som kortet har använts och för varje användningsperiod för ett visst fordon den dagen (en användningsperiod inbegriper alla på varandra följande insättnings-/uttagscykler i fordonet för kortet i fråga):

— Datum och tidpunkt för första användning av fordonet (dvs. första insättning av kort under denna användningsperiod för fordonet, eller 00.00 om användningsperioden pågår vid den tidpunkten).

— Fordonets vägmätarvärde vid den tidpunkten.

— Datum och tidpunkt för senaste användning av fordonet (dvs. senaste uttag av kort under denna användningsperiod för fordonet, eller 23.59 om användningsperioden pågår vid den tidpunkten).

▼B

— Fordonets vägmätarvärde vid den tidpunkten.

— Fordonets registreringsnummer (VRN) och registrerande medlemsstat.

270) Det ska gå att lagra minst 84 sådana poster på förarkortet.

4.5.3.1.11 Platser där dagens arbetsperioder påbörjas och/eller avslutas

271) Det ska gå att på förarkortet lagra följande data om de platser som anges av föraren där dagens arbetsperioder påbörjas och/eller avslutas:

— Datum och tidpunkt för angivelsen (eller datum/tidpunkt som avser angivelsen och som anges manuellt).

— Typ av angivelse (påbörjande eller avslutande, särskild omständighet).

— Det land och den region som anges.

— Fordonets vägmätarställning.

272) Det ska gå att lagra minst 42 par av sådana poster i förarkortets minne.

4.5.3.1.12 Data om kortsessioner

273) Det ska gå att på förarkortet lagra följande data om det fordon där den innevarande sessionen påbörjades:

— Datum och tidpunkt när sessionen påbörjades (dvs. för insättning av kort), med en upplösning av en (1) sekund.

— Fordonets registreringsnummer (VRN) och registrerande medlemsstat.

4.5.3.1.13 Data om kontrollaktiviteter

274) Det ska gå att lagra följande data om kontrollaktiviteter på förarkortet:

— Datum och tidpunkt för kontrollen.

— Kontrollkortsnummer och medlemsstat som utfärdat kortet.

— Kontrolltyp (visning och/eller utskrift och/eller överföring av data från fordonsenhet och/eller överföring av data från kort (se anmärkning)).

— Överförd period, om överföring utfördes.

— Registreringsnummer (VRN) och registrerande medlemsstat för det fordon i vilket kontrollen ägde rum.

Anmärkning: Överföring av data från kort registreras endast om den gjorts genom en färdskrivare.

275) Det ska gå att lagra en (1) sådan post på förarkortet.

4.5.3.1.14 Data om särskilda omständigheter

276) Det ska gå att på förarkortet lagra följande data om de särskilda omständigheter som angavs medan kortet var insatt (oavsett kortplats):

— Datum och tidpunkt för angivelsen.

— Typ av särskild omständighet.

▼B

277) Det ska gå att lagra minst 56 sådana poster på förarkortet.

4.5.3.2 Färdskrivartillämpning i generation 2 (ej åtkomlig för första generationens fordonsenhet)

4.5.3.2.1 Tillämpningsidentifiering

278) Det ska gå att lagra följande data för tillämpningsidentifiering på förarkortet:

— Identifiering av färdskrivartillämpning.

— Identifiering av typ av färdskrivarkort.

4.5.3.2.2 Nycklar och certifikat

279) Det ska gå att lagra ett antal kryptografiska nycklar och certifikat på förarkortet, såsom anges i tillägg 11 del B.

4.5.3.2.3 Kortidentifiering

280) Det ska gå att lagra följande data för kortidentifiering på förarkortet:

— Kortnummer.

— Utfärdande medlemsstat, utfärdande myndighet, utfärdandedatum.

— Kortets första och sista giltighetsdag.

4.5.3.2.4 Identifiering av kortinnehavare

281) Det ska gå att lagra följande identifieringsdata för kortinnehavare på förarkortet:

— Innehavarens efternamn.

— Innehavarens förnamn.

— Födelsedatum.

— Valt språk.

4.5.3.2.5 Överföring från kort

282) Det ska gå att lagra följande data om överföring från kort på förarkortet:

— Datum och tidpunkt för den senaste överföringen från kortet (för andra ändamål än kontrolländamål).

283) Det ska gå att lagra en (1) sådan post på förarkortet.

4.5.3.2.6 Information om körkort

284) Det ska gå att lagra följande körkortsdata på förarkortet:

— Utfärdande medlemsstat, utfärdande myndighet.

— Körkortsnummer (den dag då kortet utfärdas).

4.5.3.2.7 Händelsedata

För de data som avses i denna punkt ska tidpunkten lagras med en upplösning av en (1) sekund.

▼B

285) Det ska gå att på förarkortet lagra data om följande händelser som upptäckts av färdskrivaren när kortet var insatt:

— Överlappning av tider (om detta kort är orsaken till händelsen).

— Insättning av kort under körning (om händelsen gäller detta kort).

— Senaste kortsession ej korrekt avslutad (om händelsen gäller detta kort).

— Avbrott i strömtillförseln.

— Fel i kommunikation med kommunikationsanordning för fjärravläsning.

— Positionsinformation från GNSS-mottagare saknas.

— Fel i kommunikation med extern GNSS-anordning.

— Fel i rörelsedata.

— Konflikt i fordonets rörelsedata.

— Försök till säkerhetsöverträdelse.

— Tidskonflikt.

286) Det ska gå att lagra följande data om dessa händelser på förarkortet:

— Händelsekod.

— Datum och tidpunkt för händelsens början (eller för insättning av kort om händelsen pågick vid den tidpunkten).

— Datum och tidpunkt för händelsens slut (eller för uttag av kort om händelsen pågick vid den tidpunkten).

— Registreringsnummer (VRN) och registrerande medlemsstat för det fordon där händelsen ägde rum.

Anmärkning: När det gäller händelsen ”överlappning av tider” ska

— datum och tidpunkt för händelsens början motsvara datum och tidpunkt för uttag av kortet i föregående fordon,

— datum och tidpunkt för händelsens slut motsvara datum och tidpunkt för insättning av kortet i nuvarande fordon,

— fordonsdata motsvara det nuvarande fordonet, som ger upphov till händelsen.

Anmärkning: När det gäller händelsen ”senaste kortsession ej korrekt avslutad” ska

— datum och tidpunkt för händelsens början motsvara datum och tidpunkt för insättning av kortet för den session som inte avslutats korrekt,

— datum och tidpunkt för händelsens slut motsvara datum och tidpunkt för insättning av kortet för den session då händelsen upptäcks (innevarande session),

▼B

— fordonsdata motsvara det fordon där sessionen inte avslutades korrekt.

287) På förarkortet ska det gå att lagra data för de sex senaste händelserna av varje typ (dvs. 66 händelser).

4.5.3.2.8 Data om fel

För de data som avses i denna punkt ska tidpunkten registreras med en upplösning av en (1) sekund.

288) Det ska gå att på förarkortet lagra data om följande fel som upptäckts av färdskrivaren när kortet var insatt:

— Kortfel (om detta kort är orsak till felet).

— Färdskrivarfel.

289) Det ska gå att lagra följande data om dessa fel på förarkortet:

— Felkod.

— Datum och tidpunkt för felets början (eller för insättning av kort om felet pågick vid den tidpunkten).

— Datum och tidpunkt för felets slut (eller för uttag av kort om felet pågick vid den tidpunkten).

— Registreringsnummer (VRN) och registrerande medlemsstat för det fordon där felet ägde rum.

290) På förarkortet ska det gå att lagra data om de tolv senaste felen av varje typ (dvs. 24 fel).

4.5.3.2.9 Data om föraraktiviteter

291) Det ska gå att lagra följande data på förarkortet för varje kalenderdag då kortet har använts eller för vilken föraren har angivit aktiviteter manuellt:

— Datum.

— En daglig närvaroräknare (ökas med ett för varje sådan kalenderdag).

— Den sammanlagda sträcka som föraren har tillryggalagt den dagen.

— Förarstatus kl. 00.00.

— Följande data när föraren har ändrat aktivitet och/eller har ändrat körningsstatus och/eller har satt in eller tagit ut sitt kort:

— Körningsstatus (flera förare (CREW), ensam förare (SINGLE)).

— Kortplats (förare (DRIVER), medförare (CO-DRIVER)).

— Kortstatus (insatt (INSERTED), ej insatt (NOT INSERTED)).

— Aktivitet (körning (DRIVING), tillgänglighet (AVAILABILITY), annat arbete (WORK), rast/vila (BREAK/REST)).

▼B

— Tidpunkt för ändringen.

292) Det ska gå att lagra data om föraraktiviteter för minst 28 dagar i förarkortets minne (en förares genomsnittliga aktivitet är fastställd till 93 aktivitetsändringar per dygn).

293) De data som är förtecknade under krav 286, 289 och 291 ska lagras på ett sätt som möjliggör att aktiviteter tas fram i den ordning de har ägt rum, även om tiderna överlappar varandra.

4.5.3.2.10 Data om använda fordon

294) Det ska gå att lagra följande data på förarkortet för varje kalenderdag som kortet har använts och för varje användningsperiod för ett visst fordon den dagen (en användningsperiod inbegriper alla på varandra följande insättnings-/uttagscykler i fordonet för kortet i fråga):

— Datum och tidpunkt för första användning av fordonet (dvs. första insättning av kort under denna användningsperiod för fordonet, eller 00.00 om användningsperioden pågår vid den tidpunkten).

— Fordonets vägmätarvärde vid tidpunkten för första användning.

— Datum och tidpunkt för senaste användning av fordonet (dvs. senaste uttag av kort under denna användningsperiod för fordonet, eller 23.59 om användningsperioden pågår vid den tidpunkten).

— Fordonets vägmätarvärde vid tidpunkten för sista användning.

— Fordonets registreringsnummer (VRN) och registrerande medlemsstat.

— Fordonets identifieringsnummer (VIN).

295) Det ska gå att lagra minst 84 sådana poster på förarkortet.

4.5.3.2.11 Platser och positioner där dagens arbetsperioder påbörjas och/eller avslutas

296) Det ska gå att på förarkortet lagra följande data om de platser som anges av föraren där dagens arbetsperioder påbörjas och/eller avslutas:

— Datum och tidpunkt för angivelsen (eller datum/tidpunkt som avser angivelsen och som anges manuellt).

— Typ av angivelse (påbörjande eller avslutande, särskild omständighet).

— Det land och den region som anges.

— Fordonets vägmätarställning.

— Fordonets position.

— GNSS-precision, datum och tidpunkt när positionen fastställdes.

297) Det ska gå att lagra minst 84 par av sådana poster i förarkortets minne.

▼B

4.5.3.2.12 Data om kortsessioner

298) Det ska gå att på förarkortet lagra följande data om det fordon där den innevarande sessionen påbörjades:

— Datum och tidpunkt när sessionen påbörjades (dvs. för insättning av kort), med en upplösning av en (1) sekund.

— Fordonets registreringsnummer (VRN) och registrerande medlemsstat.

4.5.3.2.13 Data om kontrollaktiviteter

299) Det ska gå att lagra följande data om kontrollaktiviteter på förarkortet:

— Datum och tidpunkt för kontrollen.

— Kontrollkortsnummer och medlemsstat som utfärdat kortet.

— Kontrolltyp (visning och/eller utskrift och/eller överföring av data från fordonsenhet och/eller överföring av data från kort (se anmärkning)).

— Överförd period, om överföring utfördes.

— Registreringsnummer (VRN) och registrerande medlemsstat för det fordon i vilket kontrollen ägde rum.

Anmärkning: Säkerhetskraven medför att överföring av data från kort registreras endast om den gjorts genom en färdskrivare.

300) Det ska gå att lagra en (1) sådan post på förarkortet.

4.5.3.2.14 Data om särskilda omständigheter

301) Det ska gå att på förarkortet lagra följande data om de särskilda omständigheter som angavs medan kortet var insatt (oavsett kortplats):

— Datum och tidpunkt för angivelsen.

— Typ av särskild omständighet.

302) Det ska gå att lagra minst 56 sådana poster på förarkortet.

4.5.3.2.15 Data om använda fordonsenheter

303) Det ska gå att lagra följande data på förarkortet med avseende på de olika fordonsenheter där kortet använts:

— Datum och tidpunkt för påbörjande av fordonsenhetens användningsperiod (dvs. första insättning av kort i fordonsenheten under denna period).

— Fordonsenhetens tillverkare.

— Fordonsenhetens typ.

— Versionsnummer för fordonsenhetens programvara.

304) Det ska gå att lagra minst 84 sådana poster på förarkortet.

▼B

4.5.3.2.16 Data om platser avseende tre timmar sammanhängande körning

305) Det ska gå att lagra följande data på förarkortet om fordonets position när förarens sammanhängande körtid uppgår till en multipel av tre timmar:

— Datum och tidpunkt när kortinnehavarens sammanhängande körtid uppgår till en multipel av tre timmar.

— Fordonets position.

— GNSS-precision, datum och tidpunkt när positionen fastställdes.

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

4.5.4 *Verkstadskort*

4.5.4.1 Färdskrivartillämpning (tillgänglig för första och andra generationens fordonsenheter)

4.5.4.1.1 Tillämpningsidentifiering

307) Det ska gå att lagra följande data för tillämpningsidentifiering på verkstadskortet:

— Identifiering av färdskrivartillämpning.

— Identifiering av typ av färdskrivarkort.

4.5.4.1.2 Nycklar och certifikat

308) Verkstadskortet ska kunna lagra ett antal kryptografiska nycklar och certifikat, såsom anges i tillägg 11 del A.

309) Det ska gå att lagra ett personligt identifieringsnummer (en PIN-kod) på verkstadskortet.

4.5.4.1.3 Kortidentifiering

310) Det ska gå att lagra följande data för kortidentifiering på verkstadskortet:

— Kortnummer.

— Utfärdande medlemsstat, utfärdande myndighet, utfärdandedatum.

— Kortets första och sista giltighetsdag.

4.5.4.1.4 Identifiering av kortinnehavare

311) Det ska gå att lagra följande identifieringsdata för kortinnehavare på verkstadskortet:

— Verkstadens namn.

— Verkstadens adress.

— Innehavarens efternamn.

— Innehavarens förnamn.

— Valt språk.

4.5.4.1.5 Överföring från kort

312) På verkstadskortet ska det gå att lagra en post om överföring av data från kort på samma sätt som på ett förarkort.

▼B

4.5.4.1.6 Data om kalibrering och tidsinställning

313) På verkstadskortet ska det gå att lagra poster för kalibreringar och/eller tidsinställningar som utförts medan kortet var insatt i färdskrivaren.

314) Det ska gå att lagra följande data i varje kalibreringspost:

— Syfte med kalibreringen (aktivering, första installation, installation, periodisk besiktning).

— Fordonsidentifiering.

— Uppdaterade eller bekräftade parametrar (w, k, l, däcksdimension, den hastighetsbegränsande anordningens inställning, vägmätare (gamla och nya värden), datum och tidpunkt (gamla och nya värden).

— Identifiering av färdskrivaren (fordonsenhetens artikelnummer, fordonsenhetens serienummer, rörelsesensorns serienummer).

315) Det ska gå att lagra minst 88 sådana poster på verkstadskortet.

316) Verkstadskortet ska vara försett med en räknare som anger det sammanlagda antal kalibreringar som gjorts med kortet.

317) Verkstadskortet ska vara försett med en räknare som anger det antal kalibreringar som gjorts sedan dess senaste överföring.

4.5.4.1.7 Data om händelser och fel

318) På verkstadskortet ska det gå att lagra data om händelser och fel på samma sätt som på ett förarkort.

319) På verkstadskortet ska det gå att lagra data för de senaste tre händelserna av varje typ (dvs. 18 händelser) och de senaste sex felen av varje typ (dvs. 12 fel).

4.5.4.1.8 Data om föraraktiviteter

320) På verkstadskortet ska det gå att lagra data om föraraktiviteter på samma sätt som på ett förarkort.

321) Det ska gå att lagra data om föraraktiviteter på verkstadskortet för minst en dag av genomsnittlig föraraktivitet.

4.5.4.1.9 Data om använda fordon

322) På verkstadskortet ska det gå att lagra data om använda fordon på samma sätt som på ett förarkort.

323) Det ska gå att lagra minst 4 sådana poster på verkstadskortet.

4.5.4.1.10 Data om påbörjande och/eller avslutande av dagens arbetsperioder

324) På verkstadskortet ska det gå att lagra data om påbörjande och/eller avslutande av dagens arbetsperioder på samma sätt som på ett förarkort.

325) Det ska gå att lagra minst 3 par av sådana poster på verkstadskortet.

▼B

4.5.4.1.11 Data om kortsessioner

326) På verkstadskortet ska det gå att lagra data om kortsessioner på samma sätt som på ett förarkort.

4.5.4.1.12 Data om kontrollaktiviteter

327) På verkstadskortet ska det gå att lagra data om kontrollaktiviteter på samma sätt som på ett förarkort.

4.5.4.1.13 Data om särskilda omständigheter

328) På verkstadskortet ska det gå att lagra data om särskilda omständigheter på samma sätt som på ett förarkort.

329) Det ska gå att lagra minst 2 sådana poster på verkstadskortet.

4.5.4.2 Färdskrivartillämpning i generation 2 (ej åtkomlig för första generationens fordonsenhet)

4.5.4.2.1 Tillämpningsidentifiering

330) Det ska gå att lagra följande data för tillämpningsidentifiering på verkstadskortet:

— Identifiering av färdskrivartillämpning.

— Identifiering av typ av färdskrivarkort.

4.5.4.2.2 Nycklar och certifikat

331) Verkstadskortet ska kunna lagra ett antal kryptografiska nycklar och certifikat, såsom anges i tillägg 11 del B.

332) Det ska gå att lagra ett personligt identifieringsnummer (en PIN-kod) på verkstadskortet.

4.5.4.2.3 Kortidentifiering

333) Det ska gå att lagra följande data för kortidentifiering på verkstadskortet:

— Kortnummer.

— Utfärdande medlemsstat, utfärdande myndighet, utfärdandedatum.

— Kortets första och sista giltighetsdag.

4.5.4.2.4 Identifiering av kortinnehavare

334) Det ska gå att lagra följande identifieringsdata för kortinnehavare på verkstadskortet:

— Verkstadens namn.

— Verkstadens adress.

— Innehavarens efternamn.

— Innehavarens förnamn.

— Valt språk.

4.5.4.2.5 Överföring från kort

335) På verkstadskortet ska det gå att lagra en post om överföring av data från kort på samma sätt som på ett förarkort.

▼B

4.5.4.2.6 Data om kalibrering och tidsinställning

336) På verkstadskortet ska det gå att lagra poster för kalibreringar och/eller tidsinställningar som utförts medan kortet var insatt i färdskrivaren.

337) Det ska gå att lagra följande data i varje kalibreringspost:

— Syfte med kalibreringen (aktivering, första installation, installation, periodisk besiktning).

— Fordonsidentifiering.

— Uppdaterade eller bekräftade parametrar (w, k, l, däcksdimension, den hastighetsbegränsande anordningens inställning, vägmätare (gamla och nya värden), datum och tidpunkt (gamla och nya värden)).

— Identifiering av färdskrivaren (fordonsenhetens artikelnummer, fordonsenhetens serienummer, rörelsesensorns serienummer, serienumret för kommunikationsanordningen för fjärravläsning och den externa GNSS-anordningens serienummer, i förekommande fall).

— Typer och identifierare för samtliga befintliga plomberingar.

— Förmåga hos fordonsenheten att använda första generationens färdskrivarkort (aktiverad eller inte).

338) Det ska gå att lagra minst 88 sådana poster på verkstadskortet.

339) Verkstadskortet ska vara försett med en räknare som anger det sammanlagda antal kalibreringar som gjorts med kortet.

340) Verkstadskortet ska vara försett med en räknare som anger det antal kalibreringar som gjorts sedan dess senaste överföring.

4.5.4.2.7 Data om händelser och fel

341) På verkstadskortet ska det gå att lagra data om händelser och fel på samma sätt som på ett förarkort.

342) På verkstadskortet ska det gå att lagra data för de senaste tre händelserna av varje typ (dvs. 33 händelser) och de senaste sex felen av varje typ (dvs. 12 fel).

4.5.4.2.8 Data om föraraktiviteter

343) På verkstadskortet ska det gå att lagra data om föraraktiviteter på samma sätt som på ett förarkort.

344) Det ska gå att lagra data om föraraktiviteter på verkstadskortet för minst en dag av genomsnittlig föraraktivitet.

4.5.4.2.9 Data om använda fordon

345) På verkstadskortet ska det gå att lagra data om använda fordon på samma sätt som på ett förarkort.

346) Det ska gå att lagra minst 4 sådana poster på verkstadskortet.

▼B

4.5.4.2.10 Data om påbörjande och/eller avslutande av dagens arbetsperioder

347) På verkstadskortet ska det gå att lagra data om påbörjande och/eller avslutande av dagens arbetsperioder på samma sätt som på ett förarkort.

348) Det ska gå att lagra minst 3 par av sådana poster på verkstadskortet.

4.5.4.2.11 Data om kortsessioner

349) På verkstadskortet ska det gå att lagra data om kortsessioner på samma sätt som på ett förarkort.

4.5.4.2.12 Data om kontrollaktiviteter

350) På verkstadskortet ska det gå att lagra data om kontrollaktiviteter på samma sätt som på ett förarkort.

4.5.4.2.13 Data om använda fordonsenheter

351) Verkstadskortet ska kunna lagra följande data med avseende på de olika fordonsenheter där kortet använts:

— Datum och tidpunkt för påbörjande av fordonsenhetens användningsperiod (dvs. första insättning av kort i fordonsenheten under denna period).

— Fordonsenhetens tillverkare.

— Fordonsenhetens typ.

— Versionsnummer för fordonsenhetens programvara.

352) Det ska gå att lagra minst 4 sådana poster på verkstadskortet.

4.5.4.2.14 Data om platser avseende tre timmar sammanhängande körning

353) Det ska gå att lagra följande data på verkstadskortet om fordonets position när förarens sammanhängande körtid uppgår till en multipel av tre timmar:

— Datum och tidpunkt när kortinnehavarens sammanhängande körtid uppgår till en multipel av tre timmar.

— Fordonets position.

— GNSS-precision, datum och tidpunkt när positionen fastställdes.

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

4.5.4.2.15 Data om särskilda omständigheter

355) På verkstadskortet ska det gå att lagra data om särskilda omständigheter på samma sätt som på ett förarkort.

356) Det ska gå att lagra minst 2 sådana poster på verkstadskortet.

▼B

4.5.5 *Kontrollkort*

4.5.5.1 Färdskrivartillämpning (tillgänglig för första och andra generationens fordonsenheter)

4.5.5.1.1 Tillämpningsidentifiering

357) Det ska gå att lagra följande data för tillämpningsidentifiering på kontrollkortet:

— Identifiering av färdskrivartillämpning.

— Identifiering av typ av färdskrivarkort.

4.5.5.1.2 Nycklar och certifikat

358) Kontrollkortet ska kunna lagra ett antal kryptografiska nycklar och certifikat, såsom anges i tillägg 11 del A.

4.5.5.1.3 Kortidentifiering

359) Det ska gå att lagra följande data för kortidentifiering på kontrollkortet:

— Kortnummer.

— Utfärdande medlemsstat, utfärdande myndighet, utfärdandedatum.

— Kortets första och sista giltighetsdag (i förekommande fall).

4.5.5.1.4 Identifiering av kortinnehavare

360) Det ska gå att lagra följande identifieringsdata för kortinnehavare på kontrollkortet:

— Kontrollorganets namn.

— Kontrollorganets adress.

— Innehavarens efternamn.

— Innehavarens förnamn.

— Valt språk.

4.5.5.1.5 Data om kontrollaktiviteter

361) Det ska gå att lagra följande data om kontrollaktiviteter på kontrollkortet:

— Datum och tidpunkt för kontrollen.

— Kontrolltyp (visning och/eller utskrift och/eller överföring av data från fordonsenhet och/eller överföring av data från kort och/eller kalibreringskontroll på väg).

— Överförd period (i förekommande fall).

— Fordonets registreringsnummer (VRN) och myndighet i medlemsstaten som registrerat det kontrollerade fordonet.

— Kortnummer och medlemsstat som utfärdat det kontrollerade förarkortet.

362) Det ska gå att lagra minst 230 sådana poster på kontrollkortet.

▼B

4.5.5.2 Färdskrivartillämpning G2 (ej åtkomlig för första generationens fordonsenhet)

4.5.5.2.1 Tillämpningsidentifiering

363) Det ska gå att lagra följande data för tillämpningsidentifiering på kontrollkortet:

— Identifiering av färdskrivartillämpning.

— Identifiering av typ av färdskrivarkort.

4.5.5.2.2 Nycklar och certifikat

364) Kontrollkortet ska kunna lagra ett antal kryptografiska nycklar och certifikat, såsom anges i tillägg 11 del B.

4.5.5.2.3 Kortidentifiering

365) Det ska gå att lagra följande data för kortidentifiering på kontrollkortet:

— Kortnummer.

— Utfärdande medlemsstat, utfärdande myndighet, utfärdandedatum.

— Kortets första och sista giltighetsdag (i förekommande fall).

4.5.5.2.4 Identifiering av kortinnehavare

366) Det ska gå att lagra följande identifieringsdata för kortinnehavare på kontrollkortet:

— Kontrollorganets namn.

— Kontrollorganets adress.

— Innehavarens efternamn.

— Innehavarens förnamn.

— Valt språk.

4.5.5.2.5 Data om kontrollaktiviteter

367) Det ska gå att lagra följande data om kontrollaktiviteter på kontrollkortet:

— Datum och tidpunkt för kontrollen.

— Kontrolltyp (visning och/eller utskrift och/eller överföring av data från fordonsenhet och/eller överföring av data från kort och/eller kalibreringskontroll på väg).

— Överförd period (i förekommande fall).

— Fordonets registreringsnummer (VRN) och myndighet i medlemsstaten som registrerat det kontrollerade fordonet.

— Kortnummer och medlemsstat som utfärdat det kontrollerade förarkortet.

368) Det ska gå att lagra minst 230 sådana poster på kontrollkortet.

▼B

4.5.6 *Företagskort*

4.5.6.1 Färdskrivartillämpning (tillgänglig för första och andra generationens fordonsenheter)

4.5.6.1.1 Tillämpningsidentifiering

369) Det ska gå att lagra följande data för tillämpningsidentifiering på företagskortet:

— Identifiering av färdskrivartillämpning.

— Identifiering av typ av färdskrivarkort.

4.5.6.1.2 Nycklar och certifikat

370) Företagskortet ska kunna lagra ett antal kryptografiska nycklar och certifikat, såsom anges i tillägg 11 del A.

4.5.6.1.3 Kortidentifiering

371) Det ska gå att lagra följande data för kortidentifiering på företagskortet:

— Kortnummer.

— Utfärdande medlemsstat, utfärdande myndighet, utfärdandedatum.

— Kortets första och sista giltighetsdag (i förekommande fall).

4.5.6.1.4 Identifiering av kortinnehavare

372) Det ska gå att lagra följande identifieringsdata för kortinnehavare på företagskortet:

— Företagets namn.

— Företagets adress.

4.5.6.1.5 Data om företagsaktiviteter

373) Det ska gå att lagra följande data om företagsaktiviteter på företagskortet:

— Datum och tidpunkt för aktiviteten.

— Typ av aktivitet (låsning och/eller öppning av fordonsenhet, och/eller överföring av data från fordonsenhet och/eller överföring av data från kort).

— Överförd period (i förekommande fall).

— Fordonets registreringsnummer (VRN) och myndighet i medlemsstaten som registrerat fordonet.

— Kortnummer och medlemsstat som utfärdat kortet (vid överföring från kort).

374) Det ska gå att lagra minst 230 sådana poster på företagskortet.

▼B

4.5.6.2 Färdskrivartillämpning G2 (ej åtkomlig för första generationens fordonsenhet)

4.5.6.2.1 Tillämpningsidentifiering

375) Det ska gå att lagra följande data för tillämpningsidentifiering på företagskortet:

— Identifiering av färdskrivartillämpning.

— Identifiering av typ av färdskrivarkort.

4.5.6.2.2 Nycklar och certifikat

376) Företagskortet ska kunna lagra ett antal kryptografiska nycklar och certifikat, såsom anges i tillägg 11 del B.

4.5.6.2.3 Kortidentifiering

377) Det ska gå att lagra följande data för kortidentifiering på företagskortet:

— Kortnummer.

— Utfärdande medlemsstat, utfärdande myndighet, utfärdandedatum.

— Kortets första och sista giltighetsdag (i förekommande fall).

4.5.6.2.4 Identifiering av kortinnehavare

378) Det ska gå att lagra följande identifieringsdata för kortinnehavare på företagskortet:

— Företagets namn.

— Företagets adress.

4.5.6.2.5 Data om företagsaktiviteter

379) Det ska gå att lagra följande data om företagsaktiviteter på företagskortet:

— Datum och tidpunkt för aktiviteten.

— Typ av aktivitet (låsning och/eller öppning av fordonsenhet, och/eller överföring av data från fordonsenhet och/eller överföring av data från kort).

— Överförd period (i förekommande fall).

— Fordonets registreringsnummer (VRN) och myndighet i medlemsstaten som registrerat fordonet.

— Kortnummer och medlemsstat som utfärdat kortet (vid överföring från kort).

380) Det ska gå att lagra minst 230 sådana poster på företagskortet.

5 INSTALLATION AV FÄRDSKRIVARE

5.1 **Installation**

381) Nya färdskrivare får inte vara aktiverade när de levereras till montörer eller fordonstillverkare, och alla de kalibreringsparametrar som är förtecknade i avsnitt 3.21 ska vara inställda på passande och giltiga standardvärden. Om det inte finns något passande värde ska standardvärdet för alfanumeriska parametrar vara en sträng med ”?” och för numeriska parametrar ”0”. Leverans av säkerhetsrelaterade delar till färdskrivaren kan vid behov begränsas under säkerhetscertifieringen.

▼B

382) Innan färdskrivaren aktiveras ska den ge tillgång till kalibreringsfunktionen även om den inte är i kalibreringsläge.

383) Innan färdskrivaren aktiveras ska den varken registrera eller lagra de data som avses i punkterna 3.12.3, 3.12.9 och 3.12.12–3.12.15.

384) Vid installationen ska fordonstillverkaren förinställa alla kända parametrar.

385) Fordonstillverkare eller montörer ska aktivera den installerade färdskrivaren senast innan fordonet används inom ramen för förordning (EG) nr 561/2006.

386) Aktiveringen av färdskrivaren ska utlösas automatiskt första gången ett verkstadskort sätts in i någon av kortläsarna.

387) Den särskilda parning som krävs mellan rörelsesensorn och fordonsenheten ska i förekommande fall ske automatiskt före eller under aktivering.

388) Den särskilda koppling som krävs mellan den externa GNSS-anordningen och fordonsenheten ska i förekommande fall ske automatiskt före eller under aktivering.

389) Efter det att färdskrivaren har aktiverats ska den till fullo upprätthålla funktioner och tillträdesrättigheter till data.

390) Efter det att färdskrivaren har aktiverats ska den kommunicera de skyddade data som krävs för riktade vägkontroller till kommunikationsanordningen för fjärravläsning.

391) Färdskrivarens registrerings- och lagringsfunktioner ska vara helt klara för drift när den har aktiverats.

392) Installationen ska följas av en kalibrering. Vid den första kalibreringen behöver fordonets registreringsnummer (VRN) inte anges om den godkända verkstad som ska utföra kalibreringen inte känner till detta nummer. Endast i ett sådant fall får fordonsägaren ange registreringsnumret (VRN) med hjälp av sitt företagskort innan fordonet används inom ramen för förordning (EG) nr 561/2006 (t.ex. med hjälp av kommandon i en ändamålsenlig menystruktur i fordonsenhetens användargränssnitt) ([1]). Denna registrering ska endast kunna uppdateras eller bekräftas med hjälp av ett verkstadskort.

393) Installation av en extern GNSS-anordning förutsätter koppling med fordonsenheten och efterföljande kontroll av positionsinformationen från GNSS.

394) Färdskrivaren ska placeras i fordonet på så sätt att de nödvändiga funktionerna kan nås från förarplatsen.

([1]) EGT L 102, 11.4.2006, s.1.

▼B

5.2 **Installationsskylt**

395) Efter det att färdskrivaren har kontrollerats vid installationen ska en installationsskylt med permanent gravering eller tryck anbringas på färdskrivaren så att skylten är väl synlig och lätt tillgänglig. Om så inte är möjligt ska skylten anbringas på fordonets B-stolpe så att den är väl synlig. För fordon som saknar B-stolpe ska installationsskylten anbringas på dörrkarmen och under alla omständigheter vara väl synlig.

Efter varje besiktning av en godkänd montör eller verkstad ska skylten ersättas med en ny skylt.

396) På skylten ska åtminstone följande uppgifter finnas:

— Godkänd montörs eller verkstads namn och adress eller handelsbeteckning.

— Fordonets karakteristiska koefficient, uttryckt som ”w = … imp/km”.

— Färdskrivarkonstanten, uttryckt som ”k = … imp/km”.

— Däckens effektiva omkrets, uttryckt som ”l = … mm”.

— Däcksdimension.

— Datum för mätning av fordonets karakteristiska koefficient och däckens effektiva omkrets.

— Fordonets registreringsnummer.

— Förekomst (eller inte) av en extern GNSS-anordning.

— Den externa GNSS-anordningens serienummer.

— Serienummer för kommunikationsanordningen för fjärravläsning.

— 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.

397) En andra skylt får användas endast när det gäller fordon som tillhör kategorierna M1 och N1 och är utrustade med en adapter i enlighet med kommissionens förordning (EG) nr 68/2009 ([1]) i sin senaste lydelse, och om det inte är möjligt att ta med all information som beskrivs i krav 396. I sådana fall ska denna andra skylt innehålla minst de sista fyra strecksatserna i krav 396.

([1]) Kommissionens förordning (EG) nr 68/2009 av den 23 januari 2009 om anpassning för nionde gången till den tekniska utvecklingen av rådets förordning (EEG) nr 3821/85 om färdskrivare vid vägtransporter (EUT L 21, 24.1.2009, s. 3).

▼B

Om en sådan andra skylt används ska den anbringas nära eller bredvid den första skylten som beskrivs i krav 396, och den ska ha samma skyddsnivå. Den andra skylten ska också innehålla namn, adress eller handelsnamn för den godkända montör eller verkstad som utförde installationen, samt datum för installationen.

5.3 **Plombering**

398) Följande komponenter ska plomberas:

— Varje anslutning som om den bryts skulle orsaka förändringar eller förlust av data som inte upptäcks (detta kan gälla t.ex. rörelsesensorns infästning på växellådan, adaptern i M1/N1-fordon, den externa GNSS-anslutningen eller fordonsenheten).

— Installationsskylten, om den inte är anbringad på sådant sätt att den inte kan avlägsnas utan att texten på den förstörs.

399) Ovan nämnda plomberingar får avlägsnas

— i nödsituationer,

— för att installera, anpassa eller reparera en hastighetsbegränsande anordning eller andra anordningar som bidrar till trafiksäkerheten, förutsatt att färdskrivaren fortsätter att fungera på tillförlitligt och avsett sätt och att den åter plomberas av en godkänd montör eller verkstad (i enlighet med kapitel 6) omedelbart efter det att den hastighetsbegränsande anordningen eller någon annan anordning som bidrar till trafiksäkerheten har monterats, eller inom 7 dagar i övriga fall.

400) Varje gång dessa plomberingar bryts ska en skriftlig rapport upprättas som redovisar skälen för åtgärden och som ställs till den behöriga myndighetens förfogande.

401) Plomberingar ska ha ett identifieringsnummer som tilldelas av dess tillverkare. Detta nummer ska vara unikt och skilt från varje annat plomberingsnummer som tilldelats av någon annan tillverkare av plomberingar.

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

402) Plomberingarna ska ha ett fritt utrymme där godkända montörer, verkstäder eller fordonstillverkare kan lägga till ett särskilt märke i enlighet med artikel 22.3 i förordning (EU) nr 165/2014.

Detta märke får inte dölja plomberingens identifieringsnummer.

403) Tillverkare av plomberingar ska registreras i en särskild databas och offentliggöra sina plomberingsnummer genom ett förfarande som ska fastställas av Europeiska kommissionen.

404) Godkända verkstäder och fordonstillverkare ska, inom ramen för förordning (EU) nr 165/2014, endast använda plomberingar från de tillverkare av plomberingar som ingår i den ovan nämnda databasen.

▼B

405) Tillverkare av plomberingar och deras distributörer ska upprätthålla register som ger full spårbarhet för försålda plomberingar som ska användas inom ramen för förordning (EU) nr 165/2014 och ska vara beredda att överlämna dessa till de behöriga nationella myndigheterna närhelst detta behövs.

406) Plomberingarnas unika identifieringsnummer ska vara synliga på installationsskylten.

6 KONTROLLER, BESIKTNINGAR OCH REPARATIONER

Bestämmelserna för när plomberingarna får avlägsnas, såsom avses i artikel 22.5 i förordning (EU) nr 165/2014, anges i avsnitt 5.3 i denna bilaga.

6.1 **Godkännande av montörer, verkstäder och fordonstillverkare**

Medlemsstaterna ska godkänna, regelbundet kontrollera och auktorisera de organ som ska utföra

— installationer,

— kontroller,

— besiktningar,

— reparationer.

Såvida inte något annat vederbörligen motiveras ska verkstadskort endast utfärdas till de montörer och/eller verkstäder som godkänts för aktivering och/eller kalibrering av färdskrivare i enlighet med denna bilaga och

— som inte är berättigade till ett företagskort,

— och vars övriga yrkesverksamhet inte riskerar att äventyra den övergripande systemsäkerheten enligt krav i tillägg 10.

6.2 **Kontroll av nya eller reparerade komponenter**

407) Varje enskild anordning, vare sig 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, och sedan plomberas i enlighet med avsnitt 5.3.

6.3 **Installationsbesiktning**

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.

6.4 **Periodiska besiktningar**

409) Periodiska besiktningar av färdskrivarutrustning i fordon ska ske efter varje reparation av färdskrivarutrustningen, när fordonets karakteristiska koefficient eller däckens effektiva omkrets har ändrats, när färdskrivarens UTC-tid visar fel med mer än 20 minuter eller när fordonets registreringsnummer (VRN) har ändrats, och åtminstone en gång inom två år (24 månader) efter den senaste besiktningen.

410) Dessa besiktningar ska omfatta följande kontroller:

— Att färdskrivaren fungerar riktigt, inbegripet funktionen för datalagring på färdskrivarkort och kommunikationen med fjärravläsare.

▼B

— Att efterlevnaden av bestämmelserna i avsnitten 3.2.1 och 3.2.2 om största tillåtna toleranser vid installation är säkerställd.

— Att efterlevnaden av bestämmelserna i avsnitten 3.2.3 och 3.3 är säkerställd.

— Att typgodkännandemärket finns på färdskrivaren.

— Att den installationsskylt som anges i krav 396 och den typskylt som anges i krav 225 är anbringade.

— Att däcksdimensioner och däckens faktiska omkrets stämmer.

— Att ingen utrustning för att manipulera färdskrivaren är kopplad till utrustningen.

— Att plomberingarna är korrekt placerade och i gott skick, att deras identifieringsnummer är giltiga (referens till tillverkaren av plomberingen i EU-kommissionens databas) och att deras identifieringsnummer stämmer med de som finns på installationsskylten (se krav 401).

411) Om det konstateras att någon av de händelser som anges i avsnitt 3.9 om upptäckt av händelser och/eller fel har förekommit sedan den senaste besiktningen och som färdskrivartillverkare och/eller nationella myndigheter anser kan äventyra utrustningens säkerhet ska verkstaden

a. jämföra identifieringsdata för den rörelsesensor som är inkopplad i växellådan med identifieringsdata för den kopplade rörelsesensor som är registrerad i fordonsenheten,

b. kontrollera om informationen på installationsskylten stämmer överens med informationen i fordonsenhetens register,

c. kontrollera om rörelsesensorns serienummer och typgodkännandenummer – om dessa anges på rörelsesensorn – stämmer överens med informationen i färdskrivarens dataminne,

d. jämföra identifieringsdata på den externa GNSS-anordningens typskylt, om sådana finns, med de som är lagrade i fordonsenhetens dataminne.

412) Verkstäderna ska i sina besiktningsrapporter ange om brutna plomberingar eller manipuleringsutrustning har upptäckts. Dessa rapporter ska sparas av verkstäderna i minst två år och på förfrågan ställas till den behöriga myndighetens förfogande.

413) Dessa besiktningar ska inbegripa en kalibrering och ett förebyggande byte av de plomberingar vars anbringande ligger inom verkstädernas ansvar..

6.5 **Uppmätning av fel**

414) Uppmätning av fel vid installation och i drift ska genomföras under följande förutsättningar, vilka ska anses utgöra standardiserade provningsförhållanden:

— Fordon utan last och i körklart skick.

— Däcktryck enligt tillverkarens anvisningar.

▼B

— Däckförslitning inom av nationell lag tillåtna gränsvärden.

— Fordonets rörelse:

— Fordonet ska, framdrivet av sin egen motor, röra sig framåt i rät linje och på jämnt underlag med en hastighet av 50 ± 5 km/h. Mätsträckan ska vara åtminstone 1 000 m.

— Förutsatt att provningen kan ske med jämförbar precision får även alternativa metoder, t.ex. en passande provbänk, användas vid provningen.

6.6 **Reparationer**

415) Verkstäderna ska kunna överföra data från färdskrivare för att kunna återlämna dessa data till berört transportföretag.

416) Godkända verkstäder ska till transportföretagen utfärda ett intyg om att data inte går att överföra, om data som registrerats tidigare inte kan överföras på grund av att färdskrivaren inte fungerar korrekt även efter reparation i den berörda verkstaden. Verkstäderna ska behålla en kopia av varje utfärdat intyg i minst ett år.

7 UTFÄRDANDE AV KORT

De förfaranden för utfärdande av kort som medlemsstaterna upprättar ska överensstämma med följande:

417) Numret på det färdskrivarkort som utfärdas för första gången till en sökande ska ha ett löpnummer (i förekommande fall) och ett ersättningsindex och ett förnyelseindex som alla sätts till ”0”.

418) Kortnumren på alla opersonliga färdskrivarkort som har utfärdats till ett enskilt kontrollorgan, en enskild verkstad eller ett enskilt transportföretag ska ha samma 13 första siffror, och samtliga ska ha sitt eget löpnummer.

419) Ett färdskrivarkort som utfärdas som ersättning för ett befintligt färdskrivarkort ska ha samma kortnummer som det ersatta kortet förutom att ersättningsindex ska ökas med ”1” (i ordningen 0, …, 9, A, …, Z).

420) Ett färdskrivarkort som utfärdas som ersättning för ett befintligt färdskrivarkort ska ha samma sista giltighetsdag som det ersatta kortet.

421) Ett färdskrivarkort som utfärdas som förnyelse av ett befintligt färdskrivarkort ska ha samma kortnummer som det förnyade kortet förutom att ersättningsindex åter ska sättas till ”0” och att förnyelseindex ska ökas med ”1” (i ordningen 0, …, 9, A, …, Z).

422) Utbyte av ett befintligt färdskrivarkort för att ändra administrativa uppgifter ska ske i enlighet med reglerna för förnyelse om det sker i samma medlemsstat, eller reglerna för det första utfärdandet om det utförs av en annan medlemsstat.

423) Utrymmet för kortinnehavarens efternamn ska, när det gäller icke-personliga verkstads- eller kontrollkort, användas för verkstadens eller kontrollorganets namn eller för montörens eller kontrolltjänstemannens namn, om medlemsstaten bestämmer detta.

▼B

424) Medlemsstater ska utväxla data elektroniskt för att i enlighet med artikel 31 i förordning (EU) nr 165/2014 säkerställa att varje förarkort som de utfärdar är unikt.

8 TYPGODKÄNNANDE AV FÄRDSKRIVARE OCH FÄRDSKRIVARKORT

8.1 **Allmänt**

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 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 sin komponent tillsammans med alla typer av rörelsesensorer, externa GNSS-anordningar och vice versa, under förutsättning att varje komponent uppfyller kraven i denna bilaga. Som ett alternativ får tillverkare även ansöka om typgodkännande av färdskrivare.

425) Färdskrivare ska lämnas in för typgodkännande, komplett med eventuella integrerade extra anordningar.

426) Typgodkännande av färdskrivare och färdskrivarkort ska inbegripa säkerhetsprovningar, funktionsprovningar och provningar med avseende på driftskompatibilitet. Positiva resultat från var och en av dessa provningar ska anges i ett lämpligt intyg.

427) Medlemsstaternas myndigheter för typgodkännande får inte bevilja något intyg om typgodkännande om de inte har

— ett säkerhetsintyg,

— ett funktionsintyg, och

— ett intyg om driftskompatibilitet

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

428) Varje ändring av färdskrivarens programvara eller maskinvara eller av det slag av material som används för dess tillverkning ska, innan den tas i bruk, anmälas till den myndighet som beviljade typgodkännandet av färdskrivaren. Denna myndighet ska för tillverkaren bekräfta utvidgningen av typgodkännandet, eller får begära en uppdatering eller bekräftelse av berörda funktionsintyg, säkerhetsintyg och/eller intyg om driftskompatibilitet.

429) Förfaranden för att uppgradera programvaran i färdskrivaren på plats ska godkännas av den myndighet som beviljade typgodkännandet av färdskrivaren. Uppgradering av programvaran får inte innebära att de föraraktivitetsdata som finns lagrade i färdskrivaren ändras eller tas bort. Programvaran får bara uppgraderas under färdskrivartillverkarens ansvar.

430) Typgodkännande av programvaruändringar som syftar till att uppgradera en redan typgodkänd färdskrivare får inte avvisas om dessa ändringar endast gäller funktioner som inte specificeras i denna bilaga. Programvaruuppgradering i en färdskrivare får utesluta införande av nya teckenmängder om detta inte är tekniskt genomförbart.

▼B

8.2 **Säkerhetsintyg**

431) Säkerhetsintyget ska utfärdas i enlighet med bestämmelserna i tillägg 10 till denna bilaga. Intyget krävs för följande färdskrivarkomponenter: fordonsenhet, rörelsesensor, extern GNSS-anordning och färdskrivarkort.

432) I de exceptionella fall då de myndigheter som ansvarar för säkerhetscertifieringen vägrar att certifiera ny utrustning med hänvisning till att säkerhetsmekanismerna är föråldrade ska typgodkännandet endast i dessa specifika och exceptionella fall fortsätta att beviljas om det inte finns någon annan lösning som är förenlig med förordningen.

433) I sådana fall ska den berörda medlemsstaten utan dröjsmål underrätta Europeiska kommissionen, som inom tolv kalendermånader efter det att typgodkännandet har utfärdats ska inleda ett förfarande för att säkerställa att säkerheten har återställts till sin ursprungliga nivå.

8.3 **Funktionsintyg**

434) Alla som ansöker om typgodkännande ska förse medlemsstatens myndighet för typgodkännande med allt det material och alla de handlingar som myndigheten anser nödvändiga.

435) Tillverkare ska inom en månad efter en sådan begäran tillhandahålla relevanta prover av de produkter som ansökan om typgodkännande gäller, samt tillhörande dokumentation, som begärs av de laboratorier som har utsetts till att utföra funktionsprovningar. Eventuella kostnader till följd av en sådan begäran ska bäras av den begärande enheten. Laboratorier ska behandla alla kommersiellt känsliga uppgifter förtroligt.

436) Ett funktionsintyg får inte utfärdas till en tillverkare förrän minst alla de funktionsprovningar som anges i tillägg 9 har genomgåtts med positivt resultat.

437) Myndigheten för typgodkännande ska utfärda funktionsintyget. Förutom mottagarens namn och identifiering av modellen ska detta intyg innehålla en detaljerad förteckning över utförda provningar och erhållna resultat.

438) Funktionsintyget för en färdskrivarkomponent ska även innehålla uppgift om typgodkännandenumren för de andra typgodkända kompatibla färdskrivarkomponenter som provats i samband med komponentens certifiering.

439) Funktionsintyget för en färdskrivarkomponent ska även ange den ISO- eller CEN-standard som använts vid certifieringen av funktionsgränssnittet.

8.4 **Intyg om driftskompatibilitet**

440) Provningar av driftskompatibilitet ska utföras av ett enda laboratorium under Europeiska kommissionens ansvar och överinseende.

441) Laboratoriet ska registrera de ansökningar om provningar av driftskompatibilitet som tillverkare lämnar in i den ordning som de inkommer.

442) Ansökningarna får inte registreras officiellt förrän laboratoriet förfogar över

— allt det material och alla de handlingar som krävs för provningen av driftskompatibilitet,

▼B

— motsvarande säkerhetsintyg, och

— motsvarande funktionsintyg.

Tillverkaren ska informeras om registreringsdatum för ansökan.

443) Laboratoriet får inte utföra några provningar av driftskompatibiliteten hos en färdskrivare eller ett färdskrivarkort för vilka något säkerhetsintyg och funktionsintyg inte har beviljats, utom i det exceptionella fall som beskrivs i krav 432.

444) En tillverkare som ansöker om provningar av driftskompatibilitet ska åta sig att till det laboratorium som ansvarar för provningarna överlämna allt det material och alla de handlingar som tillverkaren anskaffat för att utföra provningarna.

445) Provningar av driftskompatibilitet ska, i enlighet med bestämmelserna i tillägg 9 till denna bilaga, utföras för alla de typer av färdskrivare och färdskrivarkort

— för vilka typgodkännandet fortfarande gäller, eller

— för vilka typgodkännandet håller på att avgöras och ett giltigt intyg om driftskompatibilitet redan finns.

446) Provningen av driftskompatibilitet ska omfatta samtliga generationer av färdskrivare eller färdskrivarkort som fortfarande är i bruk.

447) Laboratoriet får inte utfärda intyget om driftskompatibilitet till tillverkaren förrän alla nödvändiga provningar av driftskompatibilitet har genomgåtts med positivt resultat.

448) Om provningarna av driftskompatibilitet inte har genomgåtts med positivt resultat för en eller flera färdskrivare eller färdskrivarkort får något intyg om driftskompatibilitet inte utfärdas förrän den ansökande tillverkaren har genomfört nödvändiga ändringar och klarat provningarna av driftskompatibilitet. Laboratoriet ska identifiera orsaken till problemet, med hjälp av de tillverkare som berörs av detta driftskompatibilitetsfel, och ska försöka hjälpa den ansökande tillverkaren att finna en teknisk lösning. Om tillverkaren har ändrat sin produkt är det tillverkarens ansvar att hos berörda myndigheter förvissa sig om att säkerhetsintyget och funktionsintygen fortfarande gäller.

449) Intyget om driftskompatibilitet gäller i sex månader. Det återkallas vid utgången av denna period om tillverkaren inte har erhållit ett motsvarande intyg om typgodkännande. Tillverkaren ska vidarebefordra det till den myndighet för typgodkännande i den medlemsstat som har utfärdat funktionsintyget.

450) Delar som kan ligga till grund för driftskompatibilitetsfel får inte användas i vinstsyfte eller leda till dominant ställning.

8.5 **Intyg om typgodkännande**

451) Medlemsstatens myndighet för typgodkännande får utfärda intyget om typgodkännande så snart som den har de tre nödvändiga intygen.

▼B

452) Intyget om typgodkännande för en färdskrivarkomponent ska även innehålla uppgift om typgodkännandenumren för den övriga typgodkända driftskompatibla färdskrivarutrustningen.

453) Myndigheten för typgodkännande ska ge en kopia av intyget om typgodkännande till det laboratorium som ansvarar för provningarna av driftskompatibiliteten vid den tidpunkt då intyget utfärdas till tillverkaren.

454) Det laboratorium som är behörigt för provningar av driftskompatibilitet ska ha en offentlig webbplats med en uppdaterad förteckning över de färdskrivar- eller färdskrivarkortsmodeller

— för vilka en ansökan om provningar av driftskompatibilitet har registrerats,

— för vilka intyg (även provisoriskt) om driftskompatibilitet har erhållits, och

— för vilka intyg om typgodkännande har erhållits.

8.6 **Undantagsförfarande: första intyg om driftskompatibilitet för andra generationens färdskrivare och färdskrivarkort**

455) Inom fyra månader efter det att en första uppsättning av andra generationens färdskrivare och färdskrivarkort (förarkort, verkstadskort, kontrollkort och företagskort) har intygats vara driftskompatibla ska alla utfärdade intyg om driftskompatibilitet (inbegripet de första), med avseende på de ansökningar som registrerats under denna period, anses vara provisoriska.

456) Om alla berörda produkter vid utgången av denna period är ömsesidigt driftskompatibla ska alla motsvarande intyg om driftskompatibilitet bli slutliga.

457) Om driftskompatibilitetsfel påträffas under denna period ska det laboratorium som ansvarar för provningarna av driftskompatibilitet identifiera orsakerna till problemen med hjälp av alla berörda tillverkare, och uppmana dem att genomföra nödvändiga ändringar.

458) Om driftskompatibilitetsproblemen kvarstår vid utgången av denna period ska det laboratorium som ansvarar för provningarna av driftskompatibilitet, i samarbete med berörda tillverkare och med de myndigheter för typgodkännande som utfärdade motsvarande funktionsintyg, ta reda på orsakerna till kompatibilitetsfelen och ange vilka ändringar som var och en av de berörda tillverkarna bör göra. Sökandet efter tekniska lösningar får pågå i högst två månader. Om ingen gemensam lösning har hittats ska kommissionen därefter, efter att ha rådfrågat det laboratorium som ansvarar för provningarna av driftskompatibiliteten, avgöra för vilken eller vilka färdskrivare och för vilket eller vilka kort ett slutligt intyg om driftskompatibilitet beviljas, och motivera detta.

459) Alla de ansökningar om provningar av driftskompatibilitet som laboratoriet registrerar, mellan utgången av fyramånadersperioden efter det att det första provisoriska intyget om driftskompatibilitet har utfärdats och datumet för det beslut av kommissionen som avses i krav 455, ska senareläggas tills de inledande kompatibilitetsproblemen har lösts. Dessa ansökningar handläggs sedan i den ordning de registrerats.

▼B

Tillägg 1

DATAKATALOG

INNEHÅLLSFÖRTECKNING

1. INLEDNING

1.1. Metod för definition av datatyper

1.2. Referenser

2. DEFINITIONER AV DATATYPER

2.1. ActivityChangeInfo

2.2. Address

2.3. AESKey

2.4. AES128Key

2.5. AES192Key

2.6. AES256Key

2.7. BCDString

2.8. CalibrationPurpose

2.9. CardActivityDailyRecord

2.10. CardActivityLengthRange

2.11. CardApprovalNumber

2.12. CardCertificate

2.13. CardChipIdentification

2.14. CardConsecutiveIndex

2.15. CardControlActivityDataRecord

2.16. CardCurrentUse

2.17. CardDriverActivity

2.18. CardDrivingLicenceInformation

2.19. CardEventData

2.20. CardEventRecord

2.21. CardFaultData

2.22. CardFaultRecord

2.23. CardIccIdentification

2.24. CardIdentification

2.25. CardMACertificate

2.26. CardNumber

2.27. CardPlaceDailyWorkPeriod

2.28. CardPrivateKey

2.29. CardPublicKey

▼B

2.30. CardRenewalIndex

2.31. CardReplacementIndex

2.32. CardSignCertificate

2.33. CardSlotNumber

2.34. CardSlotsStatus

2.35. CardSlotsStatusRecordArray

2.36. CardStructureVersion

2.37. CardVehicleRecord

2.38. CardVehiclesUsed

2.39. CardVehicleUnitRecord

2.40. CardVehicleUnitsUsed

2.41. Certificate

2.42. CertificateContent

2.43. CertificateHolderAuthorisation

2.44. CertificateRequestID

2.45. CertificationAuthorityKID

2.46. CompanyActivityData

2.47. CompanyActivityType

2.48. CompanyCardApplicationIdentification

2.49. CompanyCardHolderIdentification

2.50. ControlCardApplicationIdentification

2.51. ControlCardControlActivityData

2.52. ControlCardHolderIdentification

2.53. ControlType

2.54. CurrentDateTime

2.55. CurrentDateTimeRecordArray

2.56. DailyPresenceCounter

2.57. Datef

2.58. DateOfDayDownloaded

2.59. DateOfDayDownloadedRecordArray

2.60. Distance

2.61. DriverCardApplicationIdentification

▼B

2.62. DriverCardHolderIdentification

2.63. DSRCSecurityData

2.64. EGFCertificate

2.65. EmbedderIcAssemblerId

2.66. EntryTypeDailyWorkPeriod

2.67. EquipmentType

2.68. EuropeanPublicKey

2.69. EventFaultRecordPurpose

2.70. EventFaultType

2.71. ExtendedSealIdentifier

2.72. ExtendedSerialNumber

2.73. FullCardNumber

2.74. FullCardNumberAndGeneration

2.75. Generation

2.76. GeoCoordinates

2.77. GNSSAccuracy

2.78. GNSSContinuousDriving

2.79. GNSSContinuousDrivingRecord

2.80. GNSSPlaceRecord

2.81. HighResOdometer

2.82. HighResTripDistance

2.83. HolderName

2.84. InternalGNSSReceiver

2.85. K-ConstantOfRecordingEquipment

2.86. KeyIdentifier

2.87. KMWCKey

2.88. Language

2.89. LastCardDownload

2.90. LinkCertificate

2.91. L-TyreCircumference

2.92. MAC

2.93. ManualInputFlag

2.94. ManufacturerCode

2.95. ManufacturerSpecificEventFaultData

2.96. MemberStateCertificate

▼B

2.97. MemberStateCertificateRecordArray

2.98. MemberStatePublicKey

2.99. Namn

2.100. NationAlpha

2.101. NationNumeric

2.102. NoOfCalibrationRecords

2.103. NoOfCalibrationsSinceDownload

2.104. NoOfCardPlaceRecords

2.105. NoOfCardVehicleRecords

2.106. NoOfCardVehicleUnitRecords

2.107. NoOfCompanyActivityRecords

2.108. NoOfControlActivityRecords

2.109. NoOfEventsPerType

2.110. NoOfFaultsPerType

2.111. NoOfGNSSCDRecords

2.112. NoOfSpecificConditionRecords

2.113. OdometerShort

2.114. OdometerValueMidnight

2.115. OdometerValueMidnightRecordArray

2.116. OverspeedNumber

2.117. PlaceRecord

2.118. PreviousVehicleInfo

2.119. PublicKey

2.120. RecordType

2.121. RegionAlpha

2.122. RegionNumeric

2.123. RemoteCommunicationModuleSerialNumber

2.124. RSAKeyModulus

2.125. RSAKeyPrivateExponent

2.126. RSAKeyPublicExponent

2.127. RtmData

2.128. SealDataCard

▼B

2.129. SealDataVu

2.130. SealRecord

2.131. SensorApprovalNumber

2.132. SensorExternalGNSSApprovalNumber

2.133. SensorExternalGNSSCoupledRecord

2.134. SensorExternalGNSSIdentification

2.135. SensorExternalGNSSInstallation

2.136. SensorExternalGNSSOSIdentifier

2.137. SensorExternalGNSSSCIdentifier

2.138. SensorGNSSCouplingDate

2.139. SensorGNSSSerialNumber

2.140. SensorIdentification

2.141. SensorInstallation

2.142. SensorInstallationSecData

2.143. SensorOSIdentifier

2.144. SensorPaired

2.145. SensorPairedRecord

2.146. SensorPairingDate

2.147. SensorSCIdentifier

2.148. SensorSerialNumber

2.149. Signature

2.150. SignatureRecordArray

2.151. SimilarEventsNumber

2.152. SpecificConditionRecord

2.153. SpecificConditions

2.154. SpecificConditionType

2.155. Hastighet

2.156. SpeedAuthorised

2.157. SpeedAverage

2.158. SpeedMax

2.159. TachographPayload

2.160. TachographPayloadEncrypted

▼B

2.161. TDesSessionKey

2.162. TimeReal

2.163. TyreSize

2.164. VehicleIdentificationNumber

2.165. VehicleIdentificationNumberRecordArray

2.166. VehicleRegistrationIdentification

2.167. VehicleRegistrationNumber

2.168. VehicleRegistrationNumberRecordArray

2.169. VuAbility

2.170. VuActivityDailyData

2.171. VuActivityDailyRecordArray

2.172. VuApprovalNumber

2.173. VuCalibrationData

2.174. VuCalibrationRecord

2.175. VuCalibrationRecordArray

2.176. VuCardIWData

2.177. VuCardIWRecord

2.178. VuCardIWRecordArray

2.179. VuCardRecord

2.180. VuCardRecordArray

2.181. VuCertificate

2.182. VuCertificateRecordArray

2.183. VuCompanyLocksData

2.184. VuCompanyLocksRecord

2.185. VuCompanyLocksRecordArray

2.186. VuControlActivityData

2.187. VuControlActivityRecord

2.188. VuControlActivityRecordArray

▼B

2.189. VuDataBlockCounter

2.190. VuDetailedSpeedBlock

2.191. VuDetailedSpeedBlockRecordArray

2.192. VuDetailedSpeedData

2.193. VuDownloadablePeriod

2.194. VuDownloadablePeriodRecordArray

2.195. VuDownloadActivityData

2.196. VuDownloadActivityDataRecordArray

2.197. VuEventData

2.198. VuEventRecord

2.199. VuEventRecordArray

2.200. VuFaultData

2.201. VuFaultRecord

2.202. VuFaultRecordArray

2.203. VuGNSSCDRecord

2.204. VuGNSSCDRecordArray

2.205. VuIdentification

2.206. VuIdentificationRecordArray

2.207. VuITSConsentRecord

2.208. VuITSConsentRecordArray

2.209. VuManufacturerAddress

2.210. VuManufacturerName

2.211. VuManufacturingDate

2.212. VuOverSpeedingControlData

2.213. VuOverSpeedingControlDataRecordArray

2.214. VuOverSpeedingEventData

▼B

2.215. VuOverSpeedingEventRecord

2.216. VuOverSpeedingEventRecordArray

2.217. VuPartNumber

2.218. VuPlaceDailyWorkPeriodData

2.219. VuPlaceDailyWorkPeriodRecord

2.220. VuPlaceDailyWorkPeriodRecordArray

2.221. VuPrivateKey

2.222. VuPublicKey

2.223. VuSerialNumber

2.224. VuSoftInstallationDate

2.225. VuSoftwareIdentification

2.226. VuSoftwareVersion

2.227. VuSpecificConditionData

2.228. VuSpecificConditionRecordArray

2.229. VuTimeAdjustmentData

2.230. VuTimeAdjustmentGNSSRecord

2.231. VuTimeAdjustmentGNSSRecordArray

2.232. VuTimeAdjustmentRecord

2.233. VuTimeAdjustmentRecordArray

2.234. WorkshopCardApplicationIdentification

2.235. WorkshopCardCalibrationData

2.236. WorkshopCardCalibrationRecord

2.237. WorkshopCardHolderIdentification

2.238. WorkshopCardPIN

2.239. W-VehicleCharacteristicConstant

2.240. VuPowerSupplyInterruptionRecord

▼B

2.241. VuPowerSupplyInterruptionRecordArray

2.242. VuSensorExternalGNSSCoupledRecordArray

2.243. VuSensorPairedRecordArray

3. DEFINITIONER AV INTERVALL FÖR VÄRDEN OCH STORLEKAR

4. TECKENMÄNGDER

5. KODNING

6. OBJEKTIDENTIFIERARE OCH TILLÄMPNINGSIDENTIFIERARE

6.1. Objektidentifierare

6.2. Tillämpningsidentifierare

1. INLEDNING

I detta tillägg specificeras de dataformat, dataelement och datastrukturer som används i färdskrivaren och på färdskrivarkorten.

1.1. **Metod för definition av datatyper**

I detta tillägg används ASN.1 (*Abstract Syntax Notation One*) för att definiera datatyper. Det gör det möjligt att definiera enkla och strukturerade data utan att ange någon specifik överföringssyntax (kodningsregler) som är beroende av tillämpning och miljö.

Namngivning enligt ASN.1 sker i enlighet med ISO/IEC 8824-1. Detta innebär följande:

— Innebörden av datatypen anges, där så är möjligt, genom de namn som väljs.

— Om en datatyp är en sammansättning av andra datatyper, utgörs datatypsnamnet fortfarande av en enda sekvens av alfabetiska tecken som börjar med en versal. Versaler används dock inne i namnet för att ge motsvarande betydelse.

— I allmänhet avser datatypsnamnen namnet på de datatyper från vilka de konstrueras, den utrustning i vilken data lagras och den funktion som hänförs till dessa data.

Om en ASN.1-typ redan har definierats som en del av en annan standard och om den kommer ifråga för användning i färdskrivaren definieras denna ASN.1-typ i detta tillägg.

För att möjliggöra flera typer av kodningsregler begränsas vissa ASN.1-typer i detta tillägg av identifierare för värdeintervall. Identifierare för värdeintervall definieras i avsnitt 3 och i tillägg 2.

1.2. **Referenser**

Följande referenser används i detta tillägg:

ISO 639	Code for the representation of names of languages. First Edition: 1988.

▼B

ISO 3166	Codes for the representation of names of countries and their subdivisions – Part 1: Country codes, 2013
ISO 3779	Road vehicles – Vehicle identification number (VIN) – Content and structure. 2009
ISO/IEC 7816-5	Identification cards – Integrated circuit cards – Part 5: Registration of application providers. Second edition: 2004.
ISO/IEC 7816-6	Identification cards – Integrated circuit cards – Part 6: Interindustry data elements for interchange, 2004 + Technical Corrigendum 1: 2006
ISO/IEC 8824-1	Information technology – Abstract Syntax Notation One (ASN.1): Specification of basic notation. 2008 + Technical Corrigendum 1: 2012 and Technical Corrigendum 2: 2014.
ISO/IEC 8825-2	Information technology – ASN.1 encoding rules: Specification of Packed Encoding Rules (PER). 2008.
ISO/IEC 8859-1	Information technology – 8 bit single-byte coded graphic character sets – Part 1: Latin alphabet No.1. First edition: 1998.
ISO/IEC 8859-7	Information technology – 8 bit single-byte coded graphic character sets – Part 7: Latin/Greek alphabet. 2003.
ISO 16844-3	Road vehicles – Tachograph systems – Motion Sensor Interface. 2004 + Technical Corrigendum 1: 2006..
TR-03110-3	BSI / ANSSI Technical Guideline TR-03110-3, Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS Token – Part 3 Common Specifications, version 2.20, 3. February 2015

2. DEFINITIONER AV DATATYPER

För samtliga nedanstående datatyper kommer standardvärdet för ett ”okänt” (*unknown*) eller ”ej tillämpligt” (*not applicable*) innehåll att skapas genom att dataelementet fylls med ′FF′-byte.

Alla datatyper används för tillämpningar i generation 1 och generation 2 om inget annat anges.

2.1. **ActivityChangeInfo**

Denna datatyp gör det möjligt att inom ett ord på två byte koda kortplatsstatus kl. 00.00 och/eller körningsstatus kl. 00.00 och/eller ändringar av aktivitet och/eller ändringar av körningsstatus och/eller ändringar av kortstatus för en förare eller medförare. Denna datatyp berörs av krav 105, 266, 291, 320, 321, 343 och 344 i bilaga 1C.

```
ActivityChangeInfo ::= OCTET STRING (SIZE(2))
```

Värdetilldelning – **oktettgrupperad**: ‘scpaatttttttttt’B (16 bitar)

För dataminnesregistreringar (eller kortplatsstatus):

‘s’B	Kortplats: ‘0’B: DRIVER (förare) ‘1’B: CO-DRIVER (medförare)

▼B

‘c’B	Körningsstatus:
	‘0’B: SINGLE (ensam förare)
	‘1’B: CREW (besättning)
‘p’B	Status för förarkort (eller verkstadskort) i relevant kortplats:
	‘0’B: INSERTED (det finns ett kort insatt)
	‘1’B: NOT INSERTED (det finns inget kort insatt)
‘aa’B	Aktivitet:
	‘00’B: BREAK/REST (rast/vila),
	‘01’B: AVAILABILITY (tillgänglighet),
	‘10’B: WORK (annat arbete),
	‘11’B: DRIVING (körning)
‘ttttttttttt’B	Tidpunkt för ändring: Antal minuter sedan kl. 00.00 dagen ifråga.

För kortregistreringar (förar- eller verkstadskort) (och körningsstatus):

‘s’B	Kortplats (ej relevant när ‘p’ = 1 förutom anmärkning nedan):
	‘0’B: DRIVER (förare)
	‘1’B: CO-DRIVER (medförare)
‘c’B	Körningsstatus (fallet ‘p’ = 0) eller
	följande aktivitetsstatus (fallet ‘p’ = 1):
	‘0’B: SINGLE (ensam förare),
	‘0’B: UNKNOWN (okänd)
	‘1’B: CREW (besättning),
	‘1’B: KNOWN (känd = manuellt angiven)
‘p’B	Kortstatus:
	‘0’B: INSERTED (kortet är insatt i en färdskrivare)
	‘1’B: NOT INSERTED (kortet är uttaget, dvs. inte insatt i en färdskrivare).
‘aa’B	Aktivitet (ej relevant när ‘p’ = 1 och ‘c’ = 0 förutom anmärkning nedan):
	‘00’B: BREAK/REST (rast/vila),
	‘01’B: AVAILABILITY (tillgänglighet),
	‘10’B: WORK (annat arbete),
	‘11’B: DRIVING (körning)
‘ttttttttttt’B	Tidpunkt för ändring: Antal minuter sedan kl. 00.00 dagen ifråga.

▼B

Observera när det gäller ”uttag av kort”:

För ett kort som tas ut gäller följande:

— ‘s’ är relevant och anger den kortplats från vilken kortet tas ut.

— ‘c’ måste sättas till 0.

— ‘p’ måste sättas till 1.

— ‘aa’ måste koda den innevarande aktivitet som var vald vid den tidpunkten.

Till följd av en manuell angivelse får bitarna ‘c’ och ‘aa’ i ordet (som lagras i ett kort) skrivas över senare för att återspegla angivelsen.

2.2. **Address**

En adress.

```
Address ::= SEQUENCE {
   codePage                          INTEGER (0..255),
   address                           OCTET STRING (SIZE(35))
}
```

codePage specificerar en teckenmängd som definieras i kapitel 4.

address är en adress som kodats enligt den specificerade teckenmängden.

2.3. **AESKey**

Generation 2:

En AES-nyckel med en längd av 128, 192 eller 256 bitar.

```
AESKey ::= CHOICE {
   aes128Key                         AES128Key,
   aes192Key                         AES192Key,
   aes256Key                         AES256Key
}
```

Värdetilldelning: Ej närmare angiven.

2.4. **AES128Key**

Generation 2:

En AES128-nyckel.

```
AES128Key ::= SEQUENCE {
   length                            INTEGER(0..255),
   aes128Key                         OCTET STRING (SIZE(16))
}
```

length anger längden för AES128-nyckeln i oktetter.

aes128Key är en AES-nyckel med en längd av 128 bitar.

Värdetilldelning:

Längden ska ha värdet 16.

▼B

2.5. **AES192Key**

Generation 2:

En AES192-nyckel.

```
AES192Key ::= SEQUENCE {
   length                              INTEGER(0..255),
   aes192Key                           OCTET STRING (SIZE(24))
}
```

length anger längden för AES192-nyckeln i oktetter.

aes192Key är en AES-nyckel med en längd av 192 bitar.

Värdetilldelning:

Längden ska ha värdet 24.

2.6. **AES256Key**

Generation 2:

En AES256-nyckel.

```
AES256Key ::= SEQUENCE {
   length                              INTEGER(0..255),
   aes256Key                           OCTET STRING (SIZE(32))
}
```

length anger längden för AES256-nyckeln i oktetter.

aes256Key är en AES-nyckel med en längd av 256 bitar.

Värdetilldelning:

Längden ska ha värdet 32.

2.7. **BCDString**

BCDString tillämpas för binärkodad decimal notation (BCD, *Binary Code Decimal*). Denna datatyp används för att återge en decimalsiffra i en semi-oktett (4 bitar). BCDString bygger på ISO/IEC 8824-1 ′CharacterStringType′.

```
BCDString ::= CHARACTER STRING (WITH COMPONENTS {
   identification ( WITH COMPONENTS {
   fixed PRESENT }) })
```

BCDString använder en ”hstring”-notation. Den hexadecimala siffran längst till vänster ska vara den mest signifikanta semi-oktetten i den första oktetten. För att producera en multipel av oktetter ska semi-oktetter bestående av nollor efter behov införas från semi-oktettpositionen längst till vänster i den första oktetten.

Följande siffror är tillåtna: 0, 1, .. 9.

2.8. **CalibrationPurpose**

Kod som förklarar varför en mängd av kalibreringsparametrar registrerades. Denna datatyp berörs av krav 097 och 098 i bilaga 1B och krav 119 i bilaga 1C.

```
CalibrationPurpose ::= OCTET STRING (SIZE(1))
```

▼B

Värdetilldelning:

Generation 1:

‘00’H	reserverat värde,
‘01’H	aktivering: registrering av kända kalibreringsparametrar, vid tidpunkten för aktivering av fordonsenheten,
‘02’H	första installation: första kalibrering av fordonsenheten efter aktivering,
‘03’H	installation: första kalibrering av fordonsenheten i nuvarande fordon,
‘04’H	periodisk besiktning.

Generation 2:

Jämfört med generation 1 används följande ytterligare värden:

‘05’H	angivelse av fordonets registreringsnummer (VRN) från företag,
‘06’H	tidsinställning utan kalibrering,
‘07’H–‘7F’H	RFU.
‘80’H–‘FF’H	Tillverkarspecifik.

2.9. **CardActivityDailyRecord**

Information lagrad i ett kort om föraraktiviteter under en viss kalenderdag. Denna datatyp berörs av krav 266, 291, 320 och 343 i bilaga 1C.

```
CardActivityDailyRecord ::= SEQUENCE {
   activityPreviousRecordLength         INTEGER(0..CardActivityLengthRange),
   activityRecordLength                 INTEGER(0..CardActivityLengthRange),
   activityRecordDate                   TimeReal,
   activityDailyPresenceCounter         DailyPresenceCounter,
   activityDayDistance                  Distance,
   activityChangeInfo                   SET SIZE(1..1440) OF ActivityChangeInfo
}
```

activityPreviousRecordLength är den totala längden i byte av den föregående dagsposten. Det största värdet ges av längden på den oktettsträng som innehåller dessa poster (se CardActivityLengthRange, tillägg 2 avsnitt 4). När denna post är den äldsta dagsposten måste värdet av activityPreviousRecordLength sättas till 0.

activityRecordLength är denna posts totala längd i byte. Det största värdet ges av längden på den oktettsträng som innehåller dessa poster.

activityRecordDate är datum för posten.

▼B

activityDailyPresenceCounter är närvaroräknaren för kortet denna dag.

activityDayDistance är den sammanlagda sträcka som tillryggalagts denna dag.

activityChangeInfo är mängden ActivityChangeInfo-data för föraren denna dag. Den får innehålla högst 1440 värden (en aktivitetsändring per minut). Denna mängd omfattar alltid den activityChangeInfo där körningsstatus kodas kl. 00.00.

2.10. **CardActivityLengthRange**

Antal byte på ett förarkort eller ett verkstadskort som finns tillgängliga för lagring av föraraktivitetsposter.

```
CardActivityLengthRange ::= INTEGER(0..2^16-1)
```

Värdetilldelning: Se tillägg 2.

2.11. **CardApprovalNumber**

Kortets typgodkännandenummer.

```
CardApprovalNumber ::= IA5String(SIZE(8))
```

Värdetilldelning:

Godkännandenumret ska återges så som det är offentliggjort på Europeiska kommissionens motsvarande webbplats, t.ex. inklusive eventuella bindestreck. Godkännandenumret ska vara vänsterjusterat.

2.12. **CardCertificate**

Generation 1:

Certifikat för kortets öppna nyckel.

```
CardCertificate ::= Certificate
```

2.13. **CardChipIdentification**

Information lagrad i ett kort om identifiering av kortets integrerade krets (IC) (krav 249 i bilaga 1C). icSerialNumber tillsammans med icManufacturingReferences utgör en unik identitet för kortets chip. Enbart icSerialNumber utgör inte någon unik identitet för kortets chip.

```
CardChipIdentification ::= SEQUENCE {
   icSerialNumber                    OCTET STRING (SIZE(4)),
   icManufacturingReferences         OCTET STRING (SIZE(4))
}
```

icSerialNumber är den integrerade kretsens serienummer.

icManufacturingReferences är den specifika identifieraren för tillverkaren av den integrerade kretsen.

2.14. **CardConsecutiveIndex**

Ett löpnummer för kortet (definition h)).

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

Värdetilldelning: (se kapitel 7 i bilaga 1C)

Ökningsföljd: ‘0, …, 9, A, …, Z, a, …, z’

▼B

2.15. **CardControlActivityDataRecord**

Information lagrad i ett förarkort eller verkstadskort om den senaste kontrollen av föraren (krav 274, 299, 327 och 350 i bilaga 1C).

```
CardControlActivityDataRecord ::= SEQUENCE {
   controlType                          ControlType,
   controlTime                          TimeReal,
   controlCardNumber                    FullCardNumber,
   controlVehicleRegistration           VehicleRegistrationIdentification,
   controlDownloadPeriodBegin           TimeReal,
   controlDownloadPeriodEnd             TimeReal
}
```

controlType är typ av kontroll.

controlTime är datum och tidpunkt för kontrollen.

controlCardNumber är FullCardNumber för den kontrolltjänsteman som har utfört kontrollen.

controlVehicleRegistration är fordonets registreringsnummer (VRN) och registrerande medlemsstat för det fordon i vilket kontrollen ägde rum.

controlDownloadPeriodBegin och **controlDownloadPeriodEnd** är överförd period, om överföring utfördes.

2.16. **CardCurrentUse**

Information om kortets innevarande användning (krav 273, 298, 326 och 349 i bilaga 1C).

```
CardCurrentUse ::= SEQUENCE {
   sessionOpenTime                      TimeReal,
   sessionOpenVehicle                   VehicleRegistrationIdentification
}
```

sessionOpenTime är den tid då kortet sätts in för innevarande användning. Detta element sätts till noll då kortet tas ut.

sessionOpenVehicle är identifiering av det fordon som används för tillfället, och sätts vid insättning av kortet. Detta element sätts till noll då kortet tas ut.

2.17. **CardDriverActivity**

Information lagrad i ett förarkort eller verkstadskort om förarens aktiviteter (krav 267, 268, 292, 293, 321 och 344 i bilaga 1C).

```
CardDriverActivity ::= SEQUENCE {
   activityPointerOldestDayRecord       INTEGER(0.. CardActivityLengthRange-1),
   activityPointerNewestRecord          INTEGER(0.. CardActivityLengthRange-1),
   activityDailyRecords                 OCTET STRING
                                        (SIZE(CardActivityLengthRange))
}
```

activityPointerOldestDayRecord är specificering av början av lagringsplats (antal byte från början av strängen) av äldsta fullständiga dagspost i strängen activityDailyRecords. Det största värdet ges av strängens längd.

▼B

activityPointerNewestRecord är specificering av början av lagringsplats (antal byte från strängens början) av senaste dagspost i strängen activityDailyRecords. Det största värdet ges av strängens längd.

activityDailyRecords är det utrymme som finns tillgängligt för att lagra data om förarens aktiviteter (datastruktur: CardActivityDailyRecord) för varje kalenderdag då kortet använts.

Värdetilldelning: Denna oktettsträng fylls cykliskt med poster med CardActivityDailyRecord. Vid den första användningen påbörjas lagring vid första byte i strängen. Alla nya poster fogas till slutet av den föregående posten. När strängen är full fortsätter lagringen vid första byte i strängen, oberoende av om en brytning finns inuti dataelementet. Innan nya aktivitetsdata placeras i strängen (eller innevarande activityDailyRecord förstoras, eller en ny activityDailyRecord placeras) som ersätter äldre aktivitetsdata, måste activityPointerOldestDayRecord uppdateras till att återspegla den nya placeringen av den äldsta kompletta dagsposten, och activityPreviousRecordLength för denna (nya) äldsta fullständiga dagspost måste återställas till 0.

2.18. **CardDrivingLicenceInformation**

Information lagrad i förarkortet om kortinnehavarens körkortsdata (krav 259 och 284 i bilaga 1C).

```
CardDrivingLicenceInformation ::= SEQUENCE {
   drivingLicenceIssuingAuthority       Name,
   drivingLicenceIssuingNation          NationNumeric,
   drivingLicenceNumber                 IA5String(SIZE(16))
}
```

drivingLicenceIssuingAuthority är den myndighet som ansvarar för utfärdandet av körkortet.

drivingLicenceIssuingNation är nationaliteten för den myndighet som utfärdade körkortet.

drivingLicenceNumber är körkortsnumret.

2.19. **CardEventData**

Information lagrad i ett förarkort eller verkstadskort om händelser som förknippas med kortinnehavaren (krav 260, 285, 318 och 341 i bilaga 1C).

```
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 händelserna av typen försök till säkerhetsöverträdelse).

▼B

2.20. **CardEventRecord**

Information lagrad i ett förarkort eller verkstadskort om en händelse som förknippas med kortinnehavaren (krav 261, 286, 318 och 341).

```
CardEventRecord ::= SEQUENCE {
   eventType                          EventFaultType,
   eventBeginTime                     TimeReal,
   eventEndTime                       TimeReal,
   eventVehicleRegistration           VehicleRegistrationIdentification
}
```

eventType är typ av händelse.

eventBeginTime är datum och tidpunkt för händelsens början.

eventEndTime är datum och tidpunkt för händelsens slut.

eventVehicleRegistration är fordonets registreringsnummer (VRN) och registrerande medlemsstat för det fordon i vilket händelsen ägde rum.

2.21. **CardFaultData**

Information lagrad i ett förarkort eller verkstadskort om de fel som förknippas med kortinnehavaren (krav 263, 288, 318 och 341).

```
CardFaultData ::= SEQUENCE SIZE(2) OF {
   cardFaultRecords                   SET SIZE(NoOfFaultsPerType) OF
                                      CardFaultRecord
}
```

CardFaultData är en sekvens av postmängder för färdskrivarfel följda av postmängder för kortfel.

cardFaultRecords är en mängd av poster om fel av en viss felkategori (färdskrivare eller kort).

2.22. **CardFaultRecord**

Information lagrad i ett förarkort eller verkstadskort om ett fel som förknippas med kortinnehavaren (krav 264, 289, 318 och 341 i bilaga 1C).

```
CardFaultRecord ::= SEQUENCE {
   faultType                          EventFaultType,
   faultBeginTime                     TimeReal,
   faultEndTime                       TimeReal,
   faultVehicleRegistration           VehicleRegistrationIdentification
}
```

faultType är typ av fel.

faultBeginTime är datum och tidpunkt för felets början.

faultEndTime är datum och tidpunkt för felets slut.

faultVehicleRegistration är registreringsnummer (VRN) och registrerande medlemsstat för det fordon där felet ägde rum.

▼B

2.23. **CardIccIdentification**

Information lagrad i ett kort om identifiering av kortets integrerade krets (krav 248 i bilaga 1C).

```
CardIccIdentification ::= SEQUENCE {
   clockStop                          OCTET STRING (SIZE(1)),
   cardExtendedSerialNumber           ExtendedSerialNumber,
   cardApprovalNumber                 CardApprovalNumber,
   cardPersonaliserID                 ManufacturerCode,
   embedderIcAssemblerId              EmbedderIcAssemblerId,
   icIdentifier                       OCTET STRING (SIZE(2))
}
```

clockStop är det klockstoppläge (*Clockstop mode*) som definieras i tillägg 2.

cardExtendedSerialNumber är smartkortets unika serienummer som specificeras vidare i datatypen ExtendedSerialNumber.

cardApprovalNumber är kortets typgodkännandenummer.

cardPersonaliserID är identitet för kortanpassare, kodad som ManufacturerCode.

embedderIcAssemblerId ger information om inbäddare/sammansättare av den integrerade kretsen.

icIdentifier är identifieraren för kortets integrerade krets och dess tillverkare enligt definition i ISO/IEC 7816-6.

2.24. **CardIdentification**

Information lagrad i ett kort om identifiering av kortet (krav 255, 280, 310, 333, 359, 365, 371 och 377 i bilaga 1C).

```
CardIdentification ::= SEQUENCE {
   cardIssuingMemberState             NationNumeric,
   cardNumber                         CardNumber,
   cardIssuingAuthorityName           Name,
   cardIssueDate                      TimeReal,
   cardValidityBegin                  TimeReal,
   cardExpiryDate                     TimeReal
}
```

cardIssuingMemberState är koden för den medlemsstat som utfärdar kortet.

cardNumber är kortets kortnummer.

cardIssuingAuthorityName är namnet på den myndighet som har utfärdat kortet.

cardIssueDate är det datum då kortet utfärdades till den nuvarande innehavaren.

cardValidityBegin är kortets första giltighetsdag.

cardExpiryDate är kortets sista giltighetsdag.

▼B

2.25. **CardMACertificate**

Generation 2:

Certifikat för kortets öppna nyckel vid ömsesidig autentisering med en fordonsenhet. Strukturen för detta certifikat anges i tillägg 11.

```
CardMACertificate ::= Certificate
```

2.26. **CardNumber**

Kortnummer – se definition g).

```
CardNumber ::= CHOICE {
   SEQUENCE {
      driverIdentification              IA5String(SIZE(14)),
      cardReplacementIndex              CardReplacementIndex,
      cardRenewalIndex                  CardRenewalIndex
   },
   SEQUENCE {
      ownerIdentification               IA5String(SIZE(13)),
      cardConsecutiveIndex              CardConsecutiveIndex,
      cardReplacementIndex              CardReplacementIndex,
      cardRenewalIndex                  CardRenewalIndex
   }
}
```

driverIdentification är en unik identifiering av en förare i en medlemsstat.

ownerIdentification är en unik identifiering av ett företag eller en verkstad eller ett kontrollorgan i en medlemsstat.

cardConsecutiveIndex är kortets löpnummer.

cardReplacementIndex är kortets ersättningsindex.

cardRenewalIndex är kortets förnyelseindex.

Sekvensen i det första alternativet (CHOICE) är lämplig för kodning av ett förarkortsnummer, sekvensen i det andra alternativet är lämplig för kodning av nummer på verkstadskort, kontrollkort och företagskort.

2.27. **CardPlaceDailyWorkPeriod**

Information lagrad i ett förarkort eller verkstadskort om de platser där dagens arbetsperioder påbörjas och/eller avslutas (krav 272, 297, 325 och 348 i bilaga 1C).

```
CardPlaceDailyWorkPeriod ::= SEQUENCE {
   placePointerNewestRecord    INTEGER(0 .. NoOfCardPlaceRecords-1),
   placeRecords                SET SIZE(NoOfCardPlaceRecords) OF PlaceRecord
}
```

placePointerNewestRecord är index för senast uppdaterade platspost.

Värdetilldelning: Ett tal som motsvarar platspostens numerator, och som börjar med ′0′ för den första gången platsposterna uppträder i strukturen.

placeRecords är den mängd poster som innehåller information om de platser som angivits.

▼B

2.28. **CardPrivateKey**

Generation 1:

Ett korts privata nyckel.

```
CardPrivateKey ::= RSAKeyPrivateExponent
```

2.29. **CardPublicKey**

Ett korts öppna nyckel.

```
CardPublicKey ::= PublicKey
```

2.30. **CardRenewalIndex**

Ett korts förnyelseindex (definition i)).

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

Värdetilldelning: (se kapitel VII i denna bilaga)

‘0’ Första utfärdande.

Ökningsföljd: ‘0, …, 9, A, …, Z’

2.31. **CardReplacementIndex**

Ett korts ersättningsindex (definition j)).

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

Värdetilldelning: (se kapitel VII i denna bilaga)

‘0’ Ursprungligt kort.

Ökningsföljd: ‘0, …, 9, A, …, Z’

2.32. **CardSignCertificate**

Generation 2:

Certifikat för kortets öppna nyckel för signering. Strukturen för detta certifikat anges i tillägg 11.

```
CardSignCertificate ::= Certificate
```

2.33. **CardSlotNumber**

Kod för att särskilja de två kortplatserna i en fordonsenhet.

```
CardSlotNumber ::= INTEGER {
   driverSlot                          (0),
   co-driverSlot                       (1)
}
```

Värdetilldelning: Ej närmare angiven.

2.34. **CardSlotsStatus**

Kod som anger den typ av kort som är insatta i de två kortplatserna i fordonsenheten.

```
CardSlotsStatus ::= OCTET STRING (SIZE(1))
```

▼B

Värdetilldelning – oktettgrupperad: ‘ccccdddd’B

‘cccc’B Identifiering av typ av kort som är insatt i medförarens kortplats.

‘dddd’B Identifiering av typ av kort som är insatt i förarens kortplats.

Följande identifieringskoder används:

‘0000’B Inget kort är insatt.

‘0001’B Ett förarkort är insatt.

‘0010’B Ett verkstadskort är insatt.

‘0011’B Ett kontrollkort är insatt.

‘0100’B Ett företagskort är insatt.

2.35. **CardSlotsStatusRecordArray**

Generation 2:

CardSlotsStatus samt metadata som används i överföringsprotokollet.

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

recordType anger typen av post (CardSlotsStatus). **Värdetilldelning:** Se RecordType.

recordSize är storleken av CardSlotsStatus i byte.

noOfRecords är antalet poster i postmängden.

records är mängden av CardSlotsStatus-poster.

2.36. **CardStructureVersion**

En kod som anger versionen för den struktur som används i ett färdskrivarkort.

```
CardStructureVersion ::= OCTET STRING (SIZE(2))
```

Värdetilldelning: ‘aabb’H:

‘aa’H Index för strukturändringar.

‘00’H för tillämpningar i generation 1.

‘01’H för tillämpningar i generation 2.

‘bb’H Index för ändringar när det gäller användning av dataelement som definierats för strukturen till följd av den höga byten.

‘00’H för denna version av tillämpning i generation 1.

‘00’H för denna version av tillämpning i generation 2.

▼B

2.37. **CardVehicleRecord**

Information lagrad i ett förar- eller verkstadskort om en användningsperiod för ett fordon under en kalenderdag (krav 269, 294, 322 och 345 i bilaga 1C).

Generation 1:

```
CardVehicleRecord ::= SEQUENCE {
   vehicleOdometerBegin                    OdometerShort,
   vehicleOdometerEnd                      OdometerShort,
   vehicleFirstUse                         TimeReal,
   vehicleLastUse                          TimeReal,
   vehicleRegistration                     VehicleRegistrationIdentification,
   vuDataBlockCounter                      VuDataBlockCounter
}
```

vehicleOdometerBegin är fordonets vägmätarställning vid början av fordonets användningsperiod.

vehicleOdometerEnd är fordonets vägmätarställning vid slutet av fordonets användningsperiod.

vehicleFirstUse är datum och tidpunkt för påbörjande av fordonets användningsperiod.

vehicleLastUse är datum och tidpunkt för avslutande av fordonets användningsperiod.

vehicleRegistration är fordonets registreringsnummer och den medlemsstat där fordonet är registrerat.

vuDataBlockCounter är värdet för VuDataBlockCounter vid senaste hämtning (*extraction*) av fordonets användningsperiod.

Generation 2:

```
CardVehicleRecord ::= SEQUENCE {
   vehicleOdometerBegin                    OdometerShort,
   vehicleOdometerEnd                      OdometerShort,
   vehicleFirstUse                         TimeReal,
   vehicleLastUse                          TimeReal,
   vehicleRegistration                     VehicleRegistrationIdentification,
   vuDataBlockCounter                      VuDataBlockCounter,
   vehicleIdentificationNumber             VehicleIdentificationNumber
}
```

Jämfört med generation 1 används följande ytterligare dataelement:

VehicleIdentificationNumber är fordonets identifieringsnummer som syftar på fordonet som helhet.

2.38. **CardVehiclesUsed**

Information lagrad i ett förarkort eller verkstadskort om de fordon som kortinnehavaren använder (krav 270, 295, 323 och 346 i bilaga 1C).

```
CardVehiclesUsed := SEQUENCE {
   vehiclePointerNewestRecord          INTEGER(0..NoOfCardVehicleRecords-1),
   cardVehicleRecords                  SET SIZE(NoOfCardVehicleRecords) OF
                                       CardVehicleRecord
}
```

vehiclePointerNewestRecord är index för senast uppdaterad fordonspost.

▼B

Värdetilldelning: Ett tal som motsvarar fordonspostens numerator, och som börjar med ‘0’ för den första gången fordonsposterna uppträder i strukturen.

cardVehicleRecords är den mängd poster som innehåller information om använda fordon.

2.39. **CardVehicleUnitRecord**

Generation 2:

Information lagrad i ett förarkort eller verkstadskort om den fordonsenhet som användes (krav 303 och 351).

```
CardVehicleUnitRecord ::= SEQUENCE {
   timeStamp                              TimeReal,
   manufacturerCode                       ManufacturerCode,
   deviceID                               INTEGER(0..255),
   vuSoftwareVersion                      VuSoftwareVersion
}
```

timeStamp är början av fordonsenhetens användningsperiod (dvs. första insättning av kort i fordonsenheten under denna period).

manufacturerCode anger fordonsenhetens tillverkare.

deviceID anger typ av fordonsenhet hos en tillverkare. Värdet är tillverkarspecifikt.

vuSoftwareVersion är numret på programvaruversionen i fordonsenheten.

2.40. **CardVehicleUnitsUsed**

Generation 2:

Information lagrad i ett förarkort eller verkstadskort om de fordonsenheter som kortinnehavaren använder (krav 306 och 352).

```
CardVehicleUnitsUsed := SEQUENCE {
   vehicleUnitPointerNewestRecord       INTEGER(0..NoOfCardVehicleUnitRecords-1),
   cardVehicleUnitRecords               SET SIZE(NoOfCardVehicleUnitRecords) OF
                                        CardVehicleUnitRecord
}
```

vehicleUnitPointerNewestRecord är index för senast uppdaterad post for fordonsenhet.

Värdetilldelning: Ett tal som motsvarar fordonspostens numerator, och som börjar med ′0′ för den första gången posterna för fordonsenhet uppträder i strukturen.

cardVehicleUnitRecords är den mängd poster som innehåller information om använda fordonsenheter.

2.41. **Certificate**

Ett certifikat för en öppen nyckel som utfärdas av en certifieringsinstans.

Generation 1:

```
Certificate ::= OCTET STRING (SIZE(194))
```

▼B

Value assignment: Digital signatur med partiell återskapning av CertificateContent (certifikatinnehåll) i enlighet med tillägg 11 om gemensamma säkerhetsmekanismer: signatur (128 byte) || återstod av öppen nyckel (58 byte) || certifieringsinstansens referens (8 byte).

Generation 2:

```
Certificate ::= OCTET STRING (SIZE(204..341))
```

Värdetilldelning: Se tillägg 11.

2.42. **CertificateContent**

Generation 1:

Innehållet (i klartext) i certifikatet för en öppen nyckel i enlighet med tillägg 11 om gemensamma säkerhetsmekanismer.

```
CertificateContent ::= SEQUENCE {
   certificateProfileIdentifier         INTEGER(0..255),
   certificationAuthorityReference      KeyIdentifier,
   certificateHolderAuthorisation       CertificateHolderAuthorisation,
   certificateEndOfValidity             TimeReal,
   certificateHolderReference           KeyIdentifier,
   publicKey                            PublicKey
}
```

certificateProfileIdentifier är versionen av motsvarande certifikat.

Värdetilldelning: ‘01h’ för denna version.

CertificationAuthorityReference identifierar den certifieringsinstans som utfärdar certifikatet. Den refererar dessutom till denna certifieringsinstans öppna nyckel.

certificateHolderAuthorisation identifierar certifikatinnehavarens rättigheter.

certificateEndOfValidity är det datum då certifikatet upphör att gälla administrativt sett.

certificateHolderReference identifierar certifikatinnehavaren. Den refererar dessutom till innehavarens öppna nyckel.

publicKey är den öppna nyckel som certifieras genom detta certifikat.

2.43. **CertificateHolderAuthorisation**

Identifiering av en certifikatinnehavares rättigheter.

```
CertificateHolderAuthorisation ::= SEQUENCE {
   tachographApplicationID              OCTET STRING(SIZE(6))
   equipmentType                        EquipmentType
}
```

Generation 1:

tachographApplicationID är tillämpningsidentifieraren för färdskrivartillämpningen.

Värdetilldelning: ‘FFh’ ‘54h’ ‘41h’ ‘43h’ ‘48h’ ‘4Fh’. Denna tillämpningsidentifierare är en proprietär (*proprietary*) icke-registrerad tillämpningsidentifierare i enlighet med ISO/IEC 7816-5.

equipmentType är identifieringen av den typ av utrustning för vilken certifikatet är avsett.

Värdetilldelning: i enlighet med datatyp EquipmentType. **0** om certifikatet tillhör en medlemsstat.

▼B

Generation 2:

tachographApplicationID anger de 6 mest signifikanta byte i tillämpningsidentifieraren (AID) för färdskrivarkortets tillämpning i generation 2. AID för färdskrivarkortets tillämpning anges i kapitel 6.2.

Värdetilldelning: ‘FF 53 4D 52 44 54’.

equipmentType är identifieringen av den typ av utrustning, såsom anges för generation 2, för vilken certifikatet är avsett.

Värdetilldelning: i enlighet med datatyp EquipmentType.

2.44. **CertificateRequestID**

Unik identifiering av en begäran om certifikat. Den kan också användas som en identifierare för öppen nyckel för fordonsenhet om serienumret på den fordonsenhet som nyckeln är avsedd för inte är känt när certifikatet genereras.

```
CertificateRequestID ::= SEQUENCE{
   requestSerialNumber                 INTEGER(0..2^32-1),
   requestMonthYear                    BCDString(SIZE(2)),
   crIdentifier                        OCTET STRING(SIZE(1)),
   manufacturerCode                    ManufacturerCode
}
```

requestSerialNumber är ett serienummer för begäran om certifikat, som är unikt för tillverkaren och månaden nedan.

requestMonthYear är identifiering av den månad och det år då certifikatet begärdes.

Värdetilldelning: BCD-kodning av månad (två siffror) och år (två sista siffrorna).

crIdentifier är en identifierare för att skilja en begäran om certifikat från ett utökat serienummer.

Värdetilldelning: ‘FFh’.

manufacturerCode är den numeriska koden för den tillverkare som begär certifikatet.

2.45. **CertificationAuthorityKID**

Identifierare för öppen nyckel för certifieringsinstans (en medlemsstats eller den europeiska certifieringsinstansen).

```
CertificationAuthorityKID ::= SEQUENCE{
   nationNumeric                       NationNumeric,
   nationAlpha                         NationAlpha,
   keySerialNumber                     INTEGER(0..255),
   additionalInfo                      OCTET STRING(SIZE(2)),
   caIdentifier                        OCTET STRING(SIZE(1))
}
```

nationNumeric är certifieringsinstansens numeriska landskod.

nationAlpha är certifieringsinstansens alfanumeriska landskod.

▼B

keySerialNumber är ett serienummer för att skilja certifieringsinstansens olika nycklar åt om man byter nycklar.

additionalInfo är ett fält på två byte för ytterligare kodning (specifik för certifieringsinstansen).

caIdentifier är en identifierare för att särskilja mellan certifieringsinstansens olika nycklar.

Värdetilldelning: ‘01h’.

2.46. **CompanyActivityData**

Information lagrad i ett företagskort om aktiviteter som utförts med kortet (krav 373 och 379 i bilaga 1C).

```
CompanyActivityData ::= SEQUENCE {
   companyPointerNewestRecord        INTEGER(0..NoOfCompanyActivityRecords-1),
   companyActivityRecords            SET SIZE(NoOfCompanyActivityRecords) OF
    companyActivityRecord             SEQUENCE {
     companyActivityType               CompanyActivityType,
     companyActivityTime               TimeReal,
     cardNumberInformation             FullCardNumber,
     vehicleRegistrationInformation    VehicleRegistrationIdentification,
     downloadPeriodBegin               TimeReal,
     downloadPeriodEnd                 TimeReal
    }
}
```

companyPointerNewestRecord är index för senast uppdaterade companyActivityRecord.

Värdetilldelning: Ett tal som motsvarar numeratorn för posten för företagsaktiviteter, och som börjar med ″0″ för den första gången posten för företagsaktiviteter uppträder i strukturen.

companyActivityRecords är mängden av alla poster för företagsaktiviteter.

companyActivityRecord är sekvensen av information om en företagsaktivitet.

companyActivityType är typen av företagsaktivitet.

companyActivityTime är datum och tidpunkt för företagsaktiviteten.

cardNumberInformation är kortnummer och utfärdande medlemsstat för det kort som överförts, i förekommande fall.

vehicleRegistrationInformation är registreringsnummer (VRN) och registrerande medlemsstat för det fordon som överförts eller som låsts eller öppnats.

downloadPeriodBegin och **downloadPeriodEnd** är den period som överförs från fordonsenheten, i förekommande fall.

2.47. **CompanyActivityType**

Kod för en aktivitet som utförs av ett företag som använder sitt företagskort.

```
CompanyActivityType ::= INTEGER {
   card downloading                  (1),
   VU downloading                    (2),
   VU lock-in                        (3),
   VU lock-out                       (4)
}
```

▼B

2.48. **CompanyCardApplicationIdentification**

Information lagrad i ett företagskort om identifiering av korttillämpningen (krav 369 och 375 i bilaga 1C).

```
CompanyCardApplicationIdentification ::= SEQUENCE {
   typeOfTachographCardId              EquipmentType,
   cardStructureVersion                CardStructureVersion,
   noOfCompanyActivityRecords          NoOfCompanyActivityRecords
}
```

typeOfTachographCardId specificerar använd korttyp.

cardStructureVersion specificerar versionen av den struktur som används i kortet.

noOfCompanyActivityRecords är det antal poster för företagsaktiviteter som kortet kan lagra.

2.49. **CompanyCardHolderIdentification**

Information lagrad i ett företagskort om identifiering av kortinnehavare (krav 372 och 378 i bilaga 1C).

```
CompanyCardHolderIdentification ::= SEQUENCE {
   companyName                         Name,
   companyAddress                      Address,
   cardHolderPreferredLanguage         Language
}
```

companyName är namn på innehavande företag.

companyAddress är adress till innehavande företag.

cardHolderPreferredLanguage är det språk som kortinnehavaren väljer.

2.50. **ControlCardApplicationIdentification**

Information lagrad i ett kontrollkort om identifiering av korttillämpningen (krav 357 och 363 i bilaga 1C).

```
ControlCardApplicationIdentification ::= SEQUENCE {
   typeOfTachographCardId              EquipmentType,
   cardStructureVersion                CardStructureVersion,
   noOfControlActivityRecords          NoOfControlActivityRecords
}
```

typeOfTachographCardId specificerar använd korttyp.

cardStructureVersion specificerar versionen av den struktur som används i kortet.

noOfControlActivityRecords är det antal poster för kontrollaktiviteter som kortet kan lagra.

▼B

2.51. **ControlCardControlActivityData**

Information lagrad i ett kontrollkort om kontrollaktiviteter som utförts med kortet (krav 361 och 367 i bilaga 1C).

```
ControlCardControlActivityData ::= SEQUENCE {
   controlPointerNewestRecord        INTEGER(0.. NoOfControlActivityRecords-1),
   controlActivityRecords            SET SIZE(NoOfControlActivityRecords) OF
    controlActivityRecord             SEQUENCE {
      controlType                       ControlType,
      controlTime                       TimeReal,
      controlledCardNumber              FullCardNumber,
      controlledVehicleRegistration     VehicleRegistrationIdentification,
      controlDownloadPeriodBegin        TimeReal,
      controlDownloadPeriodEnd          TimeReal
    }
}
```

controlPointerNewestRecord är index för senast uppdaterad post för kontrollaktiviteter.

Värdetilldelning: Ett tal som motsvarar numeratorn för posten för kontrollaktiviteter, och som börjar med ‘0’ för den första gång då posten för kontrollaktiviteter uppträder i strukturen.

controlActivityRecords är mängden av alla poster för kontrollaktiviteter.

controlActivityRecord är sekvensen av information om en kontroll.

controlType är typ av kontroll.

controlTime är datum och tidpunkt för kontrollen.

controlledCardNumber är kortnummer och utfärdande medlemsstat för det kort som kontrollerats.

controlledVehicleRegistration är registreringsnummer (VRN) och registrerande medlemsstat för det fordon i vilket kontrollen ägde rum.

controlDownloadPeriodBegin och **controlDownloadPeriodEnd** är den period som eventuellt överförs.

2.52. **ControlCardHolderIdentification**

Information lagrad i ett kontrollkort om identifiering av kortinnehavare (krav 360 och 366 i bilaga 1C).

```
ControlCardHolderIdentification ::= SEQUENCE {
   controlBodyName                     Name,
   controlBodyAddress                  Address,
   cardHolderName                      HolderName,
   cardHolderPreferredLanguage         Language
}
```

controlBodyName är namn på kortinnehavarens kontrollorgan.

controlBodyAddress är adress till kortinnehavarens kontrollorgan.

cardHolderName är kontrollkortsinnehavarens namn och förnamn.

▼B

cardHolderPreferredLanguage är det språk som kortinnehavaren väljer.

2.53. **ControlType**

Kod som anger de aktiviteter som utförts vid en kontroll. Denna datatyp berörs av krav 126, 274, 299, 327 och 350 i bilaga 1C.

```
ControlType ::= OCTET STRING (SIZE(1))
```

Generation 1:

Värdetilldelning – oktettgrupperad: ‘cvpdxxxx’B (8 bitar)

‘c’B Överföring från kort:

‘0’B: Ingen överföring från kort under denna kontrollaktivitet.

‘1’B: Överföring från kort utförd under denna kontrollaktivitet.

‘v’B Överföring från fordonsenhet:

‘0’B: Ingen överföring från fordonsenhet under denna kontrollaktivitet.

‘1’B: Överföring från fordonsenhet utförd under denna kontrollaktivitet.

‘p’B Utskrift:

‘0’B: Ingen utskrift under denna kontrollaktivitet.

‘1’B: Utskrift gjord under denna kontrollaktivitet.

‘d’B Bildskärm:

‘0’B: Ingen bildskärm använd under denna kontrollaktivitet.

‘1’B: Bildskärm använd under denna kontrollaktivitet.

‘xxxx’B Används ej.

Generation 2:

Värdetilldelning – oktettgrupperad: ‘cvpdexxx’B (8 bitar)

‘c’B Överföring från kort:

‘0’B: Ingen överföring från kort under denna kontrollaktivitet.

‘1’B: Överföring från kort utförd under denna kontrollaktivitet.

‘v’B Överföring från fordonsenhet:

‘0’B: Ingen överföring från fordonsenhet under denna kontrollaktivitet.

‘1’B: Överföring från fordonsenhet utförd under denna kontrollaktivitet.

‘p’B Utskrift.

‘0’B: Ingen utskrift under denna kontrollaktivitet.

‘1’B: Utskrift gjord under denna kontrollaktivitet.

▼B

‘d’B	Bildskärm:
	‘0’B: Ingen bildskärm använd under denna kontrollaktivitet.
	‘1’B: Bildskärm använd under denna kontrollaktivitet.
‘e’B	Kalibreringskontroll på väg:
	‘0’B: Inga kalibreringsparametrar kontrollerade under denna kontrollaktivitet.
	‘1’B: Kalibreringsparametrar kontrollerade under denna kontrollaktivitet.
‘xxx’B	RFU.

2.54. **CurrentDateTime**

Färdskrivarens aktuella datum och tidpunkt.

```
CurrentDateTime ::= TimeReal
```

Värdetilldelning: Ej närmare angiven.

2.55. **CurrentDateTimeRecordArray**

Generation 2:

Aktuellt datum och aktuell tid samt metadata som används i överföringsprotokollet.

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

recordType anger typen av post (CurrentDateTime). **Värdetilldelning:** Se RecordType.

recordSize är storleken av CurrentDateTime i byte.

noOfRecords är antalet poster i postmängden.

records är en mängd av poster med aktuellt datum och aktuell tidpunkt.

2.56. **DailyPresenceCounter**

Räknare, lagrad i ett förar- eller verkstadskort, som ökas med ett steg för varje kalenderdag som kortet varit insatt i en fordonsenhet. Denna datatyp berörs av krav 266, 299, 320 och 343 i bilaga 1C.

```
DailyPresenceCounter ::= BCDString(SIZE(2))
```

Värdetilldelning: Löpnummer med högsta värde 9 999, varpå det börjar om från 0. Då kortet utfärdas första gången sätts numret till 0.

▼B

2.57. **Datef**

Datum uttryckt i ett numeriskt format som är lätt att skriva ut.

```
Datef ::= SEQUENCE {
   year        BCDString(SIZE(2)),
   month       BCDString(SIZE(1)),
   day         BCDString(SIZE(1))
}
```

Värdetilldelning:

yyyy	År
mm	Månad
dd	Dag
‘00000000’H	Anger uttryckligen frånvaro av datum.

2.58. **DateOfDayDownloaded**

Generation 2:

Datum och tidpunkt för överföringen.

```
DateOfDayDownloaded ::= TimeReal
```

Värdetilldelning: Ej närmare angiven.

2.59. **DateOfDayDownloadedRecordArray**

Generation 2:

Datum och tid för överföringen samt metadata som används i överföringsprotokollet.

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

recordType anger typen av post (DateOfDayDownloaded). **Värdetilldelning:** Se RecordType.

recordSize är storleken av CurrentDateTime i byte.

noOfRecords är antalet poster i postmängden.

records är mängden av poster med datum och tidpunkt för överföringen.

2.60. **Distance**

En tillryggalagd sträcka (resultat av beräkning av skillnaden i kilometer mellan två vägmätarställningar i ett fordon).

```
Distance ::= INTEGER(0..2^16-1)
```

Värdetilldelning: Binär utan tecken. Värde i km i området 0 till 9 999 km.

2.61. **DriverCardApplicationIdentification**

Information lagrad i ett förarkort om identifiering av korttillämpningen (krav 253 och 278 i bilaga 1C).

▼B

Generation 1:

```
DriverCardApplicationIdentification ::= SEQUENCE {
   typeOfTachographCardId              EquipmentType,
   cardStructureVersion                CardStructureVersion,
   noOfEventsPerType                   NoOfEventsPerType,
   noOfFaultsPerType                   NoOfFaultsPerType,
   activityStructureLength             CardActivityLengthRange,
   noOfCardVehicleRecords              NoOfCardVehicleRecords,
   noOfCardPlaceRecords                NoOfCardPlaceRecords
}
```

typeOfTachographCardId specificerar använd korttyp.

cardStructureVersion specificerar versionen av den struktur som används i kortet.

noOfEventsPerType är antalet händelser per händelsetyp som kortet kan registrera.

noOfFaultsPerType är antalet fel per typ av fel som kortet kan registrera.

activityStructureLength anger antal byte som finns tillgängliga för lagring av aktivitetsposter.

noOfCardVehicleRecords är antalet fordonsposter som kortet kan registrera.

noOfCardPlaceRecords är det antal platser som kortet kan lagra.

Generation 2:

```
DriverCardApplicationIdentification ::= SEQUENCE {
   typeOfTachographCardId              EquipmentType,
   cardStructureVersion                CardStructureVersion,
   noOfEventsPerType                   NoOfEventsPerType,
   noOfFaultsPerType                   NoOfFaultsPerType,
   activityStructureLength             CardActivityLengthRange,
   noOfCardVehicleRecords              NoOfCardVehicleRecords,
   noOfCardPlaceRecords                NoOfCardPlaceRecords,
   noOfGNSSCDRecords                   NoOfGNSSCDRecords,
   noOfSpecificConditionRecords        NoOfSpecificConditionRecords
}
```

Jämfört med generation 1 används följande ytterligare dataelement:

noOfGNSSCDRecords är det antal GNSS-poster om sammanhängande körning som kortet kan lagra.

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

2.62. **DriverCardHolderIdentification**

Information lagrad i ett förarkort om identifiering av kortinnehavare (krav 256 och 281 i bilaga 1C).

```
DriverCardHolderIdentification ::= SEQUENCE {
   cardHolderName                      HolderName,
   cardHolderBirthDate                 Datef,
   cardHolderPreferredLanguage         Language
}
```

▼B

cardHolderName är förarkortsinnehavarens namn och förnamn.

cardHolderBirthDate förarkortsinnehavarens födelsedatum.

cardHolderPreferredLanguage är det språk som kortinnehavaren väljer.

2.63. **DSRCSecurityData**

Generation 2:

Information i klartext samt MAC som ska sändas via DSRC från färdskrivaren till fjärravläsaren (se tillägg 11 del B kapitel 13 för detaljinformation).

```
DSRCSecurityData ::= SEQUENCE {
   tagLenthPlainText                    OCTET STRING(SIZE(2)),
   currentDateTime                      CurrentDateTime,
   counter                              INTEGER(0..2^24-1),
   vuSerialNumber                       VuSerialNumber,
   dSRCMKVersionNumber                  INTEGER(SIZE(1)),
   tagLengthMac                         OCTET STRING(SIZE(2)),
   mac                                  MAC
}
```

tagLength utgör en del av DER-TLV-kodningen och ska sättas till ‘81 10’ (se tillägg 11 del B kapitel 13).

currentDateTime är fordonsenhetens aktuella datum och tidpunkt.

counter räknar RTM-meddelanden.

vuSerialNumber är fordonsenhetens serienummer.

dSRCMKVersionNumber är versionsnumret för den huvudnyckel till DSRC från vilken fordonsenhetens specifika DSRC-nycklar genererades.

tagLengthMac är tagg och längd för dataobjektet för MAC och utgör en del av DER-TLV-kodningen. Taggen ska sättas till ‘8E’, längden ska koda längden av MAC i oktetter (se tillägg 11 del B kapitel 13).

mac är beräknad MAC för RTM-meddelandet (se tillägg 11 del B kapitel 13).

2.64. **EGFCertificate**

Generation 2:

Certifikat för den externa GNSS-anordningens öppna nyckel vid ömsesidig autentisering med en fordonsenhet. Strukturen för detta certifikat anges i tillägg 11.

```
EGFCertificate ::= Certificate
```

▼B

2.65. **EmbedderIcAssemblerId**

Ger information om den integrerade kretsens inbäddare.

```
EmbedderIcAssemblerId ::= SEQUENCE{
   countryCode                          IA5String(SIZE(2)),
   moduleEmbedder                       BCDString(SIZE(2)),
   manufacturerInformation              OCTET STRING(SIZE(1))
}
```

countryCode är landskoden (två tecken) för modulens inbäddare i enlighet med ISO 3166.

moduleEmbedder identifierar modulens inbäddare.

manufacturerInformation är avsett för tillverkarens interna bruk.

2.66. **EntryTypeDailyWorkPeriod**

Kod för att åtskilja påbörjande och avslutande av en angivelse av plats för en arbetsperiod och angivelsevillkor.

Generation 1:

```
EntryTypeDailyWorkPeriod ::= INTEGER {
   Begin,  related time = card insertion time or time of entry          (0),
   End,    related time = card withdrawal time or time of entry        (1),
   Begin,  related time manually entered (start time)                  (2),
   End,    related time manually entered (end of work period)          (3),
   Begin,  related time assumed by VU                                  (4),
   End,    related time assumed by VU                                  (5)
}
```

Värdetilldelning: Enligt ISO/IEC8824-1.

Generation 2:

```
EntryTypeDailyWorkPeriod ::= INTEGER {
   Begin,  related time = card insertion time or time of entry          (0),
   End,    related time = card withdrawal time or time of entry        (1),
   Begin,  related time manually entered (start time)                  (2),
   End,    related time manually entered (end of work period)          (3),
   Begin,  related time assumed by VU                                  (4),
   End,    related time assumed by VU                                  (5),
   Begin,  related time based on GNSS data                             (6),
   End     related time based on GNSS data                             (7)
}
```

Värdetilldelning: Enligt ISO/IEC8824-1.

2.67. **EquipmentType**

Kod för att åtskilja olika typer av utrustning för färdskrivartillämpningen.

```
EquipmentType ::= INTEGER(0..255)
```

▼B

Generation 1:

```
--Reserved                          (0),
--Driver Card                       (1),
--Workshop Card                     (2),
--Control Card                      (3),
--Company Card                      (4),
--Manufacturing Card                (5),
--Vehicle Unit                      (6),
--Motion Sensor                     (7),
--RFU                               (8..255)
```

Värdetilldelning: Enligt ISO/IEC8824-1.

Värde 0 är reserverat för angivelse av en medlemsstat eller Europa i certifikatens CHA-fält (certifikatinnehavarens auktorisering).

Generation 2:

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
--RFU                               (17..255)
```

Anmärkning: 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.

2.68. **EuropeanPublicKey**

Generation 1:

Den europeiska öppna nyckeln.

```
EuropeanPublicKey ::= PublicKey
```

2.69. **EventFaultRecordPurpose**

Kod som anger varför en händelse eller ett fel har registrerats.

```
EventFaultRecordPurpose ::= OCTET STRING (SIZE(1))
```

Värdetilldelning:

'00'H	En/ett av de tio senaste (eller sista) händelserna eller felen.
'01'H	Den längsta händelsen för ett av de senaste tio dygnen händelsen inträffat.
'02'H	En av de fem längsta händelserna under de senaste 365 dygnen.
'03'H	Den senaste händelsen för ett av de senaste tio dygnen händelsen inträffat.
'04'H	Den allvarligaste händelsen för ett av de senaste tio dygnen händelsen inträffat.
'05'H	En av de fem allvarligaste händelserna under de senaste 365 dygnen.
'06'H	Den första händelse eller det första fel som inträffat efter senaste kalibrering.
'07'H	En aktiv/pågående händelse eller ett aktivt/pågående fel.
'08'H to '7F'H	RFU
'80'H to 'FF'H	Tillverkarspecifikt

▼B

2.70. **EventFaultType**

Kod för typ av händelse eller fel.

```
EventFaultType ::= OCTET STRING (SIZE(1))
```

Värdetilldelning:

Generation 1:

'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' to '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 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 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	Tillverkarspecifik.

▼B

Generation 2:

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

‘0B’H	Tidskonflikt (GNSS jämfört med fordonsenhetens interna klocka).
‘0C’ to ‘0F’H	RFU.
‘5x’H	Fel avseende GNSS.
‘50’H	Inga närmare detaljer.
‘51’H	Internt fel i GNSS-mottagare.
‘52’H	Externt fel i GNSS-mottagare.
‘53’H	Externt fel i GNSS-kommunikation.
‘54’H	Positionsdata från GNSS saknas.
‘55’H	GNSS-manipulering upptäckt.
‘56’H	Certifikat för extern GNSS-anordning har löpt ut.
‘57’H to ‘5F’H	RFU.
‘6x’H	Fel avseende fjärrkommunikationsmodul.
‘60’H	Inga närmare detaljer.
‘61’H	Fel i fjärrkommunikationsmodul.
‘62’H	Kommunikationsfel i fjärrkommunikationsmodul.
‘63’H to ‘6F’H	RFU.
‘7x’H	Fel i ITS-gränssnitt.
‘70’H	Inga närmare detaljer.
‘71’H to ‘7F’H	RFU

2.71. **ExtendedSealIdentifier**

Generation 2:

En unik identifierare för en plombering (krav 401 i bilaga 1C).

```
ExtendedSealIdentifier ::= SEQUENCE{
   manufacturerCode                    OCTET STRING (SIZE(2)),
   sealIdentifier                      OCTET STRING (SIZE(6))
}
```

manufacturerCode är en kod för tillverkaren av plomberingen.

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

2.72. **ExtendedSerialNumber**

Unik identifiering av en utrustning. Den kan även användas som en identifierare för en utrustnings öppna nyckel.

Generation 1:

```
ExtendedSerialNumber ::= SEQUENCE{
   serialNumber                        INTEGER(0..2^32-1),
   monthYear                           BCDString(SIZE(2)),
   type                                OCTET STRING(SIZE(1)),
   manufacturerCode                    ManufacturerCode
}
```

serialNumber är ett serienummer för utrustningen, som är unikt för tillverkaren, utrustningstypen och månaden och året nedan.

monthYear är identifiering av månad och år för tillverkning (eller för tilldelning av serienummer).

▼B

Värdetilldelning: BCD-kodning av månad (två siffror) och år (två sista siffrorna).

type är en identifierare för typ av utrustning.

Värdetilldelning: Tillverkarspecifik, med 'FFh' som reserverat värde.

manufacturerCode är den numeriska kod som identifierar en tillverkare av typgodkänd utrustning.

Generation 2:

```
ExtendedSerialNumber ::= SEQUENCE{
   serialNumber                          INTEGER(0..2^32-1),
   monthYear                             BCDString(SIZE(2)),
   type                                  EquipmentType,
   manufacturerCode                      ManufacturerCode
}
```

serialNumber: se generation 1.

monthYear: se generation 1.

type anger typ av utrustning.

manufacturerCode: se generation 1.

2.73. **FullCardNumber**

Kod som fullständigt identifierar ett färdskrivarkort.

```
FullCardNumber ::= SEQUENCE {
   cardType                              EquipmentType,
   cardIssuingMemberState                NationNumeric,
   cardNumber                            CardNumber
}
```

cardType är typ av färdskrivarkort.

cardIssuingMemberState är kod för den medlemsstat som har utfärdat kortet.

cardNumber är kortnumret.

2.74. **FullCardNumberAndGeneration**

Generation 2:

Kod som fullständigt identifierar ett färdskrivarkort och dess generation.

```
FullCardNumberAndGeneration ::= SEQUENCE {
   fullCardNumber                        FullCardNumber,
   generation                            Generation
}
```

fullcardNumber identifierar färdskrivarkortet.

generation anger den generation av färdskrivarkortet som används.

▼B

2.75. **Generation**

Generation 2:

Anger den generation av färdskrivarkortet som används.

```
Generation ::= INTEGER(0..255)
```

Värdetilldelning:

‘00’H	RFU
‘01’H	Generation 1
‘02’H	Generation 2
‘03’H .. ‘FF’H	RFU

2.76. **GeoCoordinates**

Generation 2:

Geografiska koordinater kodade som heltal. Dessa heltal är multiplar av kodningen i form av ± DDMM.M för latitud och ± DDDMM.M för longitud. ± DD respektive ± DDD anger här graderna och MM.M minuterna.

```
GeoCoordinates ::= SEQUENCE {
   latitude                                INTEGER(-90000..90001),
   longitude                               INTEGER(-180000..180001)
}
```

latitude är kodad som en multipel (faktor 10) av värdet representerat som ± DDMM.M.

longitude är kodad som en multipel (faktor 10) av värdet representerat som ± DDDMM.M.

2.77. **GNSSAccuracy**

Generation 2:

Precisionen hos positionsdata från GNSS (se definition eee)). Denna precision kodas som ett heltal och är en multipel (faktor 10) av det X.Y-värde som ges av GSA-satsen enligt NMEA.

```
GNSSAccuracy ::= INTEGER(1..100)
```

2.78. **GNSSContinuousDriving**

Generation 2:

Information lagrad på ett förarkort eller verkstadskort om fordonets GNSS-position om förarens sammanhängande körtid uppnår en multipel av tre timmar (krav 306 och 354 i bilaga 1C).

```
GNSSContinuousDriving := SEQUENCE {
   gnssCDPointerNewestRecord               INTEGER(0..NoOfGNSSCDRecords -1),
   gnssContinuousDrivingRecords            SET SIZE(NoOfGNSSCDRecords) OF
                                           GNSSContinuousDrivingRecord
}
```

gnssCDPointerNewestRecord är index för senast uppdaterade GNSS-post om sammanhängande körning.

▼B

Värdetilldelning: Ett tal som motsvarar numeratorn för GNSS-posten om sammanhängande körning, och som börjar med ‘0’ för den första gången GNSS-posterna om sammanhängande körning uppträder i strukturen.

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

2.79. **GNSSContinuousDrivingRecord**

Generation 2:

Information lagrad på ett förarkort eller verkstadskort om fordonets GNSS-position om förarens sammanhängande körtid uppnår en multipel av tre timmar (krav 305 och 353 i bilaga 1C).

```
GNSSContinuousDrivingRecord ::= SEQUENCE {
   timeStamp                                TimeReal,
   gnssPlaceRecord                          GNSSPlaceRecord
}
```

timeStamp är datum och tidpunkt när kortinnehavarens sammanhängande körtid uppgår till en multipel av tre timmar.

gnssPlaceRecord innehåller information om fordonets position.

2.80. **GNSSPlaceRecord**

Generation 2:

Information om fordonets GNSS-position (krav 108, 109, 110, 296, 305, 347 och 353 i bilaga 1C).

```
GNSSPlaceRecord ::= SEQUENCE {
   timeStamp                                TimeReal,
   gnssAccuracy                             GNSSAccuracy,
   geoCoordinates                           GeoCoordinates
}
```

timeStamp är datum och tidpunkt när fordonets GNSS-position fastställdes.

gnssAccuracy är precisionen hos positionsdata från GNSS.

geoCoordinates är den plats som registrerats med hjälp av GNSS.

2.81. **HighResOdometer**

Fordonets vägmätarställning: Sammanlagd sträcka som tillryggalagts av fordonet vid drift.

```
HighResOdometer ::= INTEGER(0..2^32-1)
```

▼B

Värdetilldelning: Binär utan tecken. Värde i intervallet från 0 till 21 055 406 km, i steg om 1/200 km.

2.82. **HighResTripDistance**

En sträcka som tillryggalagts under en hel eller en del av en resa.

```
HighResTripDistance ::= INTEGER(0..2^32-1)
```

Värdetilldelning: Binär utan tecken. Värde i intervallet från 0 till 21 055 406 km, i steg om 1/200 km.

2.83. **HolderName**

En kortinnehavares efternamn och förnamn.

```
HolderName ::= SEQUENCE {
   holderSurname                    Name,
   holderFirstNames                 Name
}
```

holderSurname är innehavarens efternamn. Efternamnet inbegriper inte titlar.

Värdetilldelning: Om ett kort inte är personligt innehåller **holderSurname** samma information som **companyName**, **workshopName** eller **controlBodyName**.

holderFirstNames är innehavarens förnamn och initialer.

2.84. **InternalGNSSReceiver**

Generation 2:

Information om huruvida GNSS-mottagaren är intern eller extern i förhållande till fordonsenheten. TRUE innebär att GNSS-mottagaren är intern. FALSE innebär att GNSS-mottagaren är extern.

```
InternalGNSSReceiver ::= BOOLEAN
```

2.85. **K-ConstantOfRecordingEquipment**

Färdskrivarens konstant (definition m)).

```
K-ConstantOfRecordingEquipment ::= INTEGER(0..2^16-1)
```

Värdetilldelning: Pulser per kilometer i intervallet från 0 till 64 255 pulser/km.

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
}
```

▼B

Det första alternativet är lämpligt för att referera till en fordonsenhets eller ett färdskrivarkorts öppna nyckel.

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

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

2.87. **KMWCKey**

Generation 2:

AES-nyckel och dess tillhörande nyckelversion som används för parning av fordonsenhet och rörelsesensor. För mer information, se tillägg 11.

```
KMWCKey ::= SEQUENCE {
   kMWCKey                                 AESKey,
   keyVersion                              INTEGER (SIZE(1))
}
```

kMWCKey AES-nyckelns längd, konkatenerad med den nyckel som används för parning av fordonsenhet och rörelsesensor.

keyVersion anger AES-nyckelns nyckelversion.

2.88. **Language**

Kod för ett språk.

```
Language ::= IA5String(SIZE(2))
```

Värdetilldelning: Kodning med två gemener enligt ISO 639.

2.89. **LastCardDownload**

Datum och tidpunkt, lagrade i förarkortet, för den senaste kortöverföringen (för andra än kontrolländamål) (krav 257 och 282 i bilaga 1C).. Detta datum kan uppdateras av en fordonsenhet och alla typer av kortläsare.

```
LastCardDownload ::= TimeReal
```

Värdetilldelning: Ej närmare angiven.

2.90. **LinkCertificate**

Generation 2:

Länkcertifikat mellan Erca-nyckelpar.

```
LinkCertificate ::= Certificate
```

2.91. **L-TyreCircumference**

Däckens effektiva omkrets (definition u)).

```
L-TyreCircumference ::= INTEGER(0.. 2^16-1)
```

▼B

Värdetilldelning: Binär utan tecken, värde i intervallet från 0 till 8 031 mm, i steg om 1/8 mm.

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(12))
}
```

2.93. **ManualInputFlag**

Kod som anger om en kortinnehavare manuellt har angivit föraraktiviteter vid kortinsättning eller inte (krav 081 i bilaga 1B och krav 102 i bilaga 1C).

```
ManualInputFlag ::= INTEGER {
   noEntry                                 (0)
   manualEntries                           (1)
}
```

Värdetilldelning: Ej närmare angiven.

2.94. **ManufacturerCode**

Kod som anger en tillverkare av typgodkänd utrustning.

```
ManufacturerCode ::= INTEGER(0..255)
```

Det laboratorium som är behörigt att utföra provningar av driftskompatibilitet ska underhålla och offentliggöra förteckningen över tillverkarkoder på sin webbplats (krav 454 i bilaga 1C).

Utvecklare av färdskrivare som ansöker om tillverkarkoder hos laboratoriet för provning av driftskompatibilitet ska tilldelas en preliminär tillverkarkod.

2.95. **ManufacturerSpecificEventFaultData**

Generation 2:

Tillverkarspecifika felkoder som förenklar felanalys i och underhåll av fordonsenheter.

```
ManufacturerSpecificEventFaultData ::= SEQUENCE {
   manufacturerCode                        ManufacturerCode,
   manufacturerSpecificErrorCode           OCTET STRING(SIZE(3))
}
```

manufacturerCode anger fordonsenhetens tillverkare.

manufacturerSpecificErrorCode är en tillverkarspecifik felkod.

▼B

2.96. **MemberStateCertificate**

Certifikat för en medlemsstats öppna nyckel utfärdat av den europeiska certifieringsinstansen.

```
MemberStateCertificate ::= Certificate
```

2.97. **MemberStateCertificateRecordArray**

Generation 2:

Medlemsstatens certifikat samt metadata som används i överföringsprotokollet.

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

recordType anger typen av post (MemberStateCertificate). **Värdetilldelning:** Se RecordType.

recordSize är storleken av MemberStateCertificate i byte.

noOfRecords är antalet poster i postmängden. Värdet ska sättas till 1 eftersom certifikaten kan ha olika längd.

records är mängden av medlemsstatscertifikat.

2.98. **MemberStatePublicKey**

Generation 1:

En medlemsstats öppna nyckel.

```
MemberStatePublicKey ::= PublicKey
```

2.99. **Namn**

Ett namn.

```
Name ::= SEQUENCE {
   codePage                            INTEGER (0..255),
   name                                OCTET STRING (SIZE(35))
}
```

codePage specificerar en teckenmängd som definieras i kapitel 4.

name är ett namn som kodats enligt den specificerade teckenmängden.

2.100. **NationAlpha**

Alfabetisk referens för ett land, i överensstämmelse med de landsbeteckningar som används på fordon i internationell trafik (Förenta nationernas konvention om vägtrafik, Wien 1968).

```
NationAlpha ::= IA5String(SIZE(3))
```

De alfabetiska och numeriska landkoderna ska finnas i en förteckning på webbplatsen för det laboratorium som har utsetts för att utföra provningar av driftskompatibilitet i enlighet med krav 440 i bilaga 1C.

▼B

2.101. **NationNumeric**

Numerisk referens för ett land.

```
NationNumeric ::= INTEGER(0 .. 255)
```

Värdetilldelning: se datatyp 2.100 (NationAlpha).

De alfabetiska eller numeriska landspecifikationer som beskrivs i respektive avsnitt får endast ändras efter det att det utsedda laboratoriet har inhämtat synpunkter från tillverkarna av de typgodkända fordonsenheterna med digital eller smart färdskrivare.

2.102. **NoOfCalibrationRecords**

Antal kalibreringsposter som ett verkstadskort kan lagra.

Generation 1:

```
NoOfCalibrationRecords ::= INTEGER(0..255)
```

Värdetilldelning: Se tillägg 2.

Generation 2:

```
NoOfCalibrationRecords ::= INTEGER(0..2^16-1)
```

Värdetilldelning: Se tillägg 2.

2.103. **NoOfCalibrationsSinceDownload**

Räknare som anger det antal kalibreringar som utförts med ett verkstadskort sedan den senaste överföringen från det (krav 317 och 340 i bilaga 1C).

```
NoOfCalibrationsSinceDownload ::= INTEGER(0..2^16-1)
```

Värdetilldelning: Ej närmare angiven.

2.104. **NoOfCardPlaceRecords**

Antal platsposter som ett förar- eller verkstadskort kan lagra.

Generation 1:

```
NoOfCardPlaceRecords ::= INTEGER(0..255)
```

Värdetilldelning: Se tillägg 2.

Generation 2:

```
NoOfCardPlaceRecords ::= INTEGER(0..2^16-1)
```

Värdetilldelning: Se tillägg 2.

▼B

2.105. **NoOfCardVehicleRecords**

Antal poster för använda fordon som ett förar- eller verkstadskort kan lagra.

```
NoOfCardVehicleRecords ::= INTEGER(0.. 2^16-1)
```

Värdetilldelning: Se tillägg 2.

2.106. **NoOfCardVehicleUnitRecords**

Generation 2:

Antal poster för använda fordonsenheter som ett förar- eller verkstadskort kan lagra.

```
NoOfCardVehicleUnitRecords ::= INTEGER(0.. 2^16-1)
```

Värdetilldelning: Se tillägg 2.

2.107. **NoOfCompanyActivityRecords**

Antal poster för företagsaktiviteter som ett företagskort kan lagra.

```
NoOfCompanyActivityRecords ::= INTEGER(0.. 2^16-1)
```

Värdetilldelning: Se tillägg 2.

2.108. **NoOfControlActivityRecords**

Antal poster för kontrollaktiviteter som ett kontrollkort kan lagra.

```
NoOfControlActivityRecords ::= INTEGER(0.. 2^16-1)
```

Värdetilldelning: Se tillägg 2.

2.109. **NoOfEventsPerType**

Antal händelser per händelsetyp som ett kort kan lagra.

```
NoOfEventsPerType ::= INTEGER(0..255)
```

Värdetilldelning: Se tillägg 2.

2.110. **NoOfFaultsPerType**

Antal fel per typ av fel som ett kort kan lagra.

```
NoOfFaultsPerType ::= INTEGER(0..255)
```

Värdetilldelning: Se tillägg 2.

▼B

2.111. **NoOfGNSSCDRecords**

Generation 2:

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

```
NoOfGNSSCDRecords ::= INTEGER(0..2^16-1)
```

Värdetilldelning: Se tillägg 2.

2.112. **NoOfSpecificConditionRecords**

Generation 2:

Det antal poster för särskilda omständigheter som ett kort kan lagra.

```
NoOfSpecificConditionRecords ::= INTEGER(0..2^16-1)
```

Värdetilldelning: Se tillägg 2.

2.113. **OdometerShort**

Fordonets vägmätarställning i kortform.

```
OdometerShort ::= INTEGER(0..2^24-1)
```

Värdetilldelning: Binär utan tecken. Värde i km i intervallet från 0 till 9 999 999 km.

2.114. **OdometerValueMidnight**

Fordonets vägmätarställning vid midnatt ett visst datum (krav 090 i bilaga 1B och krav 113 i bilaga 1C).

```
OdometerValueMidnight ::= OdometerShort
```

Värdetilldelning: Ej närmare angiven.

2.115. **OdometerValueMidnightRecordArray**

Generation 2:

OdometerValueMidnight samt metadata som används i överföringsprotokollet.

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

recordType anger typen av post (OdometerValueMidnight). **Värdetilldelning:** Se RecordType.

recordSize är storleken av OdometerValueMidnight i byte.

noOfRecords är antalet poster i postmängden.

records är mängden av OdometerValueMidnight-poster.

▼B

2.116. **OverspeedNumber**

Antalet händelser av typen hastighetsöverträdelse sedan den senaste kontrollen av hastighetsöverträdelse.

```
OverspeedNumber ::= INTEGER(0..255)
```

Värdetilldelning: 0 innebär att ingen händelse av typen hastighetsöverträdelse har ägt rum sedan den senaste kontrollen av hastighetsöverträdelse, 1 innebär att en händelse av denna typ har ägt rum sedan den senaste kontrollen av hastighetsöverträdelse, … 255 innebär att 255 eller fler händelser av typen hastighetsöverträdelse har ägt rum sedan den senaste kontrollen av hastighetsöverträdelse.

2.117. **PlaceRecord**

Information om en plats där en arbetsperiod påbörjas eller avslutas (krav 108, 271, 296, 324 och 347 i bilaga 1C).

Generation 1:

```
PlaceRecord ::= SEQUENCE {
   entryTime                          TimeReal,
   entryTypeDailyWorkPeriod           EntryTypeDailyWorkPeriod,
   dailyWorkPeriodCountry             NationNumeric,
   dailyWorkPeriodRegion              RegionNumeric,
   vehicleOdometerValue               OdometerShort
}
```

entryTime är datum och tidpunkt för angivelsen.

entryTypeDailyWorkPeriod är typ av angivelse.

dailyWorkPeriodCountry är det land som anges.

dailyWorkPeriodRegion är den region som anges.

vehicleOdometerValue är vägmätarställningen vid tidpunkten för angivelse av plats.

Generation 2:

```
PlaceRecord ::= SEQUENCE {
   entryTime                          TimeReal,
   entryTypeDailyWorkPeriod           EntryTypeDailyWorkPeriod,
   dailyWorkPeriodCountry             NationNumeric,
   dailyWorkPeriodRegion              RegionNumeric,
   vehicleOdometerValue               OdometerShort,
   entryGNSSPlaceRecord               GNSSPlaceRecord
}
```

Jämfört med generation 1 används följande ytterligare komponent:

entryGNSSPlaceRecord är den registrerade platsen och tiden.

▼B

2.118. **PreviousVehicleInfo**

Information om det fordon som tidigare använts av en förare när föraren sätter in sitt kort i en fordonsenhet (krav 081 i bilaga 1B och krav 102 i bilaga 1C).

Generation 1:

```
PreviousVehicleInfo ::= SEQUENCE {
   vehicleRegistrationIdentification      VehicleRegistrationIdentification,
   cardWithdrawalTime                     TimeReal
}
```

vehicleRegistrationIdentification är fordonets registreringsnummer och den medlemsstat där fordonet är registrerat.

cardWithdrawalTime är tidpunkt och datum för uttag av kort.

Generation 2:

```
PreviousVehicleInfo ::= SEQUENCE {
   vehicleRegistrationIdentification      VehicleRegistrationIdentification,
   cardWithdrawalTime                     TimeReal,
   vuGeneration                           Generation
}
```

Jämfört med generation 1 används följande ytterligare dataelement:

vuGeneration anger fordonsenhetens generation.

2.119. **PublicKey**

Generation 1:

En öppen RSA-nyckel.

```
PublicKey ::= SEQUENCE {
   rsaKeyModulus                          RSAKeyModulus,
   rsaKeyPublicExponent                   RSAKeyPublicExponent
}
```

rsaKeyModulus är modulus för nyckelparet.

rsaKeyPublicExponent är den öppna exponenten för nyckelparet.

2.120. **RecordType**

Generation 2:

Hänvisning till en posttyp. Denna datatyp används i RecordArrays.

```
RecordType ::= OCTET STRING(SIZE(1))
```

▼B

Värdetilldelning:

'01'H	ActivityChangeInfo
'02'H	CardSlotsStatus
'03'H	CurrentDateTime
'04'H	MemberStateCertificate
'05'H	OdometerValueMidnight
'06'H	DateOfDayDownloaded
'07'H	SensorPaired
'08'H	Signature
'09'H	SpecificConditionRecord
'0A'H	VehicleIdentificationNumber
'0B'H	VehicleRegistrationNumber
'0C'H	VuCalibrationRecord
'0D'H	VuCardIWRecord
'0E'H	VuCardRecord
'0F'H	VuCertificate
'10'H	VuCompanyLocksRecord
'11'H	VuControlActivityRecord
'12'H	VuDetailedSpeedBlock
'13'H	VuDownloadablePeriod
'14'H	VuDownloadActivityData
'15'H	VuEventRecord
'16'H	VuGNSSCDRecord
'17'H	VuITSConsentRecord
'18'H	VuFaultRecord
'19'H	VuIdentification
'1A'H	VuOverSpeedingControlData
'1B'H	VuOverSpeedingEventRecord
'1C'H	VuPlaceDailyWorkPeriodRecord
'1D'H	VuTimeAdjustmentGNSSRecord
'1E'H	VuTimeAdjustmentRecord
'1F'H	VuPowerSupplyInterruptionRecord
'20'H	SensorPairedRecord
'21'H	SensorExternalGNSSCoupledRecord
'22'H to '7F'H	RFU
'80'H to 'FF'H	Tillverkarspecifik.

2.121. **RegionAlpha**

Alfabetisk referens för en region i ett visst land.

```
RegionAlpha ::= IA5STRING(SIZE(3))
```

Generation 1:

Värdetilldelning:

' '	No information available,
Spain:	
'AN '	Andalucía,
'AR '	Aragón,
'AST'	Asturias,
'C '	Cantabria,
'CAT'	Cataluña,
'CL '	Castilla-León,
'CM '	Castilla-La-Mancha,
'CV'	Valencia,
'EXT'	Extremadura,
'G '	Galicia,
'IB '	Baleares,
'IC '	Canarias,
'LR '	La Rioja,
'M '	Madrid,
'MU '	Murcia,
'NA '	Navarra,
'PV '	País Vasco

▼B

Generation 2:

Koderna för RegionAlpha ska finnas i en förteckning på webbplatsen för det laboratorium som har utsetts för att utföra provning av driftskompatibilitet.

2.122. **RegionNumeric**

Numerisk referens för en region i ett visst land.

```
RegionNumeric ::= OCTET STRING (SIZE(1))
```

Generation 1:

Värdetilldelning:

```
'00'H        No information available,
Spain:
'01'H        Andalucía,
'02'H        Aragón,
'03'H        Asturias,
'04'H        Cantabria,
'05'H        Cataluña,
'06'H        Castilla-León,
'07'H        Castilla-La-Mancha,
'08'H        Valencia,
'09'H        Extremadura,
'0A'H        Galicia,
'0B'H        Baleares,
'0C'H        Canarias,
'0D'H        La Rioja,
'0E'H        Madrid,
'0F'H        Murcia,
'10'H        Navarra,
'11'H        País Vasco
```

Generation 2:

Koderna för RegionNumeric ska finnas i en förteckning på webbplatsen för det laboratorium som har utsetts för att utföra provning av driftskompatibilitet.

2.123. **RemoteCommunicationModuleSerialNumber**

Generation 2:

Fjärrkommunikationsmodulens serienummer.

```
RemoteCommunicationModuleSerialNumber ::= ExtendedSerialNumber
```

2.124. **RSAKeyModulus**

Generation 1:

Modulus för ett RSA-nyckelpar.

```
RSAKeyModulus ::= OCTET STRING (SIZE(128))
```

Värdetilldelning: Ospecificerad.

2.125. **RSAKeyPrivateExponent**

Generation 1:

Privat exponent för ett RSA-nyckelpar.

```
RSAKeyPrivateExponent ::= OCTET STRING (SIZE(128))
```

Värdetilldelning: Ospecificerad.

▼B

2.126. **RSAKeyPublicExponent**

Generation 1:

Öppen exponent för ett RSA-nyckelpar.

```
RSAKeyPublicExponent ::= OCTET STRING (SIZE(8))
```

Värdetilldelning: Ospecificerad.

2.127. **RtmData**

Generation 2:

Se tillägg 14 för en definition av denna datatyp.

2.128. **SealDataCard**

Generation 2:

Denna datatyp lagrar information om de plomberingar som anbringats på de olika komponenterna i ett fordon och är avsedd för lagring i ett kort. Denna datatyp berörs av krav 337 i bilaga 1C.

```
SealDataCard ::= SEQUENCE {
   noOfSealRecords                    INTEGER(1..5),
   sealRecords                        SET SIZE(noOfSealRecords) OF SealRecord
}
```

noOfSealRecords är antalet poster i sealRecords.

sealRecords är en mängd plomberingsposter.

2.129. **SealDataVu**

Generation 2:

Denna datatyp lagrar information om de plomberingar som anbringats på de olika komponenterna i ett fordon och är avsedd för lagring i en fordonsenhet.

```
SealDataVu ::= SEQUENCE SIZE(5) OF {
   sealRecords                          SealRecord
}
```

sealRecords är en mängd plomberingsposter. Om det finns färre än 5 plomberingar tillgängliga ska värdet av EquipmentType i alla ej använda sealRecords sättas till 16, dvs. ”ej använd”.

2.130. **SealRecord**

Generation 2:

Denna datatyp lagrar information om en plombering som anbringats på en komponent. Denna datatyp berörs av krav 337 i bilaga 1C.

```
SealRecord ::= SEQUENCE {
   equipmentType                        EquipmentType,
   extendedSealIdentifier               ExtendedSealIdentifier
}
```

equipmentType anger typ av utrustning som plomberingen anbringats på.

extendedSealIdentifier är identifieraren för den plombering som anbringats på utrustningen.

▼B

2.131. **SensorApprovalNumber**

Sensorns typgodkännandenummer.

Generation 1:

```
SensorApprovalNumber ::= IA5String(SIZE(8))
```

Värdetilldelning: Ospecificerad.

Generation 2:

```
SensorApprovalNumber ::= IA5String(SIZE(16))
```

Värdetilldelning:

Godkännandenumret ska återges så som det är offentliggjort på Europeiska kommissionens motsvarande webbplats, t.ex. inklusive eventuella bindestreck. Godkännandenumret ska vara vänsterjusterat.

2.132. **SensorExternalGNSSApprovalNumber**

Generation 2:

Den externa GNSS-anordningens typgodkännandenummer.

```
SensorExternalGNSSApprovalNumber ::= IA5String(SIZE(16))
```

Värdetilldelning:

Godkännandenumret ska återges så som det är offentliggjort på Europeiska kommissionens motsvarande webbplats, t.ex. inklusive eventuella bindestreck. Godkännandenumret ska vara vänsterjusterat.

2.133. **SensorExternalGNSSCoupledRecord**

Generation 2:

Information lagrad i en fordonsenhet om identifiering av den externa GNSS-anordning som är kopplad med fordonsenheten (krav 100 i bilaga 1C).

```
SensorExternalGNSSCoupledRecord ::= SEQUENCE {
   sensorSerialNumber                  SensorGNSSSerialNumber,
   sensorApprovalNumber                SensorExternalGNSSApprovalNumber,
   sensorCouplingDate                  SensorGNSSCouplingDate
}
```

sensorSerialNumber är serienumret för den externa GNSS-anordning som är kopplad med fordonsenheten.

sensorApprovalNumber är denna externa GNSS-anordnings godkännandenummer.

sensorCouplingDate är ett datum för koppling av denna externa GNSS-anordning med fordonsenheten.

2.134. **SensorExternalGNSSIdentification**

Generation 2:

Information om identifiering av den externa GNSS-anordningen (krav 98 i bilaga 1C).

▼B

```
SensorExternalGNSSIdentification ::= SEQUENCE {
   sensorSerialNumber                    SensorGNSSSerialNumber,
   sensorApprovalNumber                  SensorExternalGNSSApprovalNumber,
   sensorSCIdentifier                    SensorExternalGNSSSCIdentifier,
   sensorOSIdentifier                    SensorExternalGNSSOSIdentifier
}
```

sensorSerialNumber är den externa GNSS-anordningens utökade serienummer.

sensorApprovalNumber är den externa GNSS-anordningens godkännandenummer.

sensorSCIdentifier är identifierare för den externa GNSS-anordningens säkerhetskomponent.

sensorOSIdentifier är identifierare för den externa GNSS-anordningens operativsystem.

2.135. **SensorExternalGNSSInstallation**

Generation 2:

Information, lagrad i en extern GNSS-anordning, om installation av den externa GNSS-sensorn (krav 123 i bilaga 1C).

```
SensorExternalGNSSInstallation ::= SEQUENCE {
   sensorCouplingDateFirst               SensorGNSSCouplingDate,
   firstVuApprovalNumber                 VuApprovalNumber,
   firstVuSerialNumber                   VuSerialNumber,
   sensorCouplingDateCurrent             SensorGNSSCouplingDate,
   currentVuApprovalNumber               VuApprovalNumber,
   currentVUSerialNumber                 VuSerialNumber
}
```

sensorCouplingDateFirst är datum för den första kopplingen av den externa GNSS-anordningen med en fordonsenhet.

firstVuApprovalNumber är godkännandenummer för den första fordonsenhet som kopplas med den externa GNSS-anordningen.

firstVuSerialNumber är serienumret för den första fordonsenhet som kopplas med den externa GNSS-anordningen.

sensorCouplingDateCurrent är datum för innevarande koppling av den externa GNSS-anordningen med en fordonsenhet.

currentVuApprovalNumber är godkännandenummer för den fordonsenhet som för närvarande är kopplad med den externa GNSS-anordningen.

currentVUSerialNumber är serienummer för den fordonsenhet som för närvarande är kopplad med den externa GNSS-anordningen.

▼B

2.136. **SensorExternalGNSSOSIdentifier**

Generation 2:

Identifierare för den externa GNSS-anordningens operativsystem.

```
SensorOSIdentifier ::= IA5String(SIZE(2))
```

Värdetilldelning: tillverkarspecifik.

2.137. **SensorExternalGNSSSCIdentifier**

Generation 2:

Denna typ används exempelvis för att identifiera den externa GNSS-anordningens krypteringsmodul.

Identifierare för den externa GNSS-anordningens säkerhetskomponent.

```
SensorExternalGNSSSCIdentifier ::= IA5String(SIZE(8))
```

Värdetilldelning: specifik för komponenttillverkaren.

2.138. **SensorGNSSCouplingDate**

Generation 2:

Datum för koppling av den externa GNSS-anordningen med en fordonsenhet.

```
SensorGNSSCouplingDate ::= TimeReal
```

Värdetilldelning: Ospecificerad.

2.139. **SensorGNSSSerialNumber**

Generation 2:

Denna typ används för att lagra GNSS-mottagarens serienummer både när den finns i fordonsenheten och när den finns utanför fordonsenheten.

GNSS-mottagarens serienummer.

```
SensorGNSSSerialNumber ::= ExtendedSerialNumber
```

2.140. **SensorIdentification**

Information lagrad i en rörelsesensor om identifiering av rörelsesensorn (krav 077 i bilaga 1B och krav 95 i bilaga 1C).

```
SensorIdentification ::= SEQUENCE {
   sensorSerialNumber                    SensorSerialNumber,
   sensorApprovalNumber                  SensorApprovalNumber,
   sensorSCIdentifier                    SensorSCIdentifier,
   sensorOSIdentifier                    SensorOSIdentifier
}
```

sensorSerialNumber är rörelsesensorns utökade serienummer (inbegripet artikelnummer och tillverkarens kod).

sensorApprovalNumber är rörelsesensorns godkännandenummer.

sensorSCIdentifier är identifierare för rörelsesensorns säkerhetskomponent.

▼B

sensorOSIdentifier är identifierare för rörelsesensorns operativsystem.

2.141. **SensorInstallation**

Information lagrad i en rörelsesensor om installation av rörelsesensorn (krav 099 i bilaga 1B och krav 122 i bilaga 1C).

```
SensorInstallation ::= SEQUENCE {
   sensorPairingDateFirst                SensorPairingDate,
   firstVuApprovalNumber                 VuApprovalNumber,
   firstVuSerialNumber                   VuSerialNumber,
   sensorPairingDateCurrent              SensorPairingDate,
   currentVuApprovalNumber               VuApprovalNumber,
   currentVUSerialNumber                 VuSerialNumber
}
```

sensorPairingDateFirst är datum för den första parningen av rörelsesensorn med en fordonsenhet.

firstVuApprovalNumber är godkännandenummer för den första fordonsenhet som paras med rörelsesensorn.

firstVuSerialNumber är serienummer för den första fordonsenhet som paras med rörelsesensorn.

sensorPairingDateCurrent är datum för innevarande parning av rörelsesensorn med fordonsenheten.

currentVuApprovalNumber är godkännandenummer för den fordonsenhet som för närvarande är parad med rörelsesensorn.

currentVUSerialNumber är serienummer för den fordonsenhet som för närvarande är parad med rörelsesensorn.

2.142. **SensorInstallationSecData**

Information lagrad i ett verkstadskort om de säkerhetsdata som behövs för att para rörelsesensorer med fordonsenheter (krav 308 och 331 i bilaga 1C).

Generation 1:

```
SensorInstallationSecData ::= TdesSessionKey
```

Värdetilldelning: enligt ISO 16844-3.

Generation 2:

Såsom beskrivs i tillägg 11 ska ett verkstadskort lagra upp till tre nycklar för parning av fordonsenhet och rörelsesensor. Dessa nycklar har olika nyckelversioner.

```
SensorInstallationSecData ::= SEQUENCE {
   kMWCKey1                              KMWCKey,
   kMWCKey2                              KMWCKey OPTIONAL,
   kMWCKey3                              KMWCKey OPTIONAL
}
```

▼B

2.143. **SensorOSIdentifier**

Identifierare för rörelsesensorns operativsystem.

```
SensorOSIdentifier ::= IA5String(SIZE(2))
```

Värdetilldelning: tillverkarspecifik.

2.144. **SensorPaired**

Generation 1:

Information lagrad i en fordonsenhet om identifiering av den rörelsesensor som är parad med fordonsenheten (krav 079 i bilaga 1B).

```
SensorPaired ::= SEQUENCE {
   sensorSerialNumber                    SensorSerialNumber,
   sensorApprovalNumber                  SensorApprovalNumber,
   sensorPairingDateFirst                SensorPairingDate
}
```

sensorSerialNumber är serienummer för den rörelsesensor som för närvarande är parad med fordonsenheten.

sensorApprovalNumber är godkännandenummer för den rörelsesensor som för närvarande är parad med fordonsenheten.

sensorPairingDateFirst är datum för den första parningen med en fordonsenhet för den rörelsesensor som för närvarande är parad med fordonsenheten.

2.145. **SensorPairedRecord**

Generation 2:

Information lagrad i en fordonsenhet om identifiering av en rörelsesensor som är parad med fordonsenheten (krav 97 i bilaga 1C).

```
SensorPairedRecord ::= SEQUENCE {
   sensorSerialNumber                    SensorSerialNumber,
   sensorApprovalNumber                  SensorApprovalNumber,
   sensorPairingDate                     SensorPairingDate
}
```

sensorSerialNumber är serienummer för den rörelsesensor som är parad med fordonsenheten.

sensorApprovalNumber är rörelsesensorns godkännandenummer.

sensorPairingDate är ett datum för parning av denna rörelsesensor med fordonsenheten.

2.146. **SensorPairingDate**

Datum för parning av rörelsesensorn med en fordonsenhet.

```
SensorPairingDate ::= TimeReal
```

Värdetilldelning: Ospecificerad.

▼B

2.147. **SensorSCIdentifier**

Identifierare för rörelsesensorns säkerhetskomponent.

```
SensorSCIdentifier ::= IA5String(SIZE(8))
```

Värdetilldelning: specifik för komponenttillverkaren.

2.148. **SensorSerialNumber**

Rörelsesensorns serienummer.

```
SensorSerialNumber ::= ExtendedSerialNumber
```

2.149. **Signature**

En digital signatur.

Generation 1:

```
Signature ::= OCTET STRING (SIZE(128))
```

Värdetilldelning: enligt tillägg 11 om gemensamma säkerhetsmekanismer.

Generation 2:

```
Signature ::= OCTET STRING (SIZE(64..132))
```

Värdetilldelning: enligt tillägg 11 om gemensamma säkerhetsmekanismer.

2.150. **SignatureRecordArray**

Generation 2:

En mängd signaturer samt metadata som används i överföringsprotokollet.

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

recordType anger typen av post (Signature). **Värdetilldelning:** Se RecordType.

recordSize är storleken av Signature i byte.

noOfRecords är antalet poster i postmängden. Värdet ska sättas till 1 eftersom signaturerna kan ha olika längd.

records är mängden av signaturer.

2.151. **SimilarEventsNumber**

Antal liknande händelser under en viss dag (krav 094 i bilaga 1B och krav 117 i bilaga 1C).

```
SimilarEventsNumber ::= INTEGER(0..255)
```

Värdetilldelning: 0 används inte, 1 innebär att endast en händelse av denna typ har ägt rum och har lagrats den dagen, 2 innebär att två händelser av denna typ har ägt rum den dagen (endast en har lagrats), … 255 innebär att 255 eller fler händelser av denna typ har ägt rum den dagen.

▼B

2.152. **SpecificConditionRecord**

Information lagrad i ett förarkort, på ett verkstadskort eller i en fordonsenhet om en särskild omständighet (krav 130, 276, 301, 328 och 355 i bilaga 1C).

```
SpecificConditionRecord ::= SEQUENCE {
   entryTime                          TimeReal,
   specificConditionType              SpecificConditionType
}
```

entryTime är datum och tidpunkt för angivelsen.

specificConditionType är koden för identifiering av den särskilda omständigheten.

2.153. **SpecificConditions**

Information lagrad i ett förarkort, på ett verkstadskort eller i en fordonsenhet om en särskild omständighet (krav 131, 277, 302, 329 och 356 i bilaga 1C).

Generation 2:

```
SpecificConditions := SEQUENCE {
   conditionPointerNewestRecord         INTEGER(0..NoOfSpecificConditionRecords-1),
   specificConditionRecords             SET SIZE(NoOfSpecificConditionRecords) OF
                                        SpecificConditionRecord
}
```

controlPointerNewestRecord är index för senast uppdaterad post för särskild omständighet.

Värdetilldelning: Ett tal som motsvarar numeratorn för posten för särskild omständighet, och som börjar med ′0′ för den första gången posten för särskild omständighet uppträder i strukturen.

specificConditionRecords är den mängd poster som innehåller information om de särskilda omständigheter som registrerats.

2.154. **SpecificConditionType**

Kod för identifiering av särskild omständighet (krav 050b, 105a, 212a och 230a i bilaga 1B samt krav 62 i bilaga 1C).

```
SpecificConditionType ::= INTEGER(0..255)
```

Generation 1:

Värdetilldelning:

‘00’H	RFU
‘01’H	Omfattas ej – Början.
‘02’H	Omfattas ej – Slut.
‘03’H	Transport med färja/tåg
‘04’H .. ‘FF’H	RFU

Generation 2:

Värdetilldelning:

‘00’H	RFU
‘01’H	Omfattas ej – Början.
‘02’H	Omfattas ej – Slut.
‘03’H	Transport med färja/tåg – Början
‘04’H	Transport med färja/tåg – Slut
‘05’H .. ‘FF’H	RFU

▼B

2.155. **Hastighet**

Fordonets hastighet (km/h).

```
Speed ::= INTEGER(0..255)
```

Värdetilldelning: kilometer per timme i intervallet från 0 till 220 km/h.

2.156. **SpeedAuthorised**

Högsta tillåtna hastighet för fordonet (definition hh)).

```
SpeedAuthorised ::= Speed
```

2.157. **SpeedAverage**

Genomsnittlig hastighet under en tidigare fastställd tidsperiod (km/h).

```
SpeedAverage ::= Speed
```

2.158. **SpeedMax**

Högsta hastighet uppmätt under en tidigare fastställd tidsperiod.

```
SpeedMax ::= Speed
```

2.159. **TachographPayload**

Generation 2:

Se tillägg 14 för en definition av denna datatyp.

2.160. **TachographPayloadEncrypted**

Generation 2:

DER-TLV-krypterad nyttolast från färdskrivaren, dvs. de data som skickas krypterade i RTM-meddelandet. Information om krypteringen finns i tillägg 11 del B kapitel 13.

```
TachographPayloadEncrypted ::= SEQUENCE {
   tag                                  OCTET STRING(SIZE(1)),
   length                               OCTET STRING(SIZE(1..2)),
   paddingContentIndicatorByte          OCTET STRING(SIZE(1)),
   encryptedData                        OCTET STRING(SIZE(16..192))
}
```

tag utgör en del av DER-TLV-kodningen och ska sättas till ‘87’ (se tillägg 11 del B kapitel 13).

length utgör en del av DER-TLV-kodningen och ska koda längden av följande paddingContentIndicatorByte och encryptedData.

paddingContentIndicatorByte ska sättas till ‘00’.

encryptedData är krypterad tachographPayload i enlighet med tillägg 11 del B kapitel 13. Längden av dessa data i oktetter ska alltid vara en multipel av 16.

2.161. **TDesSessionKey**

Generation 1:

En sessionsnyckel för Triple DES.

```
TDesSessionKey ::= SEQUENCE {
   tDesKeyA                             OCTET STRING (SIZE(8)),
   tDesKeyB                             OCTET STRING (SIZE(8))
}
```

Värdetilldelning: Ej närmare angiven.

▼B

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 GMT.

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

Värdetilldelning – oktettgrupperad: Antal sekunder sedan midnatt den 1 januari 1970 GMT.

Senaste möjliga datum/tidpunkt är under år 2106.

2.163. **TyreSize**

Angivelse av däckens dimensioner.

```
TyreSize ::= IA5String(SIZE(15))
```

Värdetilldelning: i enlighet med direktiv 92/23 (EEG), 31.3.1992, EGT L129, s. 95.

2.164. **VehicleIdentificationNumber**

Fordonets identifieringsnummer (VIN) avseende fordonet som helhet, vanligtvis ramnummer eller serienummer på chassit.

```
VehicleIdentificationNumber ::= IA5String(SIZE(17))
```

Värdetilldelning: Enligt definition i ISO 3779.

2.165. **VehicleIdentificationNumberRecordArray**

Generation 2:

Fordonets identifieringsnummer (VIN) samt metadata som används i överföringsprotokollet.

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

recordType anger typen av post (VehicleIdentificationNumber). **Värdetilldelning:** Se RecordType.

recordSize är storleken av VehicleIdentificationNumber i byte.

noOfRecords är antalet poster i postmängden.

records är mängden identifieringsnummer för fordon.

2.166. **VehicleRegistrationIdentification**

Identifiering av ett fordon, som är unik för Europa (fordonets registreringsnummer (VRN) och medlemsstat).

```
VehicleRegistrationIdentification ::= SEQUENCE {
   vehicleRegistrationNation           NationNumeric,
   vehicleRegistrationNumber           VehicleRegistrationNumber
}
```

vehicleRegistrationNation är det land där fordonet är registrerat.

▼B

vehicleRegistrationNumber är fordonets registreringsnummer (VRN).

2.167. **VehicleRegistrationNumber**

Fordonets registreringsnummer (VRN). Registreringsnumret tilldelas av myndigheten för fordonsregistrering.

```
VehicleRegistrationNumber ::= SEQUENCE {
   codePage                          INTEGER (0..255),
   vehicleRegNumber                  OCTET STRING (SIZE(13))
}
```

codePage specificerar en teckenmängd som definieras i kapitel 4.

vehicleRegNumber är ett registreringsnummer för ett fordon som kodats enligt den specificerade teckenmängden.

Värdetilldelning: Landsspecifik.

2.168. **VehicleRegistrationNumberRecordArray**

Generation 2:

Fordonets registreringsnummer (VRN) samt metadata som används i överföringsprotokollet.

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

recordType anger typen av post (VehicleRegistrationNumber). **Värdetilldelning:** Se RecordType.

recordSize är storleken av VehicleRegistrationNumber i byte.

noOfRecords är antalet poster i postmängden.

records är mängden registreringsnummer för fordon.

2.169. **VuAbility**

Generation 2:

Information lagrad i en fordonsenhet om förmågan hos fordonsenheten att använda färdskrivarkort i generation 1 eller inte (krav 121 i bilaga 1C).

```
VuAbility ::= OCTET STRING (SIZE(1))
```

Värdetilldelning – oktettgrupperad: ‘xxxxxxxa’B (8 bitar)

Om förmågan att stödja generation 1:

‘a’B	Förmåga att stödja färdskrivarkort i generation 1:
	‘0’ B Generation 1 stöds.
	‘1’B Generation 1 stöds inte.
‘xxxxxxx’B	RFU

▼B

2.170. **VuActivityDailyData**

Generation 1:

Information lagrad i en fordonsenhet om ändringar av aktivitet och/eller ändringar av körningsstatus och/eller ändringar av kortstatus under en viss kalenderdag (krav 084 i bilaga 1B och krav 105, 106, 107 i bilaga 1C) och om öppningsstatusen kl. 00.00 den berörda dagen.

```
VuActivityDailyData ::= SEQUENCE {
   noOfActivityChanges                  INTEGER SIZE(0..1440),
   activityChangeInfos                  SET SIZE(noOfActivityChanges) OF
                                        ActivityChangeInfo
}
```

noOfActivityChanges är antalet ActivityChangeInfo-ord i mängden activityChangeInfos.

activityChangeInfos är mängden ActivityChangeInfo-ord som lagrats i fordonsenheten under dagen. Den omfattar alltid två ActivityChangeInfo-ord som anger statusen för de två kortplatserna kl. 00.00 den berörda dagen.

2.171. **VuActivityDailyRecordArray**

Generation 2:

Information lagrad i en fordonsenhet om ändringar av aktivitet och/eller ändringar av körningsstatus och/eller ändringar av kortstatus under en viss kalenderdag (krav 105, 106, 107 i bilaga 1C) och om öppningsstatusen kl. 00.00 den berörda dagen.

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

recordType anger typen av post (ActivityChangeInfo). **Värdetilldelning:** Se RecordType.

recordSize är storleken av ActivityChangeInfo i byte.

noOfRecords är antalet poster i postmängden.

records är mängden ActivityChangeInfo-ord som lagrats i fordonsenheten under dagen. Den omfattar alltid två ActivityChangeInfo-ord som anger statusen för de två kortplatserna kl. 00.00 den berörda dagen.

2.172. **VuApprovalNumber**

Fordonsenhetens typgodkännandenummer.

Generation 1:

```
VuApprovalNumber ::= IA5String(SIZE(8))
```

Värdetilldelning: Ospecificerad.

Generation 2:

```
VuApprovalNumber ::= IA5String(SIZE(16))
```

▼B

Värdetilldelning:

Godkännandenumret ska återges så som det är offentliggjort på Europeiska kommissionens motsvarande webbplats, t.ex. inklusive eventuella bindestreck. Godkännandenumret ska vara vänsterjusterat.

2.173. **VuCalibrationData**

Generation 1:

Information lagrad i en fordonsenhet om kalibreringar av färdskrivaren (krav 098 i bilaga 1B).

```
VuCalibrationData ::= SEQUENCE {
   noOfVuCalibrationRecords              INTEGER(0..255),
   vuCalibrationRecords                  SET SIZE(noOfVuCalibrationRecords) OF
                                         VuCalibrationRecord
}
```

noOfVuCalibrationRecords är det antal poster som mängden vuCalibrationRecords innehåller.

vuCalibrationRecords är mängden kalibreringsposter.

2.174. **VuCalibrationRecord**

Information lagrad i en fordonsenhet om en kalibrering av färdskrivaren (krav 098 i bilaga 1B och krav 119 och 120 i bilaga 1C).

Generation 1:

```
VuCalibrationRecord ::= SEQUENCE {
   calibrationPurpose                    CalibrationPurpose,
   workshopName                          Name,
   workshopAddress                       Address,
   workshopCardNumber                    FullCardNumber,
   workshopCardExpiryDate                TimeReal,
   vehicleIdentificationNumber           VehicleIdentificationNumber,
   vehicleRegistrationIdentification     VehicleRegistrationIdentification,
   wVehicleCharacteristicConstant        W-VehicleCharacteristicConstant,
   kConstantOfRecordingEquipment         K-ConstantOfRecordingEquipment,
   lTyreCircumference                    L-TyreCircumference,
   tyreSize                              TyreSize,
   authorisedSpeed                       SpeedAuthorised,
   oldOdometerValue                      OdometerShort,
   newOdometerValue                      OdometerShort,
   oldTimeValue                          TimeReal,
   newTimeValue                          TimeReal,
   nextCalibrationDate                   TimeReal
}
```

calibrationPurpose är syftet med kalibreringen.

workshopName, workshopAddress är verkstadens namn och adress.

workshopCardNumber identifierar det verkstadskort som använts vid kalibreringen.

workshopCardExpiryDate är kortets sista giltighetsdatum.

vehicleIdentificationNumber är fordonets identifieringsnummer (VIN).

▼B

vehicleRegistrationIdentification innehåller fordonets registreringsnummer (VRN) och registrerande medlemsstat.

wVehicleCharacteristicConstant är fordonets karakteristiska koefficient.

kConstantOfRecordingEquipment är färdskrivarens konstant.

lTyreCircumference är däckens effektiva omkrets.

tyreSize är angivelse av dimensionen på de däck som monterats på fordonet.

authorisedSpeed är den tillåtna hastigheten för fordonet.

oldOdometerValue, newOdometerValue är de gamla och nya vägmätarställningarna.

oldTimeValue, newTimeValue är de gamla och nya värdena för datum och tidpunkt.

nextCalibrationDate är datum för nästa kalibrering av den typ som anges i CalibrationPurpose och som ska utföras av den auktoriserade besiktningsmyndigheten.

Generation 2:

```
VuCalibrationRecord ::= SEQUENCE {
   calibrationPurpose                    CalibrationPurpose,
   workshopName                          Name,
   workshopAddress                       Address,
   workshopCardNumber                    FullCardNumber,
   workshopCardExpiryDate                TimeReal,
   vehicleIdentificationNumber           VehicleIdentificationNumber,
   vehicleRegistrationIdentification     VehicleRegistrationIdentification,
   wVehicleCharacteristicConstant        W-VehicleCharacteristicConstant,
   kConstantOfRecordingEquipment         K-ConstantOfRecordingEquipment,
   lTyreCircumference                    L-TyreCircumference,
   tyreSize                              TyreSize,
   authorisedSpeed                       SpeedAuthorised,
   oldOdometerValue                      OdometerShort,
   newOdometerValue                      OdometerShort,
   oldTimeValue                          TimeReal,
   newTimeValue                          TimeReal,
   nextCalibrationDate                   TimeReal,
   sealDataVu                            SealDataVu
}
```

Jämfört med generation 1 används följande ytterligare dataelement:

sealDataVu ger information om de plomberingar som anbringats på olika komponenter i fordonet.

2.175. **VuCalibrationRecordArray**

Generation 2:

Information lagrad i en fordonsenhet om kalibreringar av färdskrivaren (krav 119 och 120 i bilaga 1C).

▼B

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

recordType anger typen av post (VuCalibrationRecord). **Värdetilldelning:** Se RecordType.

recordSize är storleken av VuCalibrationRecord i byte.

noOfRecords är antalet poster i postmängden.

records är mängden av kalibreringsposter.

2.176. **VuCardIWData**

Generation 1:

Information lagrad i en fordonsenhet om cykler med insättning och uttag av förarkort eller verkstadskort i fordonsenheten (krav 081 i bilaga 1B och krav 103 i bilaga 1C).

```
VuCardIWData ::= SEQUENCE {
   noOfIWRecords                        INTEGER(0..2^16-1),
   vuCardIWRecords                      SET SIZE(noOfIWRecords) OF VuCardIWRecord
}
```

noOfIWRecords är antalet poster i mängden vuCardIWRecords.

vuCardIWRecords är en mängd poster för cykler med insättning/uttag av kort.

2.177. **VuCardIWRecord**

Information lagrad i en fordonsenhet om en cykel med insättning och uttag av ett förarkort eller ett verkstadskort i fordonsenheten (krav 081 i bilaga 1B och krav 102 i bilaga 1C).

Generation 1:

```
VuCardIWRecord ::= SEQUENCE {
   cardHolderName                       HolderName,
   fullCardNumber                       FullCardNumber,
   cardExpiryDate                       TimeReal,
   cardInsertionTime                    TimeReal,
   vehicleOdometerValueAtInsertion      OdometerShort,
   cardSlotNumber                       CardSlotNumber,
   cardWithdrawalTime                   TimeReal,
   vehicleOdometerValueAtWithdrawal     OdometerShort,
   previousVehicleInfo                  PreviousVehicleInfo,
   manualInputFlag                      ManualInputFlag
}
```

cardHolderName är förar- eller verkstadskortinnehavarens efternamn och förnamn sådana de lagrats på kortet.

fullCardNumber är typ av kort, dess utfärdande medlemsstat och dess kortnummer sådana de lagrats på kortet.

▼B

cardExpiryDate är kortets sista giltighetsdatum sådant det lagrats på kortet.

cardInsertionTime är datum och tidpunkt för insättning.

vehicleOdometerValueAtInsertion är vägmätarställning när kortet sätts in.

cardSlotNumber är den kortplats som kortet sätts in i.

cardWithdrawalTime är tidpunkt och datum för uttag.

vehicleOdometerValueAtWithdrawal är fordonets vägmätarställning när kortet togs ut.

previousVehicleInfo innehåller information om det föregående fordon som föraren använt, sådan den lagrats på kortet.

manualInputFlag är en markering som identifierar om kortinnehavaren manuellt har angett föraraktiviteter vid kortinsättning.

Generation 2:

```
VuCardIWRecord ::= SEQUENCE {
   cardHolderName                          HolderName,
   fullCardNumberAndGeneration             FullCardNumberAndGeneration,
   cardExpiryDate                          TimeReal,
   cardInsertionTime                       TimeReal,
   vehicleOdometerValueAtInsertion         OdometerShort,
   cardSlotNumber                          CardSlotNumber,
   cardWithdrawalTime                      TimeReal,
   vehicleOdometerValueAtWithdrawal        OdometerShort,
   previousVehicleInfo                     PreviousVehicleInfo,
   manualInputFlag                         ManualInputFlag
}
```

I stället för fullCardNumber använder datastrukturen för generation 2 följande dataelement:

fullCardNumberAndGeneration är typ av kort, dess utfärdande medlemsstat, dess kortnummer och dess generation sådana de lagrats på kortet.

2.178. **VuCardIWRecordArray**

Generation 2:

Information lagrad i en fordonsenhet om cykler med insättning och uttag av förarkort eller verkstadskort i fordonsenheten (krav 103 i bilaga 1C).

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

recordType anger typen av post (VuCardIWRecord). **Värdetilldelning:** Se RecordType.

recordSize är storleken av VuCardIWRecord i byte.

▼B

noOfRecords är antalet poster i postmängden.

records är en mängd poster för cykler med insättning/uttag av kort.

2.179. **VuCardRecord**

Generation 2:

Information lagrad i en fordonsenhet om ett färdskrivarkort som används (krav 132 i bilaga 1C).

```
VuCardRecord ::= SEQUENCE {
   cardExtendedSerialNumber            ExtendedSerialNumber,
   cardPersonaliserID                  OCTET STRING(SIZE(1)),
   typeofTachographCardID              EquipmentType,
   cardStructureVersion                CardStructureVersion,
   cardNumber                          CardNumber
}
```

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

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

typeOfTachographCardId såsom det läses från filen EF_Application_Identification under DF_Tachograph_G2.

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.

2.180. **VuCardRecordArray**

Generation 2:

Information lagrad i en fordonsenhet om de färdskrivarkort som används med denna fordonsenhet. Denna information är avsedd för analys av problem som rör fordonsenhet–kort (krav 132 i bilaga 1C).

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

recordType anger typen av post (VuCardRecord). **Värdetilldelning:** Se RecordType.

recordSize är storleken av VuCardRecord i byte.

noOfRecords är antalet poster i postmängden.

records är en mängd poster som avser de färdskrivarkort som används med fordonsenheten.

▼B

2.181. **VuCertificate**

Certifikat för en fordonsenhets öppna nyckel.

```
VuCertificate ::= Certificate
```

2.182. **VuCertificateRecordArray**

Generation 2:

Fordonsenhetens certifikat samt metadata som används i överföringsprotokollet.

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

recordType anger typen av post (VuCertificate). **Värdetilldelning:** Se RecordType.

recordSize är storleken av VuCertificate i byte.

noOfRecords är antalet poster i postmängden. Värdet ska sättas till 1 eftersom certifikaten kan ha olika längd.

records är en mängd certifikat för fordonsenheter.

2.183. **VuCompanyLocksData**

Generation 1:

Information lagrad i en fordonsenhet om företagslås (krav 104 i bilaga 1B).

```
VuCompanyLocksData ::= SEQUENCE {
   noOfLocks                           INTEGER(0..255),
   vuCompanyLocksRecords               SET SIZE(noOfLocks) OF VuCompanyLocksRecord
}
```

noOfLocks är antalet lås som finns förtecknade i vuCompanyLocksRecords.

vuCompanyLocksRecords är mängden poster för företagslås.

2.184. **VuCompanyLocksRecord**

Information lagrad i en fordonsenhet om ett företagslås (krav 104 i bilaga 1B och krav 128 i bilaga 1C).

Generation 1:

```
VuCompanyLocksRecord ::= SEQUENCE {
   lockInTime                          TimeReal,
   lockOutTime                         TimeReal,
   companyName                         Name,
   companyAddress                      Address,
   companyCardNumber                   FullCardNumber
}
```

▼B

lockInTime, lockOutTime är datum och tidpunkt för låsning och öppning.

companyName, companyAddress är det företagsnamn och den företagsadress som förknippas med låsningen.

companyCardNumber identifierar det kort som används vid låsningen.

Generation 2:

```
VuCompanyLocksRecord ::= SEQUENCE {
   lockInTime                          TimeReal,
   lockOutTime                         TimeReal,
   companyName                         Name,
   companyAddress                      Address,
   companyCardNumberAndGeneration      FullCardNumberAndGeneration
}
```

I stället för companyCardNumber använder datastrukturen för generation 2 följande dataelement:

companyCardNumberAndGeneration identifierar det kort, inbegripet dess generation, som används vid låsningen.

2.185. **VuCompanyLocksRecordArray**

Generation 2:

Information lagrad i en fordonsenhet om företagslås (krav 128 i bilaga 1C).

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

recordType anger typen av post (VuCompanyLocksRecord). **Värdetilldelning:** Se RecordType.

recordSize är storleken av VuCompanyLocksRecord i byte.

noOfRecords är antalet poster i postmängden. Värde 0..255.

records är mängden poster för företagslås.

2.186. **VuControlActivityData**

Generation 1:

Information lagrad i en fordonsenhet om kontroller som utförs med användning av denna fordonsenhet (krav 102 i bilaga 1B).

```
VuControlActivityData ::= SEQUENCE {
   noOfControls                        INTEGER(0..20),
   vuControlActivityRecords            SET SIZE(noOfControls) OF
                                       VuControlActivityRecord
}
```

▼B

noOfControls är antalet kontroller som finns förtecknade i vuControlActivityRecords.

vuControlActivityRecords är mängden poster för kontrollaktiviteter.

2.187. **VuControlActivityRecord**

Information lagrad i en fordonsenhet om en kontroll som utförs med användning av denna fordonsenhet (krav 102 i bilaga 1B och krav 126 i bilaga 1C).

Generation 1:

```
VuControlActivityRecord ::= SEQUENCE {
   controlType                          ControlType,
   controlTime                          TimeReal,
   controlCardNumber                    FullCardNumber,
   downloadPeriodBeginTime              TimeReal,
   downloadPeriodEndTime                TimeReal
}
```

controlType är typ av kontroll.

controlTime är datum och tidpunkt för kontrollen.

ControlCardNumber identifierar det kontrollkort som använts vid kontrollen.

downloadPeriodBeginTime är den överförda periodens början, om överföring utfördes.

downloadPeriodEndTime är den överförda periodens slut, om överföring utfördes.

Generation 2:

```
VuControlActivityRecord ::= SEQUENCE {
   controlType                          ControlType,
   controlTime                          TimeReal,
   controlCardNumberAndGeneration       FullCardNumberAndGeneration,
   downloadPeriodBeginTime              TimeReal,
   downloadPeriodEndTime                TimeReal
}
```

I stället för controlCardNumber använder datastrukturen för generation 2 följande dataelement:

controlCardNumberAndGeneration identifierar det kontrollkort, inbegripet dess generation, som använts vid kontrollen.

2.188. **VuControlActivityRecordArray**

Generation 2:

Information lagrad i en fordonsenhet om kontroller som utförs med användning av denna fordonsenhet (krav 126 i bilaga 1C).

▼B

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

recordType anger typen av post (VuControlActivityRecord). **Värdetilldelning:** Se RecordType.

recordSize är storleken av VuControlActivityRecord i byte.

noOfRecords är antalet poster i postmängden.

records är mängden poster för kontrollaktiviteter avseende fordonsenheten.

2.189. **VuDataBlockCounter**

Räknare lagrad i ett kort och som sekventiellt identifierar cyklerna med insättning och uttagning av kort i fordonsenheter.

```
VuDataBlockCounter ::= BCDString(SIZE(2))
```

Värdetilldelning: Löpnummer med högsta värde 9 999, varpå det börjar om från 0.

2.190. **VuDetailedSpeedBlock**

Detaljerad information, lagrad i en fordonsenhet, om fordonets hastighet under en minut under vilken fordonet har varit i rörelse (krav 093 i bilaga 1B och krav 116 i bilaga 1C).

```
VuDetailedSpeedBlock ::= SEQUENCE {
   speedBlockBeginDate    TimeReal,
   speedsPerSecond        SEQUENCE SIZE(60) OF Speed
}
```

speedBlockBeginDate är datum och tidpunkt för det första hastighetsvärdet inom blocket.

speedsPerSecond är den kronologiska sekvensen av uppmätta hastigheter varje sekund under den minut som sträcker sig fr.o.m. speedBlockBeginDate.

2.191. **VuDetailedSpeedBlockRecordArray**

Generation 2:

Detaljerad information, lagrad i en fordonsenhet, om fordonets hastighet.

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

recordType anger typen av post (VuDetailedSpeedBlock). **Värdetilldelning:** Se RecordType.

▼B

recordSize är storleken av VuDetailedSpeedBlock i byte.

noOfRecords är antalet poster i postmängden.

records är mängden block med detaljerade hastighetsdata.

2.192. **VuDetailedSpeedData**

Generation 1:

Detaljerad information, lagrad i en fordonsenhet, om fordonets hastighet.

```
VuDetailedSpeedData ::= SEQUENCE {
   noOfSpeedBlocks                    INTEGER(0..2^16-1),
   vuDetailedSpeedBlocks              SET SIZE(noOfSpeedBlocks) OF
                                      VuDetailedSpeedBlock
}
```

noOfSpeedBlocks är antalet hastighetsblock i mängden vuDetailedSpeedBlocks.

vuDetailedSpeedBlocks är mängden block med detaljerade hastighetsdata.

2.193. **VuDownloadablePeriod**

Äldsta och senaste datum för vilka en fordonsenhet har data om förar-aktiviteter (krav 081, 084 eller 087 i bilaga 1B och krav 102, 105, 108 i bilaga 1C).

```
VuDownloadablePeriod ::= SEQUENCE {
   minDownloadableTime                TimeReal
   maxDownloadableTime                TimeReal
}
```

minDownloadableTime är äldsta datum och tidpunkt för kortinsättning, aktivitetsändring eller angivelse av plats som finns lagrat i fordonsenheten.

maxDownloadableTime är senaste datum och tidpunkt för kortuttag, aktivitetsändring eller angivelse av plats som finns lagrat i fordonsenheten.

2.194. **VuDownloadablePeriodRecordArray**

Generation 2:

VUDownloadablePeriod samt metadata som används i överföringsprotokollet.

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

recordType anger typen av post (VuDownloadablePeriod). **Värdetilldelning:** Se RecordType.

▼B

recordSize är storleken av VuDownloadablePeriod i byte.

noOfRecords är antalet poster i postmängden.

records är mängden av VuDownloadablePeriod-poster.

2.195. **VuDownloadActivityData**

Information lagrad i en fordonsenhet om den senaste överföringen från fordonsenheten (krav 105 i bilaga 1B och krav 129 i bilaga 1C).

Generation 1:

```
VuDownloadActivityData ::= SEQUENCE {
   downloadingTime                        TimeReal,
   fullCardNumber                         FullCardNumber,
   companyOrWorkshopName                  Name
}
```

downloadingTime är datum och tidpunkt för en överföring.

fullCardNumber identifierar det kort som används för att auktorisera överföringen.

companyOrWorkshopName är företagets eller verkstadens namn.

Generation 2:

```
VuDownloadActivityData ::= SEQUENCE {
   downloadingTime                        TimeReal,
   fullCardNumberAndGeneration            FullCardNumberAndGeneration,
   companyOrWorkshopName                  Name
}
```

I stället för fullCardNumber använder datastrukturen för generation 2 följande dataelement:

fullCardNumberAndGeneration identifierar det kort, inbegripet dess generation, som används för att auktorisera överföringen.

2.196. **VuDownloadActivityDataRecordArray**

Generation 2:

Information om den senaste överföringen från fordonsenhet (krav 129 i bilaga 1C).

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

recordType anger typen av post (VuDownloadActivityData). **Värdetilldelning:** Se RecordType.

recordSize är storleken av VuDownloadActivityData i byte.

noOfRecords är antalet poster i postmängden.

▼B

records är mängden poster med data om överföringsaktivitet.

2.197. **VuEventData**

Generation 1:

Information lagrad i en fordonsenhet om händelser (krav 094 i bilaga 1B, utom händelse av typen hastighetsöverträdelse).

```
VuEventData ::= SEQUENCE {
   noOfVuEvents                          INTEGER(0..255),
   vuEventRecords                        SET SIZE(noOfVuEvents) OF VuEventRecord
}
```

noOfVuEvents är antalet händelser som finns förtecknade i mängden vuEventRecords.

vuEventRecords är en mängd poster för händelser.

2.198. **VuEventRecord**

Information lagrad i en fordonsenhet om en händelse (krav 094 i bilaga 1B och krav 117 i bilaga 1C, utom händelse av typen hastighetsöverträdelse).

Generation 1:

```
VuEventRecord ::= SEQUENCE {
   eventType                             EventFaultType,
   eventRecordPurpose                    EventFaultRecordPurpose,
   eventBeginTime                        TimeReal,
   eventEndTime                          TimeReal,
   cardNumberDriverSlotBegin             FullCardNumber,
   cardNumberCodriverSlotBegin           FullCardNumber,
   cardNumberDriverSlotEnd               FullCardNumber,
   cardNumberCodriverSlotEnd             FullCardNumber,
   similarEventsNumber                   SimilarEventsNumber
}
```

eventType är typ av händelse.

eventRecordPurpose är syftet med registreringen av denna händelse.

eventBeginTime är datum och tidpunkt för händelsens början.

eventEndTime är datum och tidpunkt för händelsens slut.

cardNumberDriverSlotBegin identifierar det kort som är insatt i förarens kortplats vid händelsens början.

cardNumberCodriverSlotBegin identifierar det kort som är insatt i medförarens kortplats vid händelsens början.

cardNumberDriverSlotEnd identifierar det kort som är insatt i förarens kortplats vid händelsens slut.

cardNumberCodriverSlotEnd identifierar det kort som är insatt i medförarens kortplats vid händelsens slut.

similarEventsNumber är antalet liknande händelser samma dag.

Denna sekvens ska användas vid alla händelser utom händelser av typen hastighetsöverträdelse.

▼B

Generation 2:

```
VuEventRecord ::= SEQUENCE {
   eventType                              EventFaultType,
   eventRecordPurpose                     EventFaultRecordPurpose,
   eventBeginTime                         TimeReal,
   eventEndTime                           TimeReal,
   cardNumberAndGenDriverSlotBegin        FullCardNumberAndGeneration,
   cardNumberAndGenCodriverSlotBegin      FullCardNumberAndGeneration,
   cardNumberAndGenDriverSlotEnd          FullCardNumberAndGeneration,
   cardNumberAndGenCodriverSlotEnd        FullCardNumberAndGeneration,
   similarEventsNumber                    SimilarEventsNumber,
   manufacturerSpecificEventFaultData   ManufacturerSpecificEventFaultData
}
```

Jämfört med generation 1 används följande ytterligare dataelement:

manufacturerSpecificEventFaultData innehåller ytterligare, tillverkarspecifik information om händelsen.

I stället för cardNumberDriverSlotBegin, cardNumberCodriverSlotBegin, cardNumberDriverSlotEnd och cardNumberCodriverSlotEnd använder datastrukturen för generation 2 följande dataelement:

cardNumberAndGenDriverSlotBegin identifierar det kort, inbegripet dess generation, som är insatt i förarens kortplats vid händelsens början.

cardNumberAndGenCodriverSlotBegin identifierar det kort, inbegripet dess generation, som är insatt i medförarens kortplats vid händelsens början.

cardNumberAndGenDriverSlotEnd identifierar det kort, inbegripet dess generation, som är insatt i förarens kortplats vid händelsens slut.

cardNumberAndGenCodriverSlotEnd identifierar det kort, inbegripet dess generation, som är insatt i medförarens kortplats vid händelsens slut.

Om händelsen är en tidskonflikt ska eventBeginTime och eventEndTime tolkas enligt följande:

eventBeginTime är datum och tidpunkt enligt färdskrivaren.

eventEndTime är datum och tidpunkt enligt GNSS.

2.199. **VuEventRecordArray**

Generation 2:

Information lagrad i en fordonsenhet om händelser (krav 117 i bilaga 1C, utom händelser av typen hastighetsöverträdelse).

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

recordType anger typen av post (VuEventRecord). **Värdetilldelning:** Se RecordType.

▼B

recordSize är storleken av VuEventRecord i byte.

noOfRecords är antalet poster i postmängden.

records är en mängd poster för händelser.

2.200. **VuFaultData**

Generation 1:

Information lagrad i en fordonsenhet om fel (krav 096 i bilaga 1B).

```
VuFaultData ::= SEQUENCE {
   noOfVuFaults                          INTEGER(0..255),
   vuFaultRecords                        SET SIZE(noOfVuFaults) OF VuFaultRecord
}
```

noOfVuFaults är antalet fel som finns förtecknade i mängden vuFaultRecords.

vuFaultRecords är en mängd felposter.

2.201. **VuFaultRecord**

Information lagrad i en fordonsenhet om ett fel (krav 096 i bilaga 1B och krav 118 i bilaga 1C).

Generation 1:

```
VuFaultRecord ::= SEQUENCE {
   faultType                             EventFaultType,
   faultRecordPurpose                    EventFaultRecordPurpose,
   faultBeginTime                        TimeReal,
   faultEndTime                          TimeReal,
   cardNumberDriverSlotBegin             FullCardNumber,
   cardNumberCodriverSlotBegin           FullCardNumber,
   cardNumberDriverSlotEnd               FullCardNumber,
   cardNumberCodriverSlotEnd             FullCardNumber
}
```

faultType är typ av färdskrivarfel.

faultRecordPurpose är syftet med registreringen av detta fel.

faultBeginTime är datum och tidpunkt för felets början.

faultEndTime är datum och tidpunkt för felets slut.

cardNumberDriverSlotBegin identifierar det kort som är insatt i förarens kortplats vid felets början.

cardNumberCodriverSlotBegin identifierar det kort som är insatt i medförarens kortplats vid felets början.

cardNumberDriverSlotEnd identifierar det kort som är insatt i förarens kortplats vid felets slut.

cardNumberCodriverSlotEnd identifierar det kort som är insatt i medförarens kortplats vid felets slut.

▼B

Generation 2:

```
VuFaultRecord ::= SEQUENCE {
   faultType                              EventFaultType,
   faultRecordPurpose                     EventFaultRecordPurpose,
   faultBeginTime                         TimeReal,
   faultEndTime                           TimeReal,
   cardNumberAndGenDriverSlotBegin        FullCardNumberAndGeneration,
   cardNumberAndGenCodriverSlotBegin      FullCardNumberAndGeneration,
   cardNumberAndGenDriverSlotEnd          FullCardNumberAndGeneration,
   cardNumberAndGenCodriverSlotEnd        FullCardNumberAndGeneration,
   manufacturerSpecificEventFaultData   ManufacturerSpecificEventFaultData
}
```

Jämfört med generation 1 används följande ytterligare dataelement:

manufacturerSpecificEventFaultData innehåller ytterligare, tillverkarspecifik information om felet.

I stället för cardNumberDriverSlotBegin, cardNumberCodriverSlotBegin, cardNumberDriverSlotEnd och cardNumberCodriverSlotEnd använder datastrukturen för generation 2 följande dataelement:

cardNumberAndGenDriverSlotBegin identifierar det kort, inbegripet dess generation, som är insatt i förarens kortplats vid felets början.

cardNumberAndGenCodriverSlotBegin identifierar det kort, inbegripet dess generation, som är insatt i medförarens kortplats vid felets början.

cardNumberAndGenDriverSlotEnd identifierar det kort, inbegripet dess generation, som är insatt i förarens kortplats vid felets slut.

cardNumberAndGenCodriverSlotEnd identifierar det kort, inbegripet dess generation, som är insatt i medförarens kortplats vid felets slut.

2.202. **VuFaultRecordArray**

Generation 2:

Information lagrad i en fordonsenhet om fel (krav 118 i bilaga 1C).

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

recordType anger typen av post (VuFaultRecord). **Värdetilldelning:** Se RecordType.

recordSize är storleken av VuFaultRecord i byte.

noOfRecords är antalet poster i postmängden.

records är en mängd felposter.

▼B

2.203. **VuGNSSCDRecord**

Generation 2:

Information lagrad i en fordonsenhet om fordonets GNSS-position om förarens sammanhängande körtid uppnår en multipel av tre timmar (krav 108 och 110 i bilaga 1C).

```
VuGNSSCDRecord ::= SEQUENCE {
   timeStamp                              TimeReal,
   cardNumberAndGenDriverSlot             FullCardNumberAndGeneration,
   cardNumberAndGenCodriverSlot           FullCardNumberAndGeneration,
   gnssPlaceRecord                        GNSSPlaceRecord
}
```

timeStamp är datum och tidpunkt när kortinnehavarens sammanhängande körtid uppgår till 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.

2.204. **VuGNSSCDRecordArray**

Generation 2:

Information lagrad i en fordonsenhet om fordonets GNSS-position om förarens sammanhängande körtid uppnår en multipel av tre timmar (krav 108 och 110 i bilaga 1C).

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

recordType anger typen av post (VuGNSSCDRecord). **Värdetilldelning:** Se RecordType.

recordSize är storleken av VuGNSSCDRecord i byte.

noOfRecords är antalet poster i postmängden.

records är en mängd poster om sammanhängande körning enligt GNSS.

2.205. **VuIdentification**

Information lagrad i en fordonsenhet om identifiering av fordonsenheten (krav 075 i bilaga 1B och krav 93 och 121 i bilaga 1C).

▼B

Generation 1:

```
VuIdentification ::= SEQUENCE {
   vuManufacturerName                  VuManufacturerName,
   vuManufacturerAddress               VuManufacturerAddress,
   vuPartNumber                        VuPartNumber,
   vuSerialNumber                      VuSerialNumber,
   vuSoftwareIdentification            VuSoftwareIdentification,
   vuManufacturingDate                 VuManufacturingDate,
   vuApprovalNumber                    VuApprovalNumber
}
```

vuManufacturerName är namnet på fordonsenhetens tillverkare.

vuManufacturerAddress är adressen till fordonsenhetens tillverkare.

vuPartNumber är fordonsenhetens artikelnummer.

vuSerialNumber är fordonsenhetens serienummer.

vuSoftwareIdentification identifierar den programvara som används i fordonsenheten.

vuManufacturingDate är fordonsenhetens tillverkningsdatum.

vuApprovalNumber är fordonsenhetens typgodkännandenummer.

Generation 2:

```
VuIdentification ::= SEQUENCE {
   vuManufacturerName                  VuManufacturerName,
   vuManufacturerAddress               VuManufacturerAddress,
   vuPartNumber                        VuPartNumber,
   vuSerialNumber                      VuSerialNumber,
   vuSoftwareIdentification            VuSoftwareIdentification,
   vuManufacturingDate                 VuManufacturingDate,
   vuApprovalNumber                    VuApprovalNumber,
   vuGeneration                        Generation,
   vuAbility                           VuAbility
}
```

Jämfört med generation 1 används följande ytterligare dataelement:

vuGeneration anger fordonsenhetens generation.

vuAbility ger information om huruvida fordonsenheten stöder färdskrivarkort i generation 1 eller inte.

2.206. **VuIdentificationRecordArray**

Generation 2:

VuIdentification samt metadata som används i överföringsprotokollet.

▼B

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

recordType anger typen av post (VuIdentification). **Värdetilldelning:** Se RecordType.

recordSize är storleken av VuIdentification i byte.

noOfRecords är antalet poster i postmängden.

records är mängden av VuIdentification-poster.

2.207. **VuITSConsentRecord**

Generation 2:

Information lagrad i en fordonsenhet om en förares samtycke till att använda intelligenta transportsystem (ITS).

```
VuITSConsentRecord ::= SEQUENCE {
   cardNumberAndGen                    FullCardNumberAndGeneration,
   consent                             BOOLEAN
}
```

cardNumberAndGen identifierar kortet, inbegripet dess generation. Detta måste vara ett förarkort eller ett verkstadskort.

consent är en markering som anger om föraren har gett sitt samtycke om användning av intelligenta transportsystem (ITS) med detta fordon/denna fordonsenhet.

Värdetilldelning:

TRUE	anger att föraren samtycker till att använda intelligenta transportsystem (ITS).
FALSE	anger att föraren inte samtycker till att använda intelligenta transportsystem (ITS).

2.208. **VuITSConsentRecordArray**

Generation 2:

Information lagrad i en fordonsenhet om förares samtycke till användning av intelligenta transportsystem (ITS) (krav 200 i bilaga 1C).

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

recordType anger typen av post (VuITSConsentRecord). **Värdetilldelning:** Se RecordType.

recordSize är storleken av VuITSConsentRecord i byte.

noOfRecords är antalet poster i postmängden.

records är mängden poster som rör samtycke till användning av intelligenta transportsystem (ITS).

▼B

2.209. **VuManufacturerAddress**

Adress till fordonsenhetens tillverkare.

```
VuManufacturerAddress ::= Address
```

Värdetilldelning: Ospecificerad.

2.210. **VuManufacturerName**

Namn på fordonsenhetens tillverkare.

```
VuManufacturerName ::= Name
```

Värdetilldelning: Ospecificerad.

2.211. **VuManufacturingDate**

Fordonsenhetens tillverkningsdatum.

```
VuManufacturingDate ::= TimeReal
```

Värdetilldelning: Ospecificerad.

2.212. **VuOverSpeedingControlData**

Information lagrad i en fordonsenhet om händelser av typen hastighetsöverträdelse sedan den senaste kontrollen av hastighetsöverträdelse (krav 095 i bilaga 1B och krav 117 i bilaga 1C).

```
VuOverSpeedingControlData ::= SEQUENCE {
   lastOverspeedControlTime             TimeReal,
   firstOverspeedSince                  TimeReal,
   numberOfOverspeedSince               OverspeedNumber
}
```

lastOverspeedControlTime är datum och tidpunkt för den senaste kontrollen av hastighetsöverträdelse.

firstOverspeedSince är datum och tidpunkt för den första hastighetsöverträdelsen efter denna kontroll av hastighetsöverträdelse.

numberOfOverspeedSince är antalet händelser av typen hastighetsöverträdelse sedan den senaste kontrollen av hastighetsöverträdelse.

2.213. **VuOverSpeedingControlDataRecordArray**

Generation 2:

VuOverSpeedingControlData samt metadata som används i överföringsprotokollet.

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

▼B

recordType anger typen av post (VuOverSpeedingControlData). **Värdetilldelning:** Se RecordType.

recordSize är storleken av VuOverSpeedingControlData i byte.

noOfRecords är antalet poster i postmängden.

records är en mängd poster med data om kontroller av hastighetsöverträdelse.

2.214. **VuOverSpeedingEventData**

Generation 1:

Information lagrad i en fordonsenhet om händelser av typen hastighetsöverträdelse (krav 094 i bilaga 1B).

```
VuOverSpeedingEventData ::= SEQUENCE {
   noOfVuOverSpeedingEvents              INTEGER(0..255),
   vuOverSpeedingEventRecords            SET SIZE(noOfVuOverSpeedingEvents) OF
                                         VuOverSpeedingEventRecord
}
```

noOfVuOverSpeedingEvents är det antal händelser som finns förteckнade i mängden vuOverSpeedingEventRecords.

vuOverSpeedingEventRecords är en mängd poster för händelser av typen hastighetsöverträdelse.

2.215. **VuOverSpeedingEventRecord**

Generation 1:

Information lagrad i en fordonsenhet om händelser av typen hastighetsöverträdelse (krav 094 i bilaga 1B och krav 117 i bilaga 1C).

```
VuOverSpeedingEventRecord ::= SEQUENCE {
   eventType                             EventFaultType,
   eventRecordPurpose                    EventFaultRecordPurpose,
   eventBeginTime                        TimeReal,
   eventEndTime                          TimeReal,
   maxSpeedValue                         SpeedMax,
   averageSpeedValue                     SpeedAverage,
   cardNumberDriverSlotBegin             FullCardNumber,
   similarEventsNumber                   SimilarEventsNumber
}
```

eventType är typ av händelse.

eventRecordPurpose är syftet med registreringen av denna händelse.

eventBeginTime är datum och tidpunkt för händelsens början.

eventEndTime är datum och tidpunkt för händelsens slut.

maxSpeedValue är den högsta hastighet som uppmätts under händelsen.

averageSpeedValue är den aritmetiska genomsnittliga hastighet som uppmätts under händelsen.

▼B

cardNumberDriverSlotBegin identifierar det kort som är insatt i förarens kortplats vid händelsens början.

similarEventsNumber är antalet liknande händelser samma dag.

Generation 2:

Information lagrad i en fordonsenhet om händelser av typen hastighetsöverträdelse (krav 094 i bilaga 1B och krav 117 i bilaga 1C).

```
VuOverSpeedingEventRecord ::= SEQUENCE {
   eventType                              EventFaultType,
   eventRecordPurpose                     EventFaultRecordPurpose,
   eventBeginTime                         TimeReal,
   eventEndTime                           TimeReal,
   maxSpeedValue                          SpeedMax,
   averageSpeedValue                      SpeedAverage,
   cardNumberAndGenDriverSlotBegin        FullCardNumberAndGeneration,
   similarEventsNumber                    SimilarEventsNumber
}
```

I stället för cardNumberDriverSlotBegin använder datastrukturen för generation 2 följande dataelement:

cardNumberAndGenDriverSlotBegin identifierar det kort, inbegripet dess generation, som är insatt i förarens kortplats vid händelsens början.

2.216. **VuOverSpeedingEventRecordArray**

Generation 2:

Information lagrad i en fordonsenhet om händelser av typen hastighetsöverträdelse (krav 117 i bilaga 1C).

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

recordType anger typen av post (VuOverSpeedingEventRecord). **Värdetilldelning:** Se RecordType.

recordSize är storleken av VuOverSpeedingEventRecord i byte.

noOfRecords är antalet poster i postmängden.

records är en mängd poster för händelser av typen hastighetsöverträdelse.

2.217. **VuPartNumber**

Fordonsenhetens artikelnummer.

```
VuPartNumber ::= IA5String(SIZE(16))
```

Värdetilldelning: Specifik för tillverkaren av fordonsenheter.

▼B

2.218. **VuPlaceDailyWorkPeriodData**

Generation 1:

Information lagrad i en fordonsenhet om de platser där förare påbörjar eller avslutar en arbetsperiod (krav 087 i bilaga 1B och krav 108 och 110 i bilaga 1C).

```
VuPlaceDailyWorkPeriodData ::= SEQUENCE {
   noOfPlaceRecords                    INTEGER(0..255),
   vuPlaceDailyWorkPeriodRecords       SET SIZE(noOfPlaceRecords) OF
                                       VuPlaceDailyWorkPeriodRecord
}
```

noOfPlaceRecords är antalet poster som finns förtecknade i mängden vuPlaceDailyWorkPeriodRecords.

vuPlaceDailyWorkPeriodRecords är en mängd platsrelaterade poster.

2.219. **VuPlaceDailyWorkPeriodRecord**

Generation 1:

Information lagrad i en fordonsenhet om en plats där en förare påbörjar eller avslutar en arbetsperiod (krav 087 i bilaga 1B och krav 108 och 110 i bilaga 1C).

```
VuPlaceDailyWorkPeriodRecord ::= SEQUENCE {
   fullCardNumber                      FullCardNumber,
   placeRecord                         PlaceRecord
}
```

fullCardNumber är förarens korttyp, utfärdande medlemsstat och kortnummer.

placeRecord innehåller information om den plats som angetts.

Generation 2:

Information lagrad i en fordonsenhet om en plats där en förare påbörjar eller avslutar en arbetsperiod (krav 087 i bilaga 1B och krav 108 och 110 i bilaga 1C).

```
VuPlaceDailyWorkPeriodRecord ::= SEQUENCE {
   fullCardNumberAndGeneration         FullCardNumberAndGeneration,
   placeRecord                         PlaceRecord
}
```

I stället för fullCardNumber använder datastrukturen för generation 2 följande dataelement:

fullCardNumberAndGeneration är typ av kort, dess utfärdande medlemsstat, dess kortnummer och dess generation sådana de lagrats på kortet.

▼B

2.220. **VuPlaceDailyWorkPeriodRecordArray**

Generation 2:

Information lagrad i en fordonsenhet om de platser där förare påbörjar eller avslutar en arbetsperiod (krav 108 och 110 i bilaga 1C).

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

recordType anger typen av post (VuPlaceDailyWorkPeriodRecord).
Värdetilldelning: Se RecordType.

recordSize är storleken av VuPlaceDailyWorkPeriodRecord i byte.

noOfRecords är antalet poster i postmängden.

records är en mängd platsrelaterade poster.

2.221. **VuPrivateKey**

Generation 1:

En fordonsenhets privata nyckel.

```
VuPrivateKey ::= RSAKeyPrivateExponent
```

2.222. **VuPublicKey**

Generation 1:

En fordonsenhets öppna nyckel.

```
VuPublicKey ::= PublicKey
```

2.223. **VuSerialNumber**

Fordonsenhetens serienummer (krav 075 i bilaga 1B och krav 93 i bilaga 1C).

```
VuSerialNumber ::= ExtendedSerialNumber
```

2.224. **VuSoftInstallationDate**

Datum för installation av fordonsenhetens programvaruversion.

```
VuSoftInstallationDate ::= TimeReal
```

Värdetilldelning: Ospecificerad.

▼B

2.225. **VuSoftwareIdentification**

Information lagrad i en fordonsenhet om installerad programvara.

```
VuSoftwareIdentification ::= SEQUENCE {
   vuSoftwareVersion                    VuSoftwareVersion,
   vuSoftInstallationDate               VuSoftInstallationDate
}
```

vuSoftwareVersion är numret på programvaruversionen i fordonsenheten.

vuSoftInstallationDate är datum för installation av programvaruversionen.

2.226. **VuSoftwareVersion**

Nummer på programvaruversionen i fordonsenheten.

```
VuSoftwareVersion ::= IA5String(SIZE(4))
```

Värdetilldelning: Ospecificerad.

2.227. **VuSpecificConditionData**

Generation 1:

Information lagrad i en fordonsenhet om särskilda omständigheter.

```
VuSpecificConditionData ::= SEQUENCE {
   noOfSpecificConditionRecords         INTEGER(0..2^16-1)
   specificConditionRecords             SET SIZE (noOfSpecificConditionRecords) OF
                                        SpecificConditionRecord
}
```

noOfSpecificConditionRecords är antalet poster som finns förtecknade i mängden specificConditionRecords.

specificConditionRecords är en mängd poster som rör särskilda omständigheter.

2.228. **VuSpecificConditionRecordArray**

Generation 2:

Information lagrad i en fordonsenhet om särskilda omständigheter (krav 130 i bilaga 1C).

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

recordType anger typen av post (SpecificConditionRecord). **Värdetilldelning:** Se RecordType.

recordSize är storleken av SpecificConditionRecord i byte.

noOfRecords är antalet poster i postmängden.

records är en mängd poster som rör särskilda omständigheter.

▼B

2.229. **VuTimeAdjustmentData**

Generation 1:

Information lagrad i en fordonsenhet om tidsinställningar som inte utförts vid en normal kalibrering (krav 101 i bilaga 1B).

```
VuTimeAdjustmentData ::= SEQUENCE {
   noOfVuTimeAdjRecords                 INTEGER(0..6),
   vuTimeAdjustmentRecords              SET SIZE(noOfVuTimeAdjRecords) OF
                                        VuTimeAdjustmentRecord
}
```

noOfVuTimeAdjRecords är antalet poster i vuTimeAdjustmentRecords**.**

vuTimeAdjustmentRecords är en mängd poster för tidsinställningar.

2.230. **VuTimeAdjustmentGNSSRecord**

Generation 2:

Information lagrad i en fordonsenhet om en tidsinställning som är baserad på tidsdata från GNSS (krav 124 och 125 i bilaga 1C).

```
VuTimeAdjustmentGNSSRecord ::= SEQUENCE {
   oldTimeValue                         TimeReal,
   newTimeValue                         TimeReal
}
```

oldTimeValue, newTimeValue är de gamla och nya värdena för datum och tidpunkt.

2.231. **VuTimeAdjustmentGNSSRecordArray**

Generation 2:

Information lagrad i en fordonsenhet om en tidsinställning som utförs på grundval av tidsdata från GNSS (krav 124 och 125 i bilaga 1C).

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

recordType anger typen av post (VuTimeAdjustmentGNSSRecord).
Värdetilldelning: Se RecordType.

recordSize är storleken av VuTimeAdjustmentGNSSRecord i byte.

noOfRecords är antalet poster i postmängden.

records är en mängd poster för GNSS-baserade tidsinställningar.

▼B

2.232. **VuTimeAdjustmentRecord**

Information lagrad i en fordonsenhet om en tidsinställning som inte utförts vid en normal kalibrering (krav 101 i bilaga 1B och krav 124 och 125 i bilaga 1C).

Generation 1:

```
VuTimeAdjustmentRecord ::= SEQUENCE {
   oldTimeValue                         TimeReal,
   newTimeValue                         TimeReal,
   workshopName                         Name,
   workshopAddress                      Address,
   workshopCardNumber                   FullCardNumber
}
```

oldTimeValue, newTimeValue är de gamla och nya värdena för datum och tidpunkt.

workshopName, workshopAddress är verkstadens namn och adress.

workshopCardNumber identifierar det verkstadskort som använts för att utföra tidsinställningen.

Generation 2:

```
VuTimeAdjustmentRecord ::= SEQUENCE {
   oldTimeValue                         TimeReal,
   newTimeValue                         TimeReal,
   workshopName                         Name,
   workshopAddress                      Address,
   workshopCardNumberAndGeneration      FullCardNumberAndGeneration
}
```

I stället för workshopCardNumber använder datastrukturen för generation 2 följande dataelement:

workshopCardNumberAndGeneration identifierar det verkstadskort, inbegripet dess generation, som används för att utföra tidsinställningen.

2.233. **VuTimeAdjustmentRecordArray**

Generation 2:

Information lagrad i en fordonsenhet om tidsinställningar som inte utförts vid en normal kalibrering (krav 124 och 125 i bilaga 1C).

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

recordType anger typen av post (VuTimeAdjustmentRecord). **Värdetilldelning:** Se RecordType.

recordSize är storleken av VuTimeAdjustmentRecord i byte.

▼B

noOfRecords är antalet poster i postmängden.

records är en mängd poster för tidsinställningar.

2.234. **WorkshopCardApplicationIdentification**

Information lagrad i ett verkstadskort om identifiering av korttillämpningen (krav 307 och 330 i bilaga 1C).

Generation 1:

```
WorkshopCardApplicationIdentification ::= SEQUENCE {
   typeOfTachographCardId               EquipmentType,
   cardStructureVersion                 CardStructureVersion,
   noOfEventsPerType                    NoOfEventsPerType,
   noOfFaultsPerType                    NoOfFaultsPerType,
   activityStructureLength              CardActivityLengthRange,
   noOfCardVehicleRecords               NoOfCardVehicleRecords,
   noOfCardPlaceRecords                 NoOfCardPlaceRecords,
   noOfCalibrationRecords               NoOfCalibrationRecords
}
```

typeOfTachographCardId specificerar använd korttyp.

cardStructureVersion specificerar versionen av den struktur som används i kortet.

noOfEventsPerType är antalet händelser per händelsetyp som kortet kan registrera.

noOfFaultsPerType är antalet fel per typ av fel som kortet kan registrera.

activityStructureLength anger antal byte som finns tillgängliga för lagring av aktivitetsposter.

noOfCardVehicleRecords är antalet fordonsposter som kortet kan registrera.

noOfCardPlaceRecords är det antal platser som kortet kan lagra.

noOfCalibrationRecords är det antal kalibreringsposter som kortet kan lagra.

Generation 2:

```
WorkshopCardApplicationIdentification ::= SEQUENCE {
   typeOfTachographCardId               EquipmentType,
   cardStructureVersion                 CardStructureVersion,
   noOfEventsPerType                    NoOfEventsPerType,
   noOfFaultsPerType                    NoOfFaultsPerType,
   activityStructureLength              CardActivityLengthRange,
   noOfCardVehicleRecords               NoOfCardVehicleRecords,
   noOfCardPlaceRecords                 NoOfCardPlaceRecords,
   noOfCalibrationRecords               NoOfCalibrationRecords,
   noOfGNSSCDRecords                    NoOfGNSSCDRecords,
   noOfSpecificConditionRecords         NoOfSpecificConditionRecords
}
```

Jämfört med generation 1 används följande ytterligare dataelement:

noOfGNSSCDRecords är det antal GNSS-poster om sammanhängande körning som kortet kan lagra.

▼B

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

2.235. **WorkshopCardCalibrationData**

Information lagrad i ett verkstadskort om verkstadsaktivitet som utförts med kortet (krav 314, 316, 337 och 339 i bilaga 1C).

```
WorkshopCardCalibrationData ::= SEQUENCE {
   calibrationTotalNumber                INTEGER(0 .. 2^16-1),
   calibrationPointerNewestRecord        INTEGER(0 .. NoOfCalibrationRecords-1),
   calibrationRecords                    SET SIZE(NoOfCalibrationRecords) OF
                                         WorkshopCardCalibrationRecord
}
```

calibrationTotalNumber är det sammanlagda antal kalibreringar som utförts med kortet.

calibrationPointerNewestRecord är index för senast uppdaterad kalibreringspost.

Värdetilldelning: Ett tal som motsvarar kalibreringspostens numerator, och som börjar med ′0′ för den första gången kalibreringsposterna uppträder i strukturen.

calibrationRecords är den mängd poster som innehåller information om kalibreringar och/eller tidsinställningar.

2.236. **WorkshopCardCalibrationRecord**

Information lagrad i ett verkstadskort om en kalibrering som utförts med kortet (krav 314 och 337 i bilaga 1C).

Generation 1:

```
WorkshopCardCalibrationRecord ::= SEQUENCE {
   calibrationPurpose                    CalibrationPurpose,
   vehicleIdentificationNumber           VehicleIdentificationNumber,
   vehicleRegistration                   VehicleRegistrationIdentification,
   wVehicleCharacteristicConstant        W-VehicleCharacteristicConstant,
   kConstantOfRecordingEquipment         K-ConstantOfRecordingEquipment,
   lTyreCircumference                    L-TyreCircumference,
   tyreSize                              TyreSize,
   authorisedSpeed                       SpeedAuthorised,
   oldOdometerValue                      OdometerShort,
   newOdometerValue                      OdometerShort,
   oldTimeValue                          TimeReal,
   newTimeValue                          TimeReal,
   nextCalibrationDate                   TimeReal,
   vuPartNumber                          VuPartNumber,
   vuSerialNumber                        VuSerialNumber,
   sensorSerialNumber                    SensorSerialNumber
}
```

calibrationPurpose är syftet med kalibreringen.

vehicleIdentificationNumber är fordonets identifieringsnummer (VIN).

vehicleRegistration innehåller fordonets registreringsnummer (VRN) och registrerande medlemsstat.

wVehicleCharacteristicConstant är fordonets karakteristiska koefficient.

▼B

kConstantOfRecordingEquipment är färdskrivarens konstant.

lTyreCircumference är däckens effektiva omkrets.

tyreSize är angivelse av dimensionerna på de däck som monterats på fordonet.

authorisedSpeed är den högsta tillåtna hastigheten för fordonet.

oldOdometerValue, newOdometerValue är de gamla och nya vägmätarställningarna.

oldTimeValue, newTimeValue är de gamla och nya värdena för datum och tidpunkt.

nextCalibrationDate är datum för nästa kalibrering av den typ som anges i CalibrationPurpose och som ska utföras av den auktoriserade besiktningsmyndigheten.

vuPartNumber, **vuSerialNumber** och **sensorSerialNumber** är dataelementen för identifiering av färdskrivare.

Generation 2:

```
WorkshopCardCalibrationRecord ::= SEQUENCE {
   calibrationPurpose                    CalibrationPurpose,
   vehicleIdentificationNumber           VehicleIdentificationNumber,
   vehicleRegistration                   VehicleRegistrationIdentification,
   wVehicleCharacteristicConstant        W-VehicleCharacteristicConstant,
   kConstantOfRecordingEquipment         K-ConstantOfRecordingEquipment,
   lTyreCircumference                    L-TyreCircumference,
   tyreSize                              TyreSize,
   authorisedSpeed                       SpeedAuthorised,
   oldOdometerValue                      OdometerShort,
   newOdometerValue                      OdometerShort,
   oldTimeValue                          TimeReal,
   newTimeValue                          TimeReal,
   nextCalibrationDate                   TimeReal,
   vuPartNumber                          VuPartNumber,
   vuSerialNumber                        VuSerialNumber,
   sensorSerialNumber                    SensorSerialNumber,
   sensorGNSSSerialNumber                SensorGNSSSerialNumber,
   rcmSerialNumber                       RemoteCommunicationModuleSerialNumber,
   sealDataCard                          SealDataCard
}
```

Jämfört med generation 1 används följande ytterligare dataelement:

sensorGNSSSerialNumber, som identifierar en extern GNSS-anordning.

rcmSerialNumber, som identifierar en fjärrkommunikationsmodul.

sealDataCard ger information om de plomberingar som anbringats på olika komponenter i fordonet.

▼B

2.237. **WorkshopCardHolderIdentification**

Information lagrad i ett verkstadskort om identifiering av kortinnehavare (krav 311 och 334 i bilaga 1C).

```
WorkshopCardHolderIdentification ::= SEQUENCE {
   workshopName                          Name,
   workshopAddress                       Address,
   cardHolderName                        HolderName,
   cardHolderPreferredLanguage           Language
}
```

workshopName är namnet på kortinnehavarens verkstad.

workshopAddress är adressen till kortinnehavarens verkstad.

cardHolderName är innehavarens namn och förnamn (exempelvis mekanikerns namn).

cardHolderPreferredLanguage är det språk som kortinnehavaren väljer.

2.238. **WorkshopCardPIN**

Verkstadskortets personliga identifieringsnummer (krav 309 och 332 i bilaga 1C).

```
WorkshopCardPIN ::= IA5String(SIZE(8))
```

Värdetilldelning: Den PIN-kod som kortinnehavaren har, högerutfylld med 'FF'-byte upp till 8 byte.

2.239. **W-VehicleCharacteristicConstant**

Fordonets karakteristiska koefficient (definition k)).

```
W-VehicleCharacteristicConstant ::= INTEGER(0..2^16-1))
```

Värdetilldelning: Pulser per kilometer i intervallet från 0 till 64 255 pulser/km.

2.240. **VuPowerSupplyInterruptionRecord**

Generation 2:

Information lagrad i en fordonsenhet om händelser av typen avbrott i strömtillförseln (krav 117 i bilaga 1C).

```
VuPowerSupplyInterruptionRecord ::= SEQUENCE {
   eventType                             EventFaultType,
   eventRecordPurpose                    EventFaultRecordPurpose,
   eventBeginTime                        TimeReal,
   eventEndTime                          TimeReal,
   cardNumberAndGenDriverSlotBegin       FullCardNumberAndGeneration,
   cardNumberAndGenDriverSlotEnd         FullCardNumberAndGeneration,
   cardNumberAndGenCodriverSlotBegin     FullCardNumberAndGeneration,
   cardNumberAndGenCodriverSlotEnd       FullCardNumberAndGeneration,
   similarEventsNumber                   SimilarEventsNumber
}
```

eventType är typ av händelse.

eventRecordPurpose är syftet med registreringen av denna händelse.

eventBeginTime är datum och tidpunkt för händelsens början.

▼B

eventEndTime är datum och tidpunkt för händelsens slut.

cardNumberAndGenDriverSlotBegin identifierar det kort, inbegripet dess generation, som är insatt i förarens kortplats vid händelsens början.

cardNumberAndGenDriverSlotEnd identifierar det kort, inbegripet dess generation, som är insatt i förarens kortplats vid händelsens slut.

cardNumberAndGenCodriverSlotBegin identifierar det kort, inbegripet dess generation, som är insatt i medförarens kortplats vid händelsens början.

cardNumberAndGenCodriverSlotEnd identifierar det kort, inbegripet dess generation, som är insatt i medförarens kortplats vid händelsens slut.

similarEventsNumber är antalet liknande händelser samma dag.

2.241. **VuPowerSupplyInterruptionRecordArray**

Generation 2:

Information lagrad i en fordonsenhet om händelser av typen avbrott i strömtillförseln (krav 117 i bilaga 1C).

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

recordType anger typen av post (VuPowerSupplyInterruptionRecord).
Värdetilldelning: Se RecordType.

recordSize är storleken av VuPowerSupplyInterruptionRecord i byte.

noOfRecords är antalet poster i postmängden.

records är en mängd poster för händelser av typen avbrott i strömtillförseln.

2.242. **VuSensorExternalGNSSCoupledRecordArray**

Generation 2:

En mängd SensorExternalGNSSCoupledRecord samt metadata som används i överföringsprotokollet.

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

recordType anger typen av post (SensorExternalGNSSCoupledRecord).
Värdetilldelning: Se RecordType.

▼B

recordSize är storleken av SensorExternalGNSSCoupledRecord i byte.

noOfRecords är antalet poster i postmängden.

records är en mängd poster från en kopplad extern GNSS-sensor.

2.243. **VuSensorPairedRecordArray**

Generation 2:

En mängd SensorPairedRecord samt metadata som används i överföringsprotokollet.

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

recordType anger typen av post (SensorPairedRecord). **Värdetilldelning:** Se RecordType.

recordSize är storleken av SensorPairedRecord i byte.

noOfRecords är antalet poster i postmängden.

records är mängden av poster från parade sensorer.

3. DEFINITIONER AV INTERVALL FÖR VÄRDEN OCH STORLEKAR

Definition av variabler som används för definitioner i avsnitt 2.

```
TimeRealRange ::= 2^32-1
```

4. TECKENMÄNGDER

IA5Strings använder ASCII-tecken enligt ISO/IEC 8824-1. För läsbarhet och enkel hänvisning ges värdetilldelningen nedan. ISO/IEC 8824-1 ersätter denna anmärkning i händelse av avvikelse.

```
  ! " # $ % & ' ( ) * + , - . / 0 1 2 3 4 5 6 7 8 9 : ; < = > ?
@ A B C D E F G H I J K L M N O P Q R S T U V W X Y Z [ \ ] ^ _
` a b c d e f g h i j k l m n o p q r s t u v w x y z { | } ~
```

Andra teckensträngar (Address, Name, VehicleRegistrationNumber) använder dessutom tecken från decimalkodintervall 161–255 i följande 8-bitars standardteckenuppsättning som anges av teckentabellens nummer: Standard för teckenmängd	Teckentabell (decimalt)
ISO/IEC 8859-1 Latin-1 Västeuropeisk	1
ISO/IEC 8859-2 Latin-2 Centraleuropeisk	2
ISO/IEC 8859-3 Latin-3 Sydeuropeisk	3
ISO/IEC 8859-5 Latin/kyrillisk	5
ISO/IEC 8859-7 Latin/grekisk	7
ISO/IEC 8859-9 Latin-5 Turkisk	9

▼B

Andra teckensträngar (Address, Name, VehicleRegistrationNumber) använder dessutom tecken från decimalkodintervall 161–255 i följande 8-bitars standardteckenuppsättning som anges av teckentabellens nummer: Standard för teckenmängd	Teckentabell (decimalt)
ISO/IEC 8859-13 Latin-7 baltiska	13
ISO/IEC 8859-15 Latin-9	15
ISO/IEC 8859-16 Latin-10 Sydosteuropeisk	16
KOI8-R Latin/kyrillisk	80
KOI8-U Latin/kyrillisk	85

5. KODNING

Definierade datatyper som kodas med kodningsreglerna ASN.1 ska kodas enligt ISO/IEC 8825-2, anpassad (*aligned*) variant.

6. OBJEKTIDENTIFIERARE OCH TILLÄMPNINGSIDENTIFIERARE

6.1. **Objektidentifierare**

De objektidentifierare (OID) som förtecknas i detta kapitel är relevanta endast för generation 2. Dessa OID specificeras i TR-03110-3 och återges här fullständighetens skull. Dessa OID finns i strukturen under bsi-de:

```
bsi-de OBJECT IDENTIFIER ::= {
   itu-t(0) identified-organization(4) etsi(0)
   reserved(127) etsi-identified-organization(0) 7
}
```

Protokollidentifierare för autentisering av fordonsenhet (VU)

```
id-TA         OBJECT IDENTIFIER ::= {bsi-de protocols(2) smartcard(2) 2}

id-TA-ECDSA                OBJECT IDENTIFIER ::= {id-TA 2}

id-TA-ECDSA-SHA-256 OBJECT IDENTIFIER ::= {id-TA-ECDSA 3}

id-TA-ECDSA-SHA-384 OBJECT IDENTIFIER ::= {id-TA-ECDSA 4}

id-TA-ECDSA-SHA-512 OBJECT IDENTIFIER ::= {id-TA-ECDSA 5}
```

Exempel: Antag att autentiseringen av en fordonsenhet ska utföras med SHA-384. Då ska följande objektidentifierare (i ASN.1-notation) användas: `bsi-de protocols(2) smartcard(2) 2 2 4`. Värdet för denna objektidentifierare i punktnotation är `0.4.0.127.0.7.2.2.2.2.4`.

	Punktnotation:	Bytenotation:
id-TA-ECDSA-SHA-256	0.4.0.127.0.7.2.2.2.2.3	‘04 00 7F 00 07 02 02 02 02 03’
id-TA-ECDSA-SHA-384	0.4.0.127.0.7.2.2.2.2.4	‘04 00 7F 00 07 02 02 02 02 04’
id-TA-ECDSA-SHA-512	0.4.0.127.0.7.2.2.2.2.5	‘04 00 7F 00 07 02 02 02 02 05’

▼B

Protokollidentifierare för autentisering av chip

```
id-CA         OBJECT IDENTIFIER ::= {bsi-de protocols(2) smartcard(2) 3}

id-CA-ECDH                        OBJECT IDENTIFIER ::= {id-CA 2}

id-CA-ECDH-AES-CBC-CMAC-128       OBJECT IDENTIFIER ::= {id-CA-ECDH 2}

id-CA-ECDH-AES-CBC-CMAC-192       OBJECT IDENTIFIER ::= {id-CA-ECDH 3}

id-CA-ECDH-AES-CBC-CMAC-256       OBJECT IDENTIFIER ::= {id-CA-ECDH 4}
```

Exempel: Antag att autentiseringen av ett chip ska utföras med ECDH-algoritmen som leder till en AES-sessionsnyckel med en längd av 128 bitar. Denna sessionsnyckel kommer sedan att användas i CBC-läge för att säkerställa datasekretess och med CMAC-algoritmen för att säkerställa autenticitet hos data. Därmed ska följande objektidentifierare (i ASN.1-notation) användas: `bsi-de protocols(2) smartcard(2) 3 2 2`. Värdet för denna objektidentifierare i punktnotation är `0.4.0.127.0.7.2.2.3.2.2`.

	Punktnotation:	Bytenotation:
id-CA-ECDH-AES-CBC-CMAC-128	0.4.0.127.0.7.2.2.3.2.2	‘04 00 7F 00 07 02 02 03 02 02’
id-CA-ECDH-AES-CBC-CMAC-192	0.4.0.127.0.7.2.2.3.2.3	‘04 00 7F 00 07 02 02 03 02 03’
id-CA-ECDH-AES-CBC-CMAC-256	0.4.0.127.0.7.2.2.3.2.4	‘04 00 7F 00 07 02 02 03 02 04’

6.2. **Tillämpningsidentifierare**

Generation 2:

Tillämpningsidentifieraren (AID) för den externa GNSS-anordningen i generation 2 är ‘FF 44 54 45 47 4D’. Denna är en proprietär (*proprietary*) tillämpningsidentifierare i enlighet med ISO/IEC 7816-4.

Anmärkning: De sista 5 bytarna kodar ”DTEGM” för den smarta färdskrivarens externa GNSS-anordning.

Tillämpningsidentifieraren (AID) för färdskrivarkortets tillämpning i generation 2 är ‘FF 53 4D 52 44 54’. Denna är en proprietär (*proprietary*) tillämpningsidentifierare i enlighet med ISO/IEC 7816-4.

▼B

Tillägg 2

SPECIFIKATION FÖR FÄRDSKRIVARKORT

INNEHÅLLSFÖRTECKNING

1. INLEDNING

1.1. Förkortningar

1.2. Referenser

2. ELEKTRISKA OCH FYSISKA EGENSKAPER

2.1. Försörjningsspänning och strömförbrukning

2.2. Programmeringsspänning V_{pp}

2.3. Klockgenerering och klockfrekvens

2.4. I/O-kontakt

2.5. Kortets tillstånd

3. MASKINVARA OCH KOMMUNIKATION

3.1. Inledning

3.2. Överföringsprotokoll

3.2.1 Protokoll

3.2.2 ATR

3.2.3 PTS

3.3. Tillträdesregler

3.4. Översikt av kommandon och felkoder

3.5. Kommandobeskrivning

3.5.1 SELECT

3.5.2 READ BINARY

3.5.3 UPDATE BINARY

3.5.4 GET CHALLENGE

3.5.5 VERIFY

3.5.6 GET RESPONSE

3.5.7 PSO: VERIFY CERTIFICATE

3.5.8 INTERNAL AUTHENTICATE

3.5.9 EXTERNAL AUTHENTICATE

3.5.10 GENERAL AUTHENTICATE

3.5.11 MANAGE SECURITY ENVIRONMENT

3.5.12 PSO: HASH

▼B

3.5.13 PERFORM HASH of FILE

3.5.14 PSO: COMPUTE DIGITAL SIGNATURE

3.5.15 PSO: VERIFY DIGITAL SIGNATURE

3.5.16 PROCESS DSRC MESSAGE

4. FÄRDSKRIVARKORTENS STRUKTUR

4.1. Huvudfil (MF)

4.2. Förarkortstillämpningar

4.2.1 Förarkortstillämpning (generation 1)

4.2.2 Förarkortstillämpning (generation 2)

4.3. Verkstadskortstillämpningar

4.3.1 Verkstadskortstillämpning (generation 1)

4.3.2 Verkstadskortstillämpning (generation 2)

4.4. Kontrollkortstillämpningar

4.4.1 Kontrollkortstillämpning (generation 1)

4.4.2 Kontrollkortstillämpning (generation 2)

4.5. Företagskortstillämpningar

4.5.1 Företagskortstillämpning (generation 1)

4.5.2 Företagskortstillämpning (generation 2)

1. INLEDNING

1.1. **Förkortningar**

Följande förkortningar används i detta tillägg:

AC	*Access Conditions* (tillträdesvillkor)
AES	*Advanced Encryption Standard* (standardiserad krypteringsalgoritm)
AID	*Application Identifier* (tillämpningsidentifierare)
ALW	*Always* (alltid)
APDU	*Application Protocol Data Unit* (dataenhet i ett tillämpningsprotokolls kommandostruktur)
ATR	*Answer To Reset* (återställningssignal)
AUT	*Authenticated* (autentiserad)
C6, C7	Kontakterna nr 6 och 7 på kortet enligt ISO/IEC 7816-2
cc	*clock cycles* (klockcykler)
CHV	*Card Holder Verification Information* (kortinnehavarens verifieringsinformation)
CLA	*Class byte* (byte som anger klass i ett APDU-kommando)

▼B

DSRC	*Dedicated Short Range Communication* (radiokommunikation över korta avstånd)
DF	*Dedicated File* (dedikerad fil), en dedikerad fil kan innehålla andra filer (EF eller DF)
ECC	*Elliptic Curve Cryptography* (elliptisk kryptering)
EF	*Elementary File* (elementfil)
etu	*elementary time unit* (grundläggande tidsenhet)
G1	Generation 1
G2	Generation 2
IC	*Integrated Circuit* (integrerad krets)
ICC	*Integrated Circuit Card* (smartkort, kort med integrerade kretsar)
ID	*Identifier* (identifierare)
IFD	*Interface Device* (kortläsare)
IFS	*Information Field Size* (storlek för informationsfält)
IFSC	*Information Field Size – Card* (kortets storlek för informationsfält)
IFSD	*Information Field Size – Device* (terminalens storlek för informationsfält)
INS	*Instruction byte* (byte som anger instruktion i ett APDU-kommando)
Lc	Längd på indata för ett APDU-kommando
Le	Längd på förväntade data (utdata för ett kommando)
MF	*Master File* (huvudfil, rotnivå)
NAD	*Node Address* (nodadress som används i T=1-protokoll)
NEV	*Never* (aldrig)
P1-P2	Byte som anger parameter
PIN	*Personal Identification Number* (personligt identifieringsnummer)
PRO SM	*Protected with Secure Messaging* (skyddas med säker meddelandehantering)
PTS	*Protocol Transmission Selection* (val av överföringsprotokoll)
RFU	*Reserved for Future Use* (reserverat för framtida användning)
RST	*Reset* (nollställning av kortet)
SFID	*Short EF Identifier* (kort identifierare för elementfil)
SM	*Secure Messaging* (säker meddelandehantering)
SW1-SW2	Byte som anger status
TS	Inledande ATR-tecken
VPP	*Programming Voltage* (programmeringsspänning)
VU	*Vehicle Unit* (fordonsenhet)
XXh	Värde XX hexadecimalt
‘XXh’	Värde XX hexadecimalt
||	Konkateneringssymbol (03||04=0304)

▼B

1.2. **Referenser**

Följande referenser används i detta tillägg:

ISO/IEC 7816-2	Identification cards – Integrated circuit cards – Part 2: Dimensions and location of the contacts. ISO/IEC 7816-2:2007.
ISO/IEC 7816-3	Identification cards – Integrated circuit cards – Part 3: Electrical interface and transmission protocols. ISO/IEC 7816-3:2006.
ISO/IEC 7816-4	Identification cards – Integrated circuit cards – Part 4: Organization, security and commands for interchange. ISO/IEC 7816-4:2013 + Cor 1: 2014.
ISO/IEC 7816-6	Identification cards – Integrated circuit cards – Part 6: Interindustry data elements for interchange. ISO/IEC 7816-6:2004 + Cor 1: 2006.
ISO/IEC 7816-8	Identification cards – Integrated circuit cards – Part 8: Commands for security operations. ISO/IEC 7816-8:2004.
ISO/IEC 9797-2	Information technology – Security techniques – Message Authentication Codes (MACs) – Part 2: Mechanisms using a dedicated hash-function. ISO/IEC 9797-2:2011

2. ELEKTRISKA OCH FYSISKA EGENSKAPER

TCS_01 Alla elektroniska signaler ska överensstämma med ISO/IEC 7816-3 om inte annat anges.

TCS_02 Kortkontakternas placering och dimensioner ska överensstämma med ISO/IEC 7816-2.

2.1. **Försörjningsspänning och strömförbrukning**

TCS_03 Kortet ska fungera enligt specifikationer inom de begränsningar av strömförbrukningen som anges i ISO/IEC 7816-3.

TCS_04 Kortet ska fungera med Vcc = 3 V (±0,3 V) eller med Vcc = 5 V (±0,5 V).

Spänningen ska väljas i enlighet med ISO/IEC 7816-3.

2.2. **Programmeringsspänning V_{pp}**

TCS_05 Kortet får inte kräva en programmeringsspänning vid stift C6. Det förväntas att stift C6 inte är anslutet i en kortläsare. Kontakt C6 får anslutas till V_{cc} på kortet men får inte anslutas till jord. Denna spänning saknar betydelse.

2.3. **Klockgenerering och klockfrekvens**

TCS_06 Kortet ska fungera i frekvensintervallet 1–5 MHz, men får stödja högre klockfrekvenser. Inom en kortsession får klockfrekvensen variera med ± 2 %. Klockfrekvensen genereras av fordonsenheten och inte av själva kortet. Pulsförhållandet får variera mellan 40 och 60 %.

TCS_07 Den externa klockan kan stoppas, baserat på villkor som finns i kortfilen EF ICC. Villkoren för s.k. Clockstop-läge är kodade i första byte i nyttodelen (*body*) av EF ICC:

▼B

Låg	Hög		
Bit 3	Bit 2	Bit 1	
0	0	1	Clockstop tillåtet, ingen nivå föredras
0	1	1	Clockstop tillåtet, hög nivå föredras
1	0	1	Clockstop tillåtet, låg nivå föredras
0	0	0	Clockstop ej tillåtet
0	1	0	Clockstop endast tillåtet på hög nivå
1	0	0	Clockstop endast tillåtet på låg nivå

Bitarna 4 till 8 används inte.

2.4. **I/O-kontakt**

TCS_08 I/O-kontakt C7 används för att ta emot data från och överföra data till kortläsare. Antingen kortet eller kortläsaren ska vara i överföringsläge vid drift. Kortet ska inte ta skada om båda enheterna är i överföringsläge. När kortet inte överför ska det övergå till mottagningsläge.

2.5. **Kortets tillstånd**

TCS_09 Kortet fungerar i två olika tillstånd när det matas med spänning:

Drifttillstånd när kommandon utförs eller interaktion sker med en digital enhet.

Vilotillstånd vid alla övriga tillfällen; i detta läge ska kortet behålla alla data.

3. MASKINVARA OCH KOMMUNIKATION

3.1. **Inledning**

I denna punkt beskrivs den minsta funktionalitet som krävs av färdskrivarkort och fordonsenheter för att drift och driftskompatibilitet ska kunna säkerställas.

Färdskrivarkort ska överensstämma så långt som möjligt med tillgängliga tillämpliga ISO/IEC-normer (i synnerhet ISO/IEC 7816). Kommandon och protokoll beskrivs dock fullständigt för att viss begränsad användning eller vissa skillnader ska specificeras om de existerar. Specificerade kommandon överensstämmer till fullo med referensnormerna om inte annat anges.

3.2. **Överföringsprotokoll**

TCS_10 Överföringsprotokollet ska överensstämma med ISO/IEC 7816-3 för T=0 och T=1. I synnerhet ska fordonsenheten identifiera de förlängda väntetider som kortet sänder.

3.2.1 *Protokoll*

TCS_11 Kortet ska tillhandahålla både protokoll T=0 och protokoll T=1. Dessutom får kortet stödja ytterligare kontaktbaserade protokoll.

TCS_12 T=0 är standardprotokoll, och ett PTS-kommando behövs därför för att ändra protokollet till T=1.

▼B

TCS_13 Kortläsare ska klara **direkt konvention** i båda protokollen, och detta är således obligatoriskt för kortet.

TCS_14 Byte för IFSC (*Information Field Size Card*) ska visas med tecken TA3 vid ATR. Värdet ska vara minst ‘F0h’ (= 240 byte).

Följande begränsningar gäller för protokollen:

TCS_15 **T=0**

— Kortläsaren ska stödja ett svar på I/O efter den stigande kanten (rising edge) i signalen på RST från 400 cc.

— Kortläsaren ska kunna läsa tecken som är åtskilda med 12 etu.

— Kortläsaren ska läsa ett felaktigt tecken och upprepning av detta om de är åtskilda med 13 etu. Om ett felaktigt tecken upptäcks kan felsignalen på I/O inträffa mellan 1 etu och 2 etu. Anordningen ska stödja en fördröjning på 1 etu.

— Kortläsaren ska godta en ATR på 33 byte (TS+32).

— Om TC1 är närvarande i ATR ska extra vakttid (*Extra Guard Time*) vara närvarande för tecken som sänds av kortläsaren även om tecken som sänds av kortet fortfarande kan skiljas åt med 12 etu. Detta gäller också för det ACK-tecken som sänds av kortet efter ett P3-tecken som sänts ut av kortläsaren.

— Kortläsaren ska beakta ett NUL-tecken som sänds ut av kortet.

— Kortläsaren ska godta komplementläge (*complementary mode*) för ACK.

— Kommandot GET-RESPONSE (hämta svar) kan inte användas i kedjeläge (*chaining mode*) för att hämta data vars längd skulle kunna överstiga 255 byte.

TCS_16 **T=1**

— NAD-byte: används ej (NAD ska sättas till ‘00’).

— S-block, ABORT: används ej.

— S-block, feltillstånd för VPP (*VPP state error*): används ej.

— Den sammanlagda kedjelängden för ett datafält kommer inte att överstiga 255 byte (vilket ska säkerställas av kortläsaren (IFD).

— Kortläsarens storlek för informationsfält (IFSD) ska anges av kortläsaren omedelbart efter ATR: kortläsaren ska överföra begäran om S-Block för IFS (storlek för informationsfält) efter ATR och kortet ska sända tillbaka S-Block för IFS. Det rekommenderade värdet på IFSD är 254 byte.

— Kortet kommer inte att fråga efter en justering av IFS.

▼B

3.2.2 *ATR*

TCS_17 Anordningen kontrollerar ATR-byte enligt ISO/IEC 7816-3. Ingen verifiering ska göras av *ATR Historical Characters*.

Exempel på *Basic Biprotocol ATR* enligt ISO/IEC 7816-3

Tecken	Värde	Anmärkningar
TS	‘3Bh’	Indikerar direkt kommunikation (*direct convention*)
T0	‘85h’	TD1 närvarande, 5 historiska byte närvarande
TD1	‘80h’	TD2 närvarande, T=0 ska användas
TD2	‘11h’	TA3 närvarande, T=1 ska användas
TA3	‘XXh’ (minst ‘F0h’)	Information Field Size Card (IFSC)
TH1 till TH5	‘XXh’	Historiska tecken
TCK	‘XXh’	Kontrolltecken (XOR)

TCS_18 Efter ATR väljs huvudfilen (MF) indirekt och blir aktuell katalog (*Current Directory*).

3.2.3 *PTS*

TCS_19 Standardprotokollet är T=0. För att sätta protokollet T=1 måste en PTS (även kallad PPS) sändas till kortet av anordningen.

TCS_20 Eftersom både protokoll T=0 och protokoll T=1 är obligatoriska för kortet är grundläggande PTS (*basic PTS*) för protokollväxling obligatorisk för kortet.

Som anges i ISO/IEC 7816-3, kan PTS användas för att byta till högre överföringshastigheter än den förvalda som föreslås av kortet i ATR i förekommande fall (TA(1)-byte).

Högre överföringshastigheter är valfria för kortet.

TCS_21 Om ingen annan överföringshastighet än den förvalda stöds (eller om den valda överföringshastigheten inte stöds), ska kortet svara korrekt på PTS enligt ISO/IEC 7816-3 genom att utelämna PPS1-byte.

Exempel på grundläggande PTS för protokollval är följande:

Tecken	Värde	Anmärkningar
PPSS	‘FFh’	Initialt tecken
PPS0	‘00h’ eller ‘01h’	PPS1 till PPS3 används inte; ‘00h’ för att välja T0, ‘01h’ för att välja T1.
PK	‘XXh’	Kontrolltecken: ‘XXh’ = ‘FFh’ om PPS0 = ‘00h’, ‘XXh’ = ‘FEh’ om PPS0 = ‘01h’.

▼B

3.3. **Tillträdesregler**

TCS_22 En tillträdesregel anger säkerhetsvillkoren för ett åtkomstläge, dvs. ett kommando. Om dessa säkerhetsvillkor är uppfyllda behandlas det aktuella kommandot.

TCS_23 Följande säkerhetsvillkor används för färdskrivarkortet:

Förkortning	Betydelse
ALW	Åtgärden är alltid möjlig och kan utföras utan någon begränsning. Kommando och svar (APDU) sänds i klartext, dvs. utan säker meddelandehantering.
NEV	Åtgärden är aldrig möjlig.
PLAIN-C	APDU för kommandot sänds i klartext, dvs. utan säker meddelandehantering.
PWD	Åtgärden får endast verkställas om verkstadskortets PIN-kod har kontrollerats med positivt resultat, dvs. om kortets interna säkerhetsstatus ”PIN_Verified” har satts. Kommandot måste skickas utan säker meddelandehantering.
EXT-AUT-G1	Åtgärden får endast verkställas om kommandot EXTERNAL AUTHENTICATE för autentiseringen (generation 1) (se även del A i tillägg 11) har utförts med positivt resultat.
SM-MAC-G1	APDU (kommando och svar) måste användas med säker meddelandehantering (generation 1) i läge för endast autentisering (*authentication-only mode*) (se del A i tillägg 11).
SM-C-MAC-G1	APDU för kommandot måste användas med säker meddelandehantering (generation 1) i läge för endast autentisering (*authentication-only mode*) (se del A i tillägg 11).
SM-R-ENC-G1	APDU för svaret måste användas med säker meddelandehantering (generation 1) i krypteringsläge (*encryption mode*) (se del A i tillägg 11), dvs ingen kod för meddelandeautentisering (MAC) återsänds.
SM-R-ENC-MAC-G1	APDU för svaret måste användas med säker meddelandehantering (generation 1) i läge för kryptering följd av autentisering (*encrypt-then-authenticate mode*) (se del A i tillägg 11).
SM-MAC-G2	APDU (kommando och svar) måste användas med säker meddelandehantering (generation 2) i läge för endast autentisering (*authentication-only mode*) (se del B i tillägg 11).
SM-C-MAC-G2	APDU för kommandot måste användas med säker meddelandehantering (generation 2) i läge för endast autentisering (*authentication-only mode*) (se del B i tillägg 11).
SM-R-ENC-MAC-G2	APDU för svaret måste användas med säker meddelandehantering (generation 2) i läge för kryptering följd av autentisering (*encrypt-then-authenticate mode*) (se del B i tillägg 11).

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.

▼B

TCS_25 För tillämpningen i DF Tachograph_G1 används följande tillträdesregler:

Kommando	Förarkort	Verkstadskort	Kontrollkort	Företagskort
EXTERNAL AUTHENTICATE				
— För autentisering (generation 1)	ALW	ALW	ALW	ALW
— För autentisering (generation 2)	ALW	PWD	ALW	ALW
INTERNAL AUTHENTICATE	ALW	PWD	ALW	ALW
GENERAL AUTHENTICATE	ALW	ALW	ALW	ALW
GET CHALLENGE	ALW	ALW	ALW	ALW
MSE:SET AT	ALW	ALW	ALW	ALW
MSE:SET DST	ALW	ALW	ALW	ALW
PROCESS DSRC MESSAGE	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
PSO: 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

TCS_26 För tillämpningen i DF Tachograph_G2 används följande tillträdesregler:

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

▼B

Kommando	Förarkort	Verkstadskort	Kontrollkort	Företagskort
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
PSO: 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

TCS_27 I MF används följande tillträdesregler:

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

▼B

Kommando	Förarkort	Verkstadskort	Kontrollkort	Företagskort
PSO: COMPUTE DIGITAL SIGNATURE	Ej tillämpligt	Ej tillämpligt	Ej tillämpligt	Ej tillämpligt
PSO: Hash	Ej tillämpligt	Ej tillämpligt	Ej tillämpligt	Ej tillämpligt
PSO: HASH OF FILE	Ej tillämpligt	Ej tillämpligt	Ej tillämpligt	Ej tillämpligt
PSO: VERIFY CERTIFICATE	ALW	ALW	ALW	ALW
VERIFY	Ej tillämpligt	ALW	Ej tillämpligt	Ej tillämpligt

TCS_28 Ett färdskrivarkort kan – men måste inte – acceptera ett kommando med en högre säkerhetsnivå än den som anges i säkerhetsvillkoren. Dvs. om säkerhetsvillkoret är ALW (eller PLAIN-C) kan kortet acceptera ett kommando med säker meddelandehantering (krypterings- och/eller autentiseringsläge). Om säkerhetsvillkoret kräver säker meddelandehantering med autentiseringsläge kan färdskrivarkortet acceptera ett kommando med säker meddelandehantering av samma generation i autentiserings- och krypteringsläge.

Anmärkning: Kommandobeskrivningarna ger mer information om hur kommandona stöder de olika typerna av färdskrivarkort och de olika dedikerade filerna (DF).

3.4. **Översikt av kommandon och felkoder**

Kommandon och filorganisation härleds från och överensstämmer med ISO/IEC 7816-4.

Denna del innehåller en beskrivning av följande APDU-par (kommando och svar): De kommandovarianter som stöds av en tillämpning i generation 1 och generation 2 specificeras i motsvarande kommandobeskrivningar.

Kommando	INS
SELECT	‘A4h’
READ BINARY	‘B0h’, ‘B1h’
UPDATE BINARY	‘D6h’, ‘D7h’
GET CHALLENGE	‘84h’
VERIFY	‘20h’
GET RESPONSE	‘C0h’
PERFORM SECURITY OPERATION	‘2Ah’

▼B

Kommando	INS
— VERIFY CERTIFICATE	
— COMPUTE DIGITAL SIGNATURE	
— VERIFY DIGITAL SIGNATURE	
— HASH	
— PERFORM HASH OF FILE	
— PROCESS DSRC MESSAGE	
INTERNAL AUTHENTICATE	‘88h’
EXTERNAL AUTHENTICATE	‘82h’
MANAGE SECURITY ENVIRONMENT	‘22h’
— SET DIGITAL SIGNATURE TEMPLATE	
— SET AUTHENTICATION TEMPLATE	
GENERAL AUTHENTICATE	‘86h’

TCS_29 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’.
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).

▼B

SW1	SW2	Betydelse
68	82	Säker meddelandehantering stöds inte.
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.
6 B	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.

TCS_30 Om fler än ett felvillkor är uppfyllda i ett APDU-kommando kan kortet återsända någon av de tillämpliga koderna som statusregister.

3.5. **Kommandobeskrivning**

Detta kapitel innehåller en beskrivning av de obligatoriska kommandona för färdskrivarkort.

Närmare uppgifter om krypteringsoperationer som är aktuella återfinns i tillägg 11 om gemensamma säkerhetsmekanismer för färdskrivare (generation 1 och generation 2).

Alla kommandon beskrivs oberoende av använt protokoll (T=0 eller T=1). APDU-byte CLA, INS, P1, P2, Lc och Le anges alltid. Om Lc eller Le inte krävs för det kommando som beskrivs är tillhörande längd, värde och beskrivning tomma.

TCS_31 Om båda byte för längd (Lc och Le) begärs måste det kommando som beskrivs delas i två delar om kortläsaren använder protokollet T=0: kortläsaren skickar kommandot enligt beskrivningen med P3=Lc + data och skickar därefter kommandot GET RESPONSE (se avsnitt 3.5.6) med P3=Le.

TCS_32 Om båda byte för längd begärs och Le=0 (säker meddelandehantering):

▼B

— När protokollet T=1 används, ska kortet svara på Le=0 genom att sända alla tillgängliga utdata.

— När protokollet T=0 används, ska kortläsaren sända det första kommandot med P3=Lc + data, och kortet ska svara (på detta indirekta Le=0) genom byte för status '**61La**', där La är antal tillgängliga byte för svar. Kortläsaren ska sedan generera ett GET RESPONSE-kommando med P3 = La för att läsa dessa data.

TCS_33 Ett färdskrivarkort får stödja fält med utökad längd enligt ISO/IEC 7816-4 som en tillvalsfunktion. Ett färdskrivarkort som stöder fält med utökad längd ska

— ange stödet för fält med utökad längd i ATR,

— ange de buffertstorlekar som stöds med hjälp av informationen om utökad längd i EF ATR/INFO (se TCS_146),

— ange om det stöder fält med utökad längd för T=1 och/eller T=0 i EF Extended Length (se TCS_147),

— stödja fält med utökad längd för färdskrivartillämpningar (generation 1 och 2).

Anmärkningar:

Alla kommandon beskrivs för fält med kort längd. Hur dataenheter (APDU) med utökad längd ska användas framgår av ISO/IEC 7816-4.

I allmänhet beskrivs kommandona för "klarläge" (*plain mode*), dvs. utan säker meddelandehantering, eftersom säker meddelandehantering beskrivs i tillägg 11. Det framgår av tillträdesreglerna för ett kommando om kommandot ska stödja säker meddelandehantering eller inte och om kommandot ska stödja säker meddelandehantering (generation 1 och/eller generation 2). Vissa kommandovarianter beskrivs med säker meddelandehantering för att åskådliggöra användningen av säker meddelandehantering.

TCS_34 Fordonsenheten ska använda det fullständiga protokollet för ömsesidig autentisering mellan fordonsenhet (generation 2) och kort för en session, inbegripet verifieringen av certifikat (om detta krävs), antingen i DF Tachograph, DF Tachograph_G2 eller MF.

3.5.1 *SELECT*

Detta kommando överensstämmer med ISO/IEC 7816-4, men det har en begränsad användning jämfört med det kommando som definieras i normen.

Kommandot SELECT används

— för att välja DF för en tillämpning (val genom namn krävs),

— för att välja en elementfil som motsvarar det fil-ID som angetts.

3.5.1.1 Val genom namn (AID – tillämpningsidentifierare)

Detta kommando gör det möjligt att välja DF för en tillämpning på kortet.

TCS_35 Detta kommando kan utföras från vilken plats som helst i filstrukturen (efter ATR eller när som helst).

▼B

TCS_36 Vid valet av tillämpning nollställs den aktuella säkerhetsmiljön (*security environment*). Efter det att en tillämpning valts är inte längre någon aktuell öppen nyckel utvald. Tillträdesvillkoret EXT-AUT-G1 förloras också. Om kommandot utfördes utan säker meddelandehantering är de tidigare sessionsnycklarna för säker meddelandehantering inte längre tillgängliga.

TCS_37 **Kommandomeddelande**

Byte	Längd	Värde	Beskrivning
CLA	1	‘00h’	
INS	1	‘A4h’	
P1	1	‘04h’	Val genom namn (AID – tillämpningsidentifierare)
P2	1	‘0Ch’	Inget svar förväntas
Lc	1	‘NNh’	Antal byte som sänds till kortet (längd på AID): ‘06h’ för färdskrivartillämpningen
#6-#(5+NN)	NN	‘XX..XXh’	AID: ‘FF 54 41 43 48 4F’ för färdskrivartillämpningen (generation 1) AID: ‘FF 53 4D 52 44 54’ för färdskrivartillämpningen (generation 2)

Inget svar på kommandot SELECT behövs (Le frånvarande i T=1, eller inget svar efterfrågas i T=0).

TCS_38 **Svarsmeddelande (inget svar efterfrågas)**

Byte	Längd	Värde	Beskrivning
SW	2	‘XXXXh’	Statusregister (SW1,SW2)

— Om kommandot lyckas återsänder kortet ‘**9000**’.

— Om den tillämpning som motsvarar AID inte kan hittas, återsänds bearbetningsstatus (*processing state*) ‘**6A82**’.

— För T=1, om byte Le är närvarande, återsänds status ‘**6700**’.

— För T=0, om ett svar efterfrågas efter kommandot SELECT, återsänds status ‘**6900**’.

— Om den valda tillämpningen anses korrupt (integritetsfel upptäcks i filattributen), återsänds bearbetningsstatus ‘**6400**’ eller ‘**6581**’.

3.5.1.2 Val av en elementfil med hjälp av dess filidentifierare

TCS_39 **Kommandomeddelande**

TCS_40 Ett färdskrivarkort ska stödja säker meddelandehantering (generation 2) i enlighet med del B i tillägg 11 för denna kommandovariant.

Byte	Längd	Värde	Beskrivning
CLA	1	‘00h’	
INS	1	‘A4h’	
P1	1	‘02h’	Val av en elementfil under aktuell DF

▼B

Byte	Längd	Värde	Beskrivning
P2	1	‘0Ch’	Inget svar förväntas
Lc	1	‘02h’	Antal byte som sänds till kortet
#6-#7	2	‘XXXXh’	Filidentifierare

Inget svar på kommandot SELECT behövs (Le frånvarande i T=1, eller inget svar efterfrågas i T=0).

TCS_41 **Svarsmeddelande (inget svar efterfrågas)**

Byte	Längd	Värde	Beskrivning
SW	2	‘XXXXh’	Statusregister (SW1,SW2)

— Om kommandot lyckas återsänder kortet ‘**9000**’.

— Om den fil som motsvarar filidentifieraren inte kan hittas, återsänds bearbetningsstatus ‘**6A82**’.

— För T=1, om byte Le är närvarande, återsänds status ‘**6700**’.

— För T=0, om ett svar efterfrågas efter kommandot SELECT, återsänds status ‘**6900**’.

— Om den valda filen anses vara skadad (integritetsfel upptäcks i filattributen), återsänds bearbetningsstatus ‘**6400**’ eller ‘**6581**’.

3.5.2 *READ BINARY*

Detta kommando överensstämmer med ISO/IEC 7816-4, men det har en begränsad användning jämfört med det kommando som definieras i normen.

Kommandot READ BINARY används för att läsa data från en transparent fil.

Svaret från kortet består i att lästa data återsänds, eventuellt inkapslade i en struktur för säker meddelandehantering.

3.5.2.1 Kommando med offset i P1-P2

Detta kommando gör det möjligt för kortläsare att läsa data från den elementfil som för närvarande är vald, utan säker meddelandehantering.

Anmärkning: Detta kommando utan säker meddelandehantering kan endast användas för att läsa en fil som stöder säkerhetsvillkoret ALW för åtkomstläget för läsning (*read*).

TCS_42 **Kommandomeddelande**

Byte	Längd	Värde	Beskrivning
CLA	1	‘00h’	
INS	1	‘B0h’	READ BINARY
P1	1	‘XXh’	Offset i byte från början av filen: Mest signifikanta byte

▼B

Byte	Längd	Värde	Beskrivning
P2	1	‘XXh’	Offset i byte från början av filen: Minst signifikanta byte
Le	1	‘XXh’	Längd på förväntade data. Antal byte som ska läsas

Anmärkning: bit 8 i P1 måste sättas till 0.

TCS_43 **Svarsmeddelande**

Byte	Längd	Värde	Beskrivning
#1-#X	X	‘XX..XXh’	Lästa data
SW	2	‘XXXXh’	Statusregister (SW1,SW2)

— Om kommandot lyckas återsänder kortet ‘**9000**’.

— Om ingen elementfil väljs återsänds bearbetningsstatus ‘**6986**’.

— Om säkerhetsvillkoren för den valda filen inte uppfylls, avbryts kommandot med ‘**6982**’.

— Om offset inte överensstämmer med storleken på elementfilen (*Offset > EF size*), återsänds bearbetningsstatus ‘**6B00**’.

— Om storleken på de data som ska läsas inte överensstämmer med storleken på elementfilen (*Offset + Le > EF size*) återsänds bearbetningsstatus ‘**6700**’ eller ‘**6Cxx**’, där ‘xx’ avser den exakta längden.

— Om ett integritetsfel upptäcks i filattributen, ska kortet anse filen vara skadad och omöjlig att återställa, och återsända bearbetningsstatus ‘**6400**’ eller ‘**6581**’.

— Om ett integritetsfel upptäcks i lagrade data, ska kortet återsända begärda data, och bearbetningsstatus ‘**6281**’ ska återsändas.

3.5.2.1.1 Kommando med säker meddelandehantering (exempel)

Detta kommando gör det möjligt för kortläsare att läsa data från den elementfil som för närvarande är vald med säker meddelandehantering, för att verifiera integriteten hos de data som tas emot och för att skydda sekretessen hos dem om säkerhetsvillkoret SM-R-ENC-MAC-G1 (generation 1) eller SM-R-ENC-MAC-G2 (generation 2) tillämpas.

TCS_44 **Kommandomeddelande**

Byte	Längd	Värde	Beskrivning
CLA	1	‘0Ch’	Säker meddelandehantering efterfrågad
INS	1	‘B0h’	READ BINARY
P1	1	‘XXh’	P1 (offset i byte från början av filen): Mest signifikanta byte
P2	1	‘XXh’	P2 (offset i byte från början av filen): Minst signifikanta byte

▼B

Byte	Längd	Värde	Beskrivning
Lc	1	‘XXh’	Längd på indata för säker meddelandehantering
#6	1	‘97h’	T_{LE}: Tagg för specificering av förväntad längd
#7	1	‘01h’	L_{LE}: Längd på förväntad längd
#8	1	‘NNh’	Specificering av förväntad längd (ursprunglig Le): Antal byte som ska läsas
#9	1	‘8Eh’	T_{CC}: Tagg för kryptografisk kontrollsumma
#10	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)
#11-#(10+L)	L	‘XX..XXh’	Kryptografisk kontrollsumma
Le	1	‘00h’	Enligt ISO/IEC 7816-4

TCS_45 **Svarsmeddelande om SM-R-ENC-MAC-G1 (generation 1) / SM-R-ENC-MAC-G2 (generation 2) inte krävs och om indataformatet för säker meddelandehantering är korrekt:**

Byte	Längd	Värde	Beskrivning
#1	1	‘99h’	Tagg för bearbetningsstatus (SW1-SW2) – frivillig uppgift för säker meddelandehantering (generation 1)
#2	1	‘02h’	Längd för bearbetningsstatus
#3 – #4	2	‘XX XXh’	Bearbetningsstatus för APDU för oskyddat svar
#5	1	‘81h’	T_{PV}: Tagg för data med klarvärde
#6	L	‘NNh’ eller ‘81 NNh’	L_{PV}: längd på återsända data (= ursprunglig Le). L är 2 byte om L_{PV} > 127 byte.
#(6+L)-#(5+L+NN)	NN	‘XX..XXh’	Data med klarvärde
#(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)
#(8+L+NN)-#(7+M+L+NN)	M	‘XX..XXh’	Kryptografisk kontrollsumma
SW	2	‘XXXXh’	Statusregister (SW1,SW2)

▼B

TCS_46 **Svarsmeddelande om SM-R-ENC-MAC-G1 (generation 1) / SM-R-ENC-MAC-G2 (generation 2) krävs och om indataformatet för säker meddelandehantering är korrekt:**

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
#(4+L+MM) – #(5+L+MM)	2	‘XX XXh’	Bearbetningsstatus för APDU för oskyddat svar
#(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)

Kommandot READ BINARY kan återsända normal bearbetningsstatus som förtecknas i TCS_43 under taggen ‘99h’ enligt beskrivningen i TCS_59 med hjälp av svarsstrukturen för säker meddelandehantering.

Vissa fel, som specifikt kan hänföras till säker meddelandehantering, kan inträffa. I så fall återsänds helt enkelt bearbetningsstatusen utan någon struktur för säker meddelandehantering.

TCS_47 **Svarsmeddelande om indataformatet för säker meddelandehantering är inkorrekt**

Byte	Längd	Värde	Beskrivning
SW	2	‘XXXXh’	Statusregister (SW1,SW2)

— Om ingen aktuell sessionsnyckel finns tillgänglig återsänds bearbetningsstatus ‘**6A88**’. Detta inträffar antingen om sessionsnyckeln ännu inte har genererats eller om giltigheten för sessionsnyckeln har utgått (i detta fall måste kortläsaren upprepa en ömsesidig autentiseringsprocess för att bestämma en ny sessionsnyckel).

▼B

— Om vissa förväntade dataobjekt (enligt specifikation ovan) saknas i formatet för säker meddelandehantering återsänds bearbetningsstatus ‘**6987**’: detta fel inträffar om en förväntad tagg saknas eller om kommandots nyttodel (*body*) inte är rätt konstruerad.

— Om vissa data är felaktiga återsänds bearbetningsstatus ‘**6988**’: detta fel inträffar om alla nödvändiga taggar är närvarande men vissa längder skiljer sig från vad som förväntas.

— Om verifieringen av den kryptografiska kontrollsumman misslyckas, återsänds bearbetningsstatus ‘**6688**’.

3.5.2.2 Kommando med kort identifierare för elementfil (SFID)

Denna kommandovariant gör det möjligt för kortläsaren att välja en elementfil med hjälp av en kort identifierare för elementfil och läsa data från den elementfilen.

TCS_48 Ett färdskrivarkort ska stödja denna kommandovariant för alla elementfiler med en angiven kort identifierare för elementfil. Dessa korta identifierare för elementfil specificeras i kapitel 4.

TCS_49 **Kommandomeddelande**

Byte	Längd	Värde	Beskrivning
CLA	1	‘00h’	
INS	1	‘B0h’	READ BINARY
P1	1	‘XXh’	Bit 8 sätts till 1 Bitarna 7 och 6 sätts till 00 Bitarna 5–1 kodar den korta identifieraren för motsvarande elementfil
P2	1	‘XXh’	Kodar en offset från 0 till 255 byte i den elementfil anges i P1
Le	1	‘XXh’	Längd på förväntade data. Antal byte som ska läsas.

Anmärkning: De korta identifierare för elementfil vilka används för färdskrivartillämpningen (generation 2) specificeras i kapitel 4.

Om P1 kodar en kort identifierare för elementfil och kommandot lyckas blir den identifierade elementfilen aktuell elementfil (*current EF*).

TCS_50 **Svarsmeddelande**

Byte	Längd	Värde	Beskrivning
#1-#L	L	‘XX..XXh’	Lästa data
SW	2	‘XXXXh’	Statusregister (SW1,SW2)

— Om kommandot lyckas återsänder kortet ‘**9000**’.

— Om den fil som motsvarar den korta identifieraren för elementfil inte kan hittas, återsänds bearbetningsstatus ‘**6A82**’.

— Om säkerhetsvillkoren för den valda filen inte uppfylls, avbryts kommandot med ‘**6982**’.

▼B

— Om offset inte överensstämmer med storleken på elementfilen (*Offset > EF size*), återsänds bearbetningsstatus ‘**6B00**’.

— Om storleken på de data som ska läsas inte överensstämmer med storleken på elementfilen (*Offset + Le > EF size*) återsänds bearbetningsstatus ‘**6700**’ eller ‘**6Cxx**’, där ‘xx’ avser den exakta längden.

— Om ett integritetsfel upptäcks i filattributen, ska kortet anse filen vara skadad och omöjlig att återställa, och återsända bearbetningsstatus ‘**6400**’ eller ‘**6581**’.

— Om ett integritetsfel upptäcks i lagrade data, ska kortet återsända begärda data, och bearbetningsstatus ‘**6281**’ ska återsändas.

3.5.2.3 Kommando med udda INS-byte (instruktion)

Denna kommandovariant gör det möjligt för kortläsaren att läsa data från en EF med 32 768 byte eller mer.

TCS_51 Ett färdskrivarkort som stöder EF med 32 768 byte eller mer ska stödja denna kommandovariant för dessa EF. Ett färdskrivarkort kan klara, men måste inte klara, denna kommandovariant, med undantag för EF Sensor_Installation_Data (se TCS_156 och TCS_160).

TCS_52 **Kommandomeddelande**

Byte	Längd	Värde	Beskrivning
CLA	1	‘00h’	
INS	1	‘B1h’	READ BINARY
P1	1	‘00h’	Aktuell elementfil
P2	1	‘00h’	
Lc	1	‘NNh’	Längd på offsetdataobjekt.
#6-#(5+NN)	NN	‘XX..XXh’	Offsetdataobjekt: Tagg ‘54h’ Längd ‘01h’ eller ‘02h’ Värde offset
Le	1	‘XXh’	Antal byte som ska läsas.

Kortläsaren ska koda offsetdataobjektets längd med ett minsta möjliga antal oktetter, dvs. med hjälp av byte för längd ‘01h’ ska kortläsare koda en offset från 0 till 255 och med hjälp av byte för längd ‘02h’ en offset från 256 upp till 65 535 byte.

TCS_53 **Svarsmeddelande**

Byte	Längd	Värde	Beskrivning
#1-#L	L	‘XX..XXh’	Lästa data inkapslade i ett godtyckligt (*discretionary*) dataobjekt med taggen ‘53h’.
SW	2	‘XXXXh’	Statusregister (SW1,SW2)

▼B

— Om kommandot lyckas återsänder kortet ‘**9000**’.

— Om ingen elementfil väljs återsänds bearbetningsstatus ‘**6986**’.

— Om säkerhetsvillkoren för den valda filen inte uppfylls, avbryts kommandot med ‘**6982**’.

— Om offseten inte överensstämmer med storleken på elementfilen (Offset > EF size), återsänds bearbetningsstatus ‘**6B00**’.

— Om storleken på de data som ska läsas inte överensstämmer med storleken på elementfilen (Offset + Le > EF size) återsänds bearbetningsstatus ‘**6700**’ eller ‘**6Cxx**’, där ‘xx’ avser den exakta längden.

— Om ett integritetsfel upptäcks i filattributen, ska kortet anse filen vara skadad och omöjlig att återställa, och återsända bearbetningsstatus ‘**6400**’ eller ‘**6581**’.

— Om ett integritetsfel upptäcks i lagrade data, ska kortet återsända begärda data, och bearbetningsstatus ‘**6281**’ ska återsändas.

3.5.2.3.1 Kommando med säker meddelandehantering (exempel)

Följande exempel åskådliggör användningen av säker meddelandehantering om säkerhetsvillkoret SM-MAC-G2 tillämpas.

TCS_54 Kommandomeddelande

Byte	Längd	Värde	Beskrivning
CLA	1	‘0Ch’	Säker meddelandehantering efterfrågad
INS	1	‘B1h’	READ BINARY
P1	1	‘00h’	Aktuell elementfil
P2	1	‘00h’	
Lc	1	‘XXh’	Fältlängd för skyddade data
#6	1	‘B3h’	Tagg för BER-TLV-kodade data med klarvärde
#7	1	‘NNh’	L_{PV}: Längd på överförda data
#(8)-#(7+NN)	NN	‘XX..XXh’	BER-TLV-kodade data med klarvärde, dvs. offsetdata-objektet med taggen ‘54’
#(8+NN)	1	‘97h’	T_{LE}: Tagg för specificering av förväntad längd
#(9+NN)	1	‘01h’	L_{LE}: Längd på förväntad längd
#(10+NN)	1	‘XXh’	Specificering av förväntad längd (ursprunglig Le): Antal byte som ska läsas
#(11+NN)	1	‘8Eh’	T_{CC}: Tagg för kryptografisk kontrollsumma
#(12+NN)	1	‘XXh’	L_{CC}: Längd på efterföljande kryptografiska kontrollsumma: ‘08h’, ‘0Ch’ eller ‘10h’ beroende på AES-nyckelns längd för säker meddelandehantering (generation 2) (se del B i tillägg 11)
#(13+NN)-#(12+M+NN)	M	‘XX..XXh’	Kryptografisk kontrollsumma
Le	1	‘00h’	Enligt ISO/IEC 7816-4

▼B

TCS_55 Svarsmeddelande om kommandot lyckas

Byte	Längd	Värde	Beskrivning
#1	1	‘B3h’	BER-TLV-kodade 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’	BER-TLV-kodade data med klarvärde, dvs. lästa data inkapslade i ett godtyckligt (*discretionary*) dataobjekt med taggen ‘53h’.
#(2+L+NN)	1	‘99h’	Bearbetningsstatus för APDU för oskyddat svar
#(3+L+NN)	1	‘02h’	Längd för bearbetningsstatus
#(4+L+NN) – #(5+L+NN)	2	‘XX XXh’	Bearbetningsstatus för APDU för oskyddat svar
#(6+L+NN)	1	‘8Eh’	T_{CC}: Tagg för kryptografisk kontrollsumma
#(7+L+NN)	1	‘XXh’	L_{CC}: Längd på efterföljande kryptografiska kontrollsumma: ‘08h’, ‘0Ch’ eller ‘10h’ beroende på AES-nyckelns längd för säker meddelandehantering (generation 2) (se del B i tillägg 11)
#(8+L+NN)-#(7+M+L+NN)	M	‘XX..XXh’	Kryptografisk kontrollsumma
SW	2	‘XXXXh’	Statusregister (SW1,SW2)

3.5.3 *UPDATE BINARY*

Detta kommando överensstämmer med ISO/IEC 7816-4, men det har en begränsad användning jämfört med det kommando som definieras i normen.

Kommandomeddelandet UPDATE BINARY initierar uppdateringen (*erase+write*) av de bitar som redan finns närvarande i en binär elementfil med bitar givna i dataenheten (APDU) för kommandot.

3.5.3.1 Kommando med offset i P1-P2

Detta kommando gör det möjligt för kortläsare att skriva data i den elementfil som för närvarande är vald, utan att kortet verifierar integriteten hos mottagna data.

Anmärkning: Detta kommando utan säker meddelandehantering kan endast användas för att uppdatera en fil som stöder säkerhetsvillkoret ALW för åtkomstläget för uppdatering (*update*).

TCS_56 **Kommandomeddelande**

Byte	Längd	Värde	Beskrivning
CLA	1	‘00h’	
INS	1	‘D6h’	UPDATE BINARY
P1	1	‘XXh’	Offset i byte från början av filen: Mest signifikanta byte
P2	1	‘XXh’	Offset i byte från början av filen: Minst signifikanta byte

▼B

Byte	Längd	Värde	Beskrivning
Lc	1	‘NNh’	Längd på data som ska uppdateras. Antal byte som ska skrivas.
#6-#(5+NN)	NN	‘XX..XXh’	Data som ska skrivas

Anmärkning: bit 8 i P1 måste sättas till 0.

TCS_57 **Svarsmeddelande**

Byte	Längd	Värde	Beskrivning
SW	2	‘XXXXh’	Statusregister (SW1,SW2)

— Om kommandot lyckas återsänder kortet ‘**9000**’.

— Om ingen elementfil väljs återsänds bearbetningsstatus ‘**6986**’.

— Om säkerhetsvillkoren för den valda filen inte uppfylls, avbryts kommandot med ‘**6982**’.

— Om offset inte överensstämmer med storleken på elementfilen (*Offset > EF size*), återsänds bearbetningsstatus ‘**6B00**’.

— Om storleken på de data som ska skrivas inte överensstämmer med storleken på elementfilen (Offset + Lc > EF size) återsänds bearbetningsstatus ‘**6700**’.

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

— Om det inte går att skriva data, återsänds bearbetningsstatus ‘**6581**’.

3.5.3.1.1 Kommando med säker meddelandehantering (exempel)

Detta kommando gör det möjligt för kortläsaren att skriva data i den elementfil som för närvarande är vald, varvid kortet verifierar integriteten hos mottagna data. Eftersom ingen sekretess krävs ska dessa data inte krypteras.

TCS_58 **Kommandomeddelande**

Byte	Längd	Värde	Beskrivning
CLA	1	‘0Ch’	Säker meddelandehantering efterfrågad
INS	1	‘D6h’	UPDATE BINARY
P1	1	‘XXh’	Offset i byte från början av filen: Mest signifikanta byte
P2	1	‘XXh’	Offset i byte från början av filen: Minst signifikanta byte
Lc	1	‘XXh’	Fältlängd för skyddade data
#6	1	‘81h’	T_{PV}: Tagg för data med klarvärde
#7	L	‘NNh’ eller ‘81 NNh’	L_{PV}: längd på överförda data L är 2 byte om L_{PV} > 127 byte.

▼B

Byte	Längd	Värde	Beskrivning
#(7+L)-#(6+L+NN)	NN	‘XX..XXh’	Data med klarvärde (data som ska skrivas)
#(7+L+NN)	1	‘8Eh’	T_{CC}: Tagg för kryptografisk kontrollsumma
#(8+L+NN)	1	‘XXh’	L_{CC}: Längd på efterföljande kryptografisk 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)
#(9+L+NN)-#(8+M+L+NN)	M	‘XX..XXh’	Kryptografisk kontrollsumma
Le	1	‘00h’	Enligt ISO/IEC 7816-4

TCS_59 **Svarsmeddelande om indataformatet för säker meddelandehantering är korrekt**

Byte	Längd	Värde	Beskrivning
#1	1	‘99h’	T_{SW}: Tagg för statusregister (ska skyddas av CC)
#2	1	‘02h’	L_{SW}: längd på återsända statusregister
#3-#4	2	‘XXXXh’	Bearbetningsstatus för APDU för oskyddat svar
#5	1	‘8Eh’	T_{CC}: Tagg för kryptografisk kontrollsumma
#6	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)
#7-#(6+L)	L	‘XX..XXh’	Kryptografisk kontrollsumma
SW	2	‘XXXXh’	Statusregister (SW1,SW2)

”Normal” bearbetningsstatus, som beskrivs för kommandot UPDATE BINARY utan säker meddelandehantering (se avsnitt 3.5.3.1), kan återsändas med hjälp av den struktur för svarsmeddelanden som beskrivs ovan.

Vissa fel, som specifikt kan hänföras till säker meddelandehantering, kan inträffa. I så fall återsänds helt enkelt bearbetningsstatusen utan någon struktur för säker meddelandehantering.

TCS_60 **Svarsmeddelande vid fel i den säkra meddelandehanteringen**

Byte	Längd	Värde	Beskrivning
SW	2	‘XXXXh’	Statusregister (SW1,SW2)

▼B

— Om ingen aktuell sessionsnyckel finns tillgänglig återsänds bearbetningsstatus ‘**6A88**’.

— Om vissa förväntade dataobjekt (enligt specifikation ovan) saknas i formatet för säker meddelandehantering återsänds bearbetningsstatus ‘**6987**’: detta fel inträffar om en förväntad tagg saknas eller om kommandots nyttodel (*body*) inte är rätt konstruerad.

— Om vissa data är felaktiga återsänds bearbetningsstatus ‘**6988**’: detta fel inträffar om alla nödvändiga taggar är närvarande men vissa längder skiljer sig från vad som förväntas.

— Om verifieringen av den kryptografiska kontrollsumman misslyckas, återsänds bearbetningsstatus ‘**6688**’.

3.5.3.2 Kommando med kort identifierare för elementfil

Denna kommandovariant gör det möjligt för kortläsaren att välja en elementfil med hjälp av en kort identifierare för elementfil och skriva data från den elementfilen.

TCS_61 Ett färdskrivarkort ska stödja denna kommandovariant för alla elementfiler med en angiven kort identifierare för elementfil. Dessa korta identifierare för elementfil specificeras i kapitel 4.

TCS_62 **Kommandomeddelande**

Byte	Längd	Värde	Beskrivning
CLA	1	‘00h’	
INS	1	‘D6h’	UPDATE BINARY
P1	1	‘XXh’	Bit 8 sätts till 1 Bitarna 7 och 6 sätts till 00 Bitarna 5–1 kodar den korta identifieraren för motsvarande elementfil
P2	1	‘XXh’	Kodar en offset från 0 till 255 byte i den elementfil anges i P1
Lc	1	‘NNh’	Längd på data som ska uppdateras. Antal byte som ska skrivas.
#6-#(5+NN)	NN	‘XX..XXh’	Data som ska skrivas

TCS_63 **Svarsmeddelande**

Byte	Längd	Värde	Beskrivning
SW	2	‘XXXXh’	Statusregister (SW1,SW2)

Anmärkning: De korta identifierare för elementfil vilka används för färdskrivartillämpningen (generation 2) specificeras i kapitel 4.

Om P1 kodar en kort identifierare för elementfil och kommandot lyckas blir den identifierade elementfilen aktuell elementfil (*current EF*).

▼B

— Om kommandot lyckas återsänder kortet ‘**9000**’.

— Om den fil som motsvarar den korta identifieraren för elementfil inte kan hittas, återsänds bearbetningsstatus ‘**6A82**’.

— Om säkerhetsvillkoren för den valda filen inte uppfylls, avbryts kommandot med ‘**6982**’.

— Om offset inte överensstämmer med storleken på elementfilen (*Offset > EF size*), återsänds bearbetningsstatus ‘**6B00**’.

— Om storleken på de data som ska skrivas inte överensstämmer med storleken på elementfilen (Offset + Lc > EF size) återsänds bearbetningsstatus ‘**6700**’.

— Om ett integritetsfel upptäcks i filattributen, ska kortet anse filen vara skadad och omöjlig att återställa, och återsända bearbetningsstatus ‘**6400**’ eller ‘**6581**’.

— Om det inte går att skriva data, återsänds bearbetningsstatus ‘**6581**’.

3.5.3.3 Kommando med udda INS-byte (instruktion)

Denna kommandovariant gör det möjligt för kortläsare att skriva data till en elementfil med 32 768 byte eller mer.

TCS_64 Ett färdskrivarkort som stöder EF med 32 768 byte eller mer ska stödja denna kommandovariant för dessa EF. Ett färdskrivarkort kan – men måste inte – stödja denna kommandovariant för andra elementfiler.

TCS_65 **Kommandomeddelande**

Byte	Längd	Värde	Beskrivning
CLA	1	‘00h’	
INS	1	‘D7h’	UPDATE BINARY
P1	1	‘00h’	Aktuell elementfil
P2	1	‘00h’	
Lc	1	‘NNh’	Längd på data i kommandodatafältet
#6-#(5+NN)	NN	‘XX..XXh’	Offsetdataobjekt med taggen ‘54h’ || Godtyckligt (*discretionary*) dataobjekt med taggen ‘53h’ som inkapslar de data som ska skrivas

Kortläsaren ska koda offsetdataobjektets och det godtyckliga (*discretionary*) dataobjektets längd med minsta möjliga antal oktetter, dvs. med hjälp av byte för längd ‘01h’ ska kortläsaren koda en offset/längd från 0 till 255 och med hjälp av byte för längd ‘02h’ en offset/längd från 256 upp till 65 535 byte.

TCS_66 **Svarsmeddelande**

Byte	Längd	Värde	Beskrivning
SW	2	‘XXXXh’	Statusregister (SW1,SW2)

▼B

— Om kommandot lyckas återsänder kortet ‘**9000**’.

— Om ingen elementfil väljs återsänds bearbetningsstatus ‘**6986**’.

— Om säkerhetsvillkoren för den valda filen inte uppfylls, avbryts kommandot med ‘**6982**’.

— Om offset inte överensstämmer med storleken på elementfilen (*Offset > EF size*), återsänds bearbetningsstatus ‘**6B00**’.

— Om storleken på de data som ska skrivas inte överensstämmer med storleken på elementfilen (Offset + Lc > EF size) återsänds bearbetningsstatus ‘**6700**’.

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

— Om det inte går att skriva data, återsänds bearbetningsstatus ‘**6581**’.

3.5.3.3.1 Kommando med säker meddelandehantering (exempel)

Följande exempel åskådliggör användningen av säker meddelandehantering om säkerhetsvillkoret SM-MAC-G2 tillämpas.

TCS_67 Kommandomeddelande

Byte	Längd	Värde	Beskrivning
CLA	1	‘0Ch’	Säker meddelandehantering efterfrågad
INS	1	‘D7h’	UPDATE BINARY
P1	1	‘00h’	Aktuell elementfil
P2	1	‘00h’	
Lc	1	‘XXh’	Fältlängd för skyddade data
#6	1	‘B3h’	Tagg för BER-TLV-kodade data med klarvärde
#7	L	‘NNh’ eller ‘81 NNh’	L_{PV}: längd på överförda data L är 2 byte om L_{PV} > 127 byte.
#(7+L)-#(6+L+NN)	NN	‘XX..XXh’	BER-TLV-kodade data med klarvärde, dvs. offsetdataobjekt med taggen ‘54h’ ‖ Godtyckligt (*discretionary*) dataobjekt med taggen ‘53h’ som inkapslar de data som ska skrivas
#(7+L+NN)	1	‘8Eh’	T_{CC}: Tagg för kryptografisk kontrollsumma
#(8+L+NN)	1	‘XXh’	L_{CC}: Längd på efterföljande kryptografiska kontrollsumma: ‘08h’, ‘0Ch’ eller ‘10h’ beroende på AES-nyckelns längd för säker meddelandehantering (generation 2) (se del B i tillägg 11)
#(9+L+NN)-#(8+M+L+NN)	M	‘XX..XXh’	Kryptografisk kontrollsumma
Le	1	‘00h’	Enligt ISO/IEC 7816-4

▼B

TCS_68 Svarsmeddelande om kommandot lyckas

Byte	Längd	Värde	Beskrivning
#1	1	‘99h’	T_{SW}: Tagg för statusregister (ska skyddas av CC)
#2	1	‘02h’	L_{SW}: längd på återsända statusregister
#3-#4	2	‘XXXXh’	Bearbetningsstatus för APDU för oskyddat svar
#5	1	‘8Eh’	T_{CC}: Tagg för kryptografisk kontrollsumma
#6	1	‘XXh’	L_{CC}: Längd på efterföljande kryptografiska kontrollsumma: ‘08h’, ‘0Ch’ eller ‘10h’ beroende på AES-nyckelns längd för säker meddelandehantering (generation 2) (se del B i tillägg 11)
#7-#(6+L)	L	‘XX..XXh’	Kryptografisk kontrollsumma
SW	2	‘XXXXh’	Statusregister (SW1,SW2)

3.5.4 *GET CHALLENGE*

Detta kommando överensstämmer med ISO/IEC 7816-4, men det har en begränsad användning jämfört med det kommando som definieras i normen.

Kommandot GET CHALLENGE ber kortet att utfärda en utmaning (*challenge*) för att använda den i ett säkerhetsförfarande i vilket ett kryptogram eller några chiffrerade data sänds till kortet.

TCS_69 Den utmaning som utfärdas av kortet är endast giltig för nästa kommando som använder en utmaning som sänds till kortet.

TCS_70 **Kommandomeddelande**

Byte	Längd	Värde	Beskrivning
CLA	1	‘00h’	
INS	1	‘84h’	INS
P1	1	‘00h’	P1
P2	1	‘00h’	P2
Le	1	‘08h’	Le (Längd på den utmaning som förväntas)

TCS_71 **Svarsmeddelande**

Byte	Längd	Värde	Beskrivning
#1-#8	8	‘XX..XXh’	Utmaning
SW	2	‘XXXXh’	Statusregister (SW1,SW2)

— Om kommandot lyckas återsänder kortet ‘**9000**’.

— Om Le skiljer sig från ‘08h’ är bearbetningsstatusen ‘**6700**’.

— Om parametrarna P1-P2 är inkorrekta är bearbetningsstatusen ‘**6A86**’.

▼B

3.5.5 *VERIFY*

Detta kommando överensstämmer med ISO/IEC 7816-4, men det har en begränsad användning jämfört med det kommando som definieras i normen.

Endast verkstadskortet måste stödja detta kommando.

Andra typer av färdskrivarkort kan ha, men måste inte ha, detta kommando infört, men för dessa kort finns ingen användaranpassad referens-CHV. Därför kan dessa kort inte utföra detta kommando. För andra typer av färdskrivarkort än verkstadskort omfattas inte kortets reaktion på detta kommando, dvs. den felkod som återsänds, av denna specifikation.

Kommandot VERIFY initierar jämförelsen i kortet av CHV (PIN)-data som sänds från kommandot med den referens-CHV som lagras i kortet.

TCS_72 Den PIN-kod som anges av användaren måste vara ASCII-kodad och utfylld till höger av kortläsaren med ‘FFh’-byte upp till en längd av 8 byte (se även datatyp WorkshopCardPIN i tillägg 1).

TCS_73 Färdskrivartillämpningar i generation 1 och generation 2 ska använda samma referens-CHV.

TCS_74 Färdskrivarkortet ska kontrollera om kommandot kodas korrekt. Om kommandot inte kodas korrekt ska kortet inte jämföra CHV-värdena, inte minska värdet på räknaren av återstående CHV-försök och inte återställa säkerhetsstatusen ”PIN_Verified”, men avbryta kommandot. Ett kommando är korrekt kodat om byte CLA, INS, P1, P2 och Lc har angivna värden, Le är frånvarande och kommandodatafältet har korrekt längd.

TCS_75 Om kommandot lyckas återinitialiseras räknaren av återstående CHV-försök. Startvärdet för räknaren av återstående CHV-försök är 5. Om kommandot lyckas ska kortet sätta den interna säkerhetsstatusen ”PIN_Verified”. Kortet ska återställa denna säkerhetsstatus om kortet återställs eller om den CHV-kod som sänds i kommandot inte överensstämmer med den referens-CHV som lagrats.

Anmärkning: Användning av samma referens-CHV och en global säkerhetsstatus förhindrar att en verkstadsanställd på nytt måste ange PIN efter det att en annan dedikerad fil för en färdskrivartillämpning valts.

TCS_76 En misslyckad jämförelse registreras i kortet, dvs. värdet på räknaren av återstående CHV-försök ska minskas med 1, för att begränsa antalet ytterligare försök att använda referens-CHV.

TCS_77 **Kommandomeddelande**

Byte	Längd	Värde	Beskrivning
CLA	1	‘00h’	
INS	1	‘20h’	INS
P1	1	‘00h’	P1

▼B

Byte	Längd	Värde	Beskrivning
P2	1	‘00h’	P2 (den verifierade CHV är indirekt känd)
Lc	1	‘08h’	Längd på överförd CHV-kod
#6-#13	8	‘XX..XXh’	CHV

TCS_78 **Svarsmeddelande**

Byte	Längd	Värde	Beskrivning
SW	2	‘XXXXh’	Statusregister (SW1,SW2)

— Om kommandot lyckas återsänder kortet ‘**9000**’.

— Om referens-CHV inte hittas, återsänds bearbetningsstatus ‘**6A88**’.

— Om CHV blockeras (räknaren av återstående CHV-försök står på noll) återsänds bearbetningsstatus ‘**6983**’. När CHV väl är i detta tillstånd kan den inte användas mer.

— Om jämförelsen misslyckas minskas värdet på räknaren av återstående försök och status ‘**63CX**’ återsänds (X > 0 och X = värdet på räknaren av återstående CHV-försök).

— Om referens-CHV anses skadad, återsänds bearbetningsstatus ‘**6400**’ eller ‘**6581**’.

— Om Lc skiljer sig från ‘08h’ är bearbetningsstatusen ‘**6700**’.

3.5.6 *GET RESPONSE*

Detta kommando överensstämmer med ISO/IEC 7816-4.

Detta kommando (som bara behövs och finns för protokoll T=0) används för att överföra förberedda data från kortet till kortläsaren (om ett kommando inbegriper både Lc och Le).

Kommandot GET RESPONSE måste ges omedelbart efter det kommando som förbereder data, annars går dessa data förlorade. Efter verkställandet av kommandot GET RESPONSE (utom om felet ‘**61xx**’ eller ‘**6Cxx**’ inträffar, se nedan), finns tidigare förberedda data inte längre tillgängliga.

TCS_79 **Kommandomeddelande**

Byte	Längd	Värde	Beskrivning
CLA	1	‘00h’	
INS	1	‘C0h’	
P1	1	‘00h’	
P2	1	‘00h’	
Le	1	‘XXh’	Antal förväntade byte

▼B

TCS_80 **Svarsmeddelande**

Byte	Längd	Värde	Beskrivning
#1-#X	X	‘XX..XXh’	Data
SW	2	‘XXXXh’	Statusregister (SW1,SW2)

— Om kommandot lyckas återsänder kortet ‘**9000**’.

— Om kortet inte har förberett några data återsänds bearbetningsstatus ‘**6900**’ eller ‘**6F00**’.

— Om Le överstiger antal tillgängliga byte eller om Le är noll återsänds bearbetningsstatus ‘**6Cxx**’, där xx betecknar exakt antal tillgängliga byte. I detta fall finns förberedda data fortfarande tillgängliga för ett efterföljande GET RESPONSE-kommando.

— Om Le inte är noll och är mindre än antal tillgängliga byte, sänds begärda data på normalt sätt av kortet, och bearbetningsstatus ‘**61xx**’ återsänds, där xx anger ett antal extra byte som fortfarande är tillgängliga för ett efterföljande GET RESPONSE-kommando.

— Om kommandot inte stöds (protokoll T=1), återsänder kortet ‘**6D00**’.

3.5.7 *PSO: VERIFY CERTIFICATE*

Detta kommando överensstämmer med ISO/IEC 7816-8, men det har en begränsad användning jämfört med det kommando som definieras i normen.

Kortet använder kommandot VERIFY CERTIFICATE för att erhålla en öppen nyckel utifrån och för att kontrollera dess giltighet.

3.5.7.1 Meddelandepar (kommando och svar) för generation 1

TCS_81 Denna kommandovariant stöds endast av en färdskrivartillämpning i generation 1.

TCS_82 När ett VERIFY CERTIFICATE-kommando lyckas lagras den öppna nyckeln i säkerhetsmiljön (*security environment*) för framtida användning. Denna nyckel ska uttryckligen ställas in för användning i säkerhetsrelaterade kommandon (INTERNAL AUTHENTICATE, EXTERNAL AUTHENTICATE eller VERIFY CERTIFICATE) av MSE-kommandot (se avsnitt 3.5.11) med hjälp av dess nyckelidentifierare.

TCS_83 I alla händelser använder kommandot VERIFY CERTIFICATE den öppna nyckel som MSE-kommandot tidigare valt för att öppna certifikatet. Denna öppna nyckel ska tillhöra antingen en medlemsstat eller Europa.

TCS_84 **Kommandomeddelande**

Byte	Längd	Värde	Beskrivning
CLA	1	‘00h’	
INS	1	‘2Ah’	PERFORM SECURITY OPERATION
P1	1	‘00h’	P1

▼B

Byte	Längd	Värde	Beskrivning
P2	1	‘AEh’	P2: icke BER-TLV-kodade data (konkatenering av dataelement)
Lc	1	‘C2h’	Lc: Certifikatets längd, 194 byte
#6-#199	194	‘XX..XXh’	Certifikat: konkatenering av dataelement (enligt tillägg 11)

TCS_85 **Svarsmeddelande**

Byte	Längd	Värde	Beskrivning
SW	2	‘XXXXh’	Statusregister (SW1,SW2)

— Om kommandot lyckas återsänder kortet ‘**9000**’.

— Om verifieringen av certifikat misslyckas, återsänds bearbetningsstatus ‘**6688**’. Verifiering och uppackning av certifikat beskrivs i tillägg 11 för G1 och G2.

— Om ingen öppen nyckel är närvarande i säkerhetsmiljön (*security environment*) återsänds ‘**6A88**’.

— Om den valda öppna nyckeln (som används för att packa upp certifikatet) anses skadad återsänds bearbetningsstatus ‘**6400**’ eller ‘**6581**’.

— Endast generation 1: Om den valda öppna nyckeln (som används för att packa upp certifikatet) har en annan CHA.LSB (`CertificateHolderAuthorisation.equipmentType`) än ‘00’ (dvs. om den varken är en medlemsstats eller Europas öppna nyckel) återsänds bearbetningsstatus ‘**6985**’.

3.5.7.2 Meddelandepar (kommando och svar) för generation 2

Beroende på kurvstorlek kan ECC-certifikat vara så långa att de inte kan överföras i en enda APDU. I detta fall måste en kommandokedja i enlighet med ISO/IEC 7816-4 användas, och certifikatet överförs i två på varandra följande PSO: VERIFY CERTIFICATE (APDU).

Certifikatets struktur och domänparametrarna definieras i tillägg 11.

TCS_86 Detta kommando kan utföras på huvudfil (MF) och i DF Tachograph och DF Tachograph_G2 (se även TCS_33).

TCS_87 **Kommandomeddelande**

Byte	Längd	Värde	Beskrivning
CLA	1	‘X0h’	CLA-byte anger kommandokedja: ‘00h’: det enda eller sista kommandot i kedjan ‘10h’: inte det sista kommandot i en kedja
INS	1	‘2Ah’	PERFORM SECURITY OPERATION
P1	1	‘00h’	
P2	1	‘BEh’	Kontrollera självbeskrivande (*self-descriptive*) certifikat

▼B

Byte	Längd	Värde	Beskrivning
Lc	1	‘XXh’	Kommandodatafältets längd, se TCS_88 och TCS_89.
#6-#5+L	L	‘XX..XXh’	DER-TLV-kodade data: Dataobjektet *ECC Certificate Body* som första dataobjekt som konkatenerats med dataobjektet *ECC Certificate Signature* som andra dataobjekt eller en del av denna konkatenering. Taggen ‘7F21’ och motsvarande längd ska inte överföras. Ordningsföljden för dessa dataobjekt är fast.

TCS_88 För dataenheter (APDU) med kort längd gäller följande bestämmelser: Kortläsaren ska använda det minsta antal dataenheter (APDU) som krävs för att överföra kommandots nyttolast (*payload*) och överföra det maximala antalet byte i den första dataenheten (APDU) för kommandot i enlighet med värdet i den byte som betecknar *Information Field Size Card* (se TCS_14). Om kortläsaren inte gör detta så betyder det att kortets funktion ligger utanför tillämpningsområdet.

TCS_89 För dataenheter (APDU) med utökad längd gäller följande bestämmelser: Om certifikatet inte ryms i en enda APDU ska kortet stödja kommandokedjor. Kortläsaren ska använda det minsta antal dataenheter (APDU) som krävs för att överföra kommandots nyttolast (*payload*) och överföra det maximala antalet byte i den första dataenheten (APDU) för kommandot. Om kortläsaren inte gör detta så betyder det att kortets funktion ligger utanför tillämpningsområdet.

Anmärkning: Enligt tillägg 11 lagras certifikatet, eller det innehåll som är relevant i certifikatet, i kortet, och dess *currentAuthenticatedTime* uppdateras.

Strukturen för svarsmeddelanden samt statusregister definieras i TCS_85.

TCS_90 Utöver de felkoder som förtecknas i TCS_85 kan kortet återsända följande felkoder:

— Om den valda öppna nyckeln (som används för att packa upp certifikatet) har en CHA.LSB (*CertificateHolderAuthorisation.equipmentType*) som inte är lämplig för certifikatet enligt tillägg 11 återsänds bearbetningsstatus ‘**6985**’.

— Om kortets *currentAuthenticatedTime* är senare än certifikatets sista giltighetsdag återsänds bearbetningsstatus ‘**6985**’.

— Om det sista kommandot i kedjan förväntas återsänder kortet ‘**6883**’.

— Om felaktiga parameterar sänds i kommandodatafältet återsänder kortet ‘**6A80**’ (används även om dataobjekten inte sänds i den angivna ordningen).

▼B

3.5.8 *INTERNAL AUTHENTICATE*

Detta kommando överensstämmer med ISO/IEC 7816-4.

TCS_91 Alla färdskrivarkort ska stödja detta kommando i DF Tachograph för generation 1. Kommandot kan vara, men måste inte vara, åtkomligt i huvudfilen (MF) och/eller DF Tachograph_G2. I så fall ska kommandot avbrytas med en lämplig felkod eftersom kortets privata nyckel (Card.SK) för autentiseringsprotokollet i generation 1 endast är åtkomlig i DF_Tachograph för generation 1.

Med hjälp av kommandot INTERNAL AUTHENTICATE kan kortläsaren autentisera kortet. Autentiseringen beskrivs i tillägg 11. Den inbegriper nedanstående programsatser.

TCS_92 Kommandot INTERNAL AUTHENTICATE använder kortets privata nyckel (indirekt vald) för att signera autentiseringsdata, inbegripet K1 (första elementet för överenskommelse om sessionsnycklar) och RND1, och använder den öppna nyckel som för närvarande är vald (genom det sista MSE-kommandot) för att kryptera signaturen och utforma token för autentisering (närmare beskrivning i tillägg 11).

TCS_93 **Kommandomeddelande**

Byte	Längd	Värde	Beskrivning
CLA	1	‘00h’	CLA
INS	1	‘88h’	INS
P1	1	‘00h’	P1
P2	1	‘00h’	P2
Lc	1	‘10h’	Längd på de data som sänds till kortet
#6 – #13	8	‘XX..XXh’	Utmaning som används för att autentisera kortet
#14 -#21	8	‘XX..XXh’	VU.CHR (se tillägg 11)
Le	1	‘80h’	Längd på de data som förväntas från kortet

TCS_94 **Svarsmeddelande**

Byte	Längd	Värde	Beskrivning
#1-#128	128	‘XX..XXh’	Token för autentisering av kort (se tillägg 11)
SW	2	‘XXXXh’	Statusregister (SW1,SW2)

— Om kommandot lyckas återsänder kortet ‘**9000**’.

— Om ingen öppen nyckel är närvarande i säkerhetsmiljön (*security environment*) återsänds bearbetningsstatus ‘**6A88**’.

— Om ingen privat nyckel är närvarande i säkerhetsmiljön återsänds bearbetningsstatus ‘**6A88**’.

— Om VU.CHR inte överensstämmer med identifieraren för den aktuella öppna nyckeln återsänds bearbetningsstatus ‘**6A88**’.

▼B

— Om den valda privata nyckeln anses skadad, återsänds bearbetningsstatus ‘**6400**’ eller ‘**6581**’.

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

3.5.9 *EXTERNAL AUTHENTICATE*

Detta kommando överensstämmer med ISO/IEC 7816-4.

Med hjälp av kommandot EXTERNAL AUTHENTICATE kan kortet autentisera kortläsaren. Autentiseringen beskrivs i tillägg 11 för Tachograph G1 och G2 (autentisering av fordonsenhet).

TCS_96 Kommandovarianten för mekanismen för ömsesidig autentisering i generation 1 stöds endast av en färdskrivartillämpning i generation 1.

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).

TCS_98 **Kommandomeddelande**

Byte	Längd	Värde	Beskrivning
CLA	1	‘00h’	CLA
INS	1	‘82h’	INS
P1	1	‘00h’	Indirekt kända nycklar och algoritmer
P2	1	‘00h’	
Lc	1	‘XXh’	Lc (längd på de data som sänds till kortet)
#6-#(5+L)	L	‘XX..XXh’	Autentisering (generation 1): Kryptogram (se del A i tillägg 11) Autentisering (generation 2): Signatur genereras av kortläsaren (se del B i tillägg 11)

TCS_99 **Svarsmeddelande**

Byte	Längd	Värde	Beskrivning
SW	2	‘XXXXh’	Statusregister (SW1,SW2)

— Om kommandot lyckas återsänder kortet ‘**9000**’.

— Om CHA för den för närvarande satta öppna nyckeln inte är en konkatenering av färdskrivartillämpningens AID (tillämpningsidentifierare) och av en typ av fordonsenhetsutrustning, återsänds bearbetningsstatus ‘**6F00**’.

— Om kommandot inte omedelbart föregås av kommandot GET CHALLENGE återsänds bearbetningsstatus ‘6985’.

▼B

Färdskrivartillämpningen (generation 1) kan dessutom återsända följande felkoder:

— Om ingen öppen nyckel är närvarande i säkerhetsmiljön (*security environment*) återsänds ‘**6A88**’.

— Om ingen privat nyckel är närvarande i säkerhetsmiljön återsänds bearbetningsstatus ‘**6A88**’.

— Om verifieringen av kryptogrammet misslyckas, återsänds bearbetningsstatus ‘**6688**’.

— Om den valda privata nyckeln anses skadad, återsänds bearbetningsstatus ‘**6400**’ eller ‘**6581**’.

Kommandovarianten för autentiseringen (generation 2) kan dessutom återsända följande felkod:

— Om verifieringen av signaturen misslyckas, återsänder kortet ‘**6300**’.

3.5.10 *GENERAL AUTHENTICATE*

Detta kommando används för det protokoll för autentisering av chip i generation 2 som specificeras i del B i tillägg 11 och överensstämmer med ISO/IEC 7816-4.

TCS_100 Detta kommando kan utföras på huvudfil (MF) och i DF Tachograph och DF Tachograph_G2 (se även TCS_34).

TCS_101 **Kommandomeddelande**

Byte	Längd	Värde	Beskrivning
CLA	1	‘00h’	
INS	1	‘86h’	
P1	1	‘00h’	Indirekt kända nycklar och protokoll
P2	1	‘00h’	
Lc	1	‘NNh’	Lc: Längd på efterföljande datafält
#6-#(5+L)	L	‘7Ch’ + L_{7C} + ‘80h’ + L_{80} + ‘XX..XXh’	DER-TLV-kodat värde på tillfällig (*ephemeral*) öppen nyckel (se tillägg 11) Fordonsenheten ska sända dataobjekten i denna ordningsföljd.

TCS_102 **Svarsmeddelande**

Byte	Längd	Värde	Beskrivning
#1-#L	L	‘7Ch’ + L_{7C} + ‘81h’ + ‘08h’ + ‘XX..XXh’ + ‘82h’ + L_{82} + ‘XX..XXh’	DER-TLV-kodade data för dynamisk autentisering (*Dynamic Authentication Data*): tal som används en gång (*nonce*) och token för autentisering (se tillägg 11)
SW	2	‘XXXXh’	Statusregister (SW1,SW2)

— Om kommandot lyckas återsänder kortet ‘**9000**’.

— Kortet återsänder ‘**6A80**’ för att ange att datafältet innehåller felaktiga parameterar.

▼B

— Kortet återsänder ‘**6982**’ om kommandot EXTERNAL AUTHENTICATE inte har utförts med tillfredsställande resultat

Svarsobjektet (*Dynamic Authentication Data*) ‘7Ch’

— måste vara närvarande om operationen lyckas, dvs. statusregistret är ‘**9000**’,

— måste vara frånvarande vid exekveringsfel eller kontrollfel, dvs. om statusregistret är i intervallet ‘**6400**’–‘**6FFF**’, och

— kan vara frånvarande vid varning, dvs. om statusregistret är i intervallet ‘**6200**’–‘**63FF**’.

3.5.11 *MANAGE SECURITY ENVIRONMENT*

Detta kommando används för att bestämma en öppen nyckel i autentiseringssyfte.

3.5.11.1 Meddelandepar (kommando och svar) för generation 1

Detta kommando överensstämmer med ISO/IEC 7816-4. Användningen av detta kommando är begränsad med avseende på berörd standard.

TCS_103 Detta kommando stöds endast av en färdskrivartillämpning i generation 1.

TCS_104 Den nyckel som det refereras till i MSE-fältet förblir aktuell öppen nyckel tills nästa korrekta MSE-kommando ges, en dedikerad fil (DF) väljs eller kortet återställs.

TCS_105 Om den nyckel som det refereras till inte (redan) är närvarande i kortet, förblir säkerhetsmiljön (*security environment*) oförändrad.

TCS_106 **Kommandomeddelande**

Byte	Längd	Värde	Beskrivning
CLA	1	‘00h’	CLA
INS	1	‘22h’	INS
P1	1	‘C1h’	P1: refererad nyckel som är giltig för alla kryptografiska operationer
P2:	1	‘B6h’	P2 (refererade data om digital signatur)
Lc	1	‘0Ah’	Lc: längd på efterföljande datafält
#6	1	‘83h’	Tagg för att referera till en öppen nyckel i asymmetriska fall
#7	1	‘08h’	Längd på nyckelreferensen (nyckelidentifierare)
#8-#15	8	‘XX..XXh’	Nyckelidentifierare enligt tillägg 11

TCS_107 **Svarsmeddelande**

Byte	Längd	Värde	Beskrivning
SW	2	‘XXXXh’	Statusregister (SW1,SW2)

▼B

— Om kommandot lyckas återsänder kortet ‘**9000**’.

— Om den refererade nyckeln inte är närvarande i kortet återsänds bearbetningsstatus ‘**6A88**’.

— Om vissa förväntade dataobjekt saknas i formatet för säker meddelandehantering, återsänds bearbetningsstatus ‘**6987**’. Detta kan inträffa om taggen ‘83h’ saknas.

— Om några dataobjekt är inkorrekta, återsänds bearbetningsstatus ‘**6988**’. Detta kan inträffa om längden på nyckelidentifieraren inte är ‘08h’.

— Om den valda nyckeln anses skadad, återsänds bearbetningsstatus ‘**6400**’ eller ‘**6581**’.

3.5.11.2 Meddelandepar (kommando och svar) för generation 2

För autentiseringen i generation 2 stöder färdskrivarkortet följande MSE: Kommandoversioner med SET som överensstämmer med ISO/IEC 7816-4. Dessa kommandoversioner stöds inte för autentisering i generation 1.

3.5.11.2.1 MSE:SET AT för autentisering av chip

Följande MSE:SET AT-kommando används för att välja parametrarna för den autentisering av chip som utförs av ett efterföljande GENERAL AUTHENTICATE-kommando.

TCS_108 Detta kommando kan utföras på huvudfil (MF) och i DF Tachograph och DF Tachograph_G2, se även TCS_34.

TCS_109 **MSE:SET AT – kommandomeddelande för autentisering av chip**

Byte	Längd	Värde	Beskrivning
CLA	1	‘00h’	
INS	1	‘22h’	
P1	1	‘41h’	Inställd för intern autentisering
P2	1	‘A4h’	Autentisering
Lc	1	‘NNh’	Lc: längd på efterföljande datafält
#6-#(5+L)	L	‘80h’ + ‘0Ah’ + ‘XX..XXh’	DER-TLV-kodad referens till kryptografisk mekanism: Objektidentifierare för autentisering av chip (endast värde, taggen ‘06h’ utelämnas). Se tillägg 1 angående värdena på objektidentifierare; bytenotation ska användas. Se tillägg 11 för vägledning om hur man ska välja en av dessa objektidentifierare.

3.5.11.2.2 MSE:SET AT för autentisering av fordonsenhet

Följande MSE:SET AT-kommando används för att välja parametrarna och nycklarna för den autentisering av fordonsenhet som utförs av ett efterföljande EXTERNAL AUTHENTICATE-kommando.

▼B

TCS_110 Detta kommando kan utföras på huvudfil (MF) och i DF Tachograph och DF Tachograph_G2, se även TCS_34.

TCS_111 **MSE:SET AT – kommandomeddelande för autentisering av fordonsenhet**

Byte	Längd	Värde	Beskrivning
CLA	1	‘00h’	
INS	1	‘22h’	
P1	1	‘81h’	Inställd för extern autentisering
P2	1	‘A4h’	Autentisering
Lc	1	‘NNh’	Lc: längd på efterföljande datafält
#6-#(5+L)	L	‘80h’ + ‘0Ah’ + ‘XX..XXh’	DER-TLV-kodad referens till kryptografisk mekanism: Objektidentifierare för autentisering av fordonsenhet (endast värde, taggen ‘06h’ utelämnas). Se tillägg 1 angående värdena på objektidentifierare; bytenotation ska användas. Se tillägg 11 för vägledning om hur man ska välja en av dessa objektidentifierare.
		‘83h’ + ‘08h’ + ‘XX..XXh’	DER-TLV-kodad referens till fordonsenhetens öppna nyckel genom den CHR (*Certificate Holder Reference*) som nämns i dess certifikat.
		‘91h’ + L_{91} + ‘XX..XXh’	DER-TLV-kodad komprimerad representation av fordonsenhetens tillfälliga (*ephemeral*) öppna nyckel, som kommer att användas vid autentisering av chip (se tillägg 11)

3.5.11.2.3 MSE:SET DST

Följande MSE:SET DST-kommando används för att bestämma en öppen nyckel antingen

— för verifiering av en signatur som tillhandahålls i ett efterföljande PSO: VERIFY DIGITAL SIGNATURE, eller

— för verifiering av en signatur för ett certifikat som tillhandahålls i ett efterföljande PSO: VERIFY CERTIFICATE.

TCS_112 Detta kommando kan utföras på huvudfil (MF) och i DF Tachograph och DF Tachograph_G2 (se även TCS_33).

TCS_113 **MSE:SET DST – kommandomeddelande**

Byte	Längd	Värde	Beskrivning
CLA	1	‘00h’	
INS	1	‘22h’	
P1	1	‘81h’	Inställd för verifiering
P2	1	‘B6h’	Digital signatur

▼B

Lc	1	‘NNh’	Lc: längd på efterföljande datafält
#6-#(5+L)	L	‘83h’ + ‘08h’ + ‘XX...XXh’	DER-TLV-kodad referens till en öppen nyckel, dvs. CHR (*Certificate Holder Reference*) i certifikatet för den öppna nyckeln (se tillägg 11).

För alla kommandoversioner ges svarsmeddelandets struktur och statusregistret av följande:

TCS_114 **Svarsmeddelande**

Byte	Längd	Värde	Beskrivning
SW	2	‘XXXXh’	Statusregister (SW1,SW2)

— Om kommandot lyckas återsänder kortet ‘**9000**’. Protokollet har valts och initialiserats.

— ‘**6A80**’ anger felaktiga parametrar i kommandodatafältet.

— ‘**6A88**’ anger att refererade data (dvs. en refererad nyckel) inte är tillgängliga.

3.5.12 *PSO: HASH*

Detta kommando används för att till kortet överföra resultatet från en hashberäkning på vissa data. Detta kommando används för att verifiera digitala signaturer. Hashvärdet lagras tillfälligt för det efterföljande kommandot PSO: VERIFY DIGITAL SIGNATURE

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

Endast kontrollkortet måste stödja detta kommando i DF Tachograph och DF Tachograph_G2.

Andra typer av färdskrivarkort kan ha, men måste inte ha, detta kommando infört. Kommandot kan vara, men måste inte vara, åtkomligt i huvudfilen (MF).

Kontrollkortstillämpningen (generation 1) stöder endast SHA-1.

TCS_115 Det tillfälligt lagrade hashvärdet ska raderas om ett nytt hashvärde beräknas med hjälp av kommandot PSO: HASH, om en dedikerad fil (DF) väljs, och om färdskrivarkortet återställs.

TCS_116 **Kommandomeddelande**

Byte	Längd	Värde	Beskrivning
CLA	1	‘00h’	CLA
INS	1	‘2Ah’	PERFORM SECURITY OPERATION
P1	1	‘90h’	Återsänd hashkod

▼B

Byte	Längd	Värde	Beskrivning
P2	1	‘A0h’	Tagg: datafältet innehåller dataobjekt som är relevanta för hashning
Lc	1	‘XXh’	Längd Lc på efterföljande datafält
#6	1	‘90h’	Tagg för hashkoden
#7	1	‘XXh’	Längden L på hashkoden: ‘14h’ för tillämpning i generation 1 (se del A i tillägg 11) ‘20h’, ‘30h’ eller ‘40h’ för tillämpning i generation 2 (se del B i tillägg 11)
#8-#(7+L)	L	‘XX..XXh’	Hashkod

TCS_117 **Svarsmeddelande**

Byte	Längd	Värde	Beskrivning
SW	2	‘XXXXh’	Statusregister (SW1,SW2)

— Om kommandot lyckas återsänder kortet ‘**9000**’.

— Om några förväntade dataobjekt (enligt specifikation ovan) saknas återsänds bearbetningsstatus ‘**6987**’. Detta kan inträffa om en av taggarna ‘90h’ saknas.

— Om några dataobjekt är inkorrekta, återsänds bearbetningsstatus ‘**6988**’. Detta fel inträffar om den nödvändiga taggen är närvarande men med en annan längd än ‘14h’ för SHA-1, ‘20h’ för SHA-256, ‘30h’ för SHA-384, ‘40h’ för SHA-512 (tillämpning i generation 2).

3.5.13 *PERFORM HASH of FILE*

Detta kommando överensstämmer inte med ISO/IEC 7816-8. CLA-byte i detta kommando anger sålunda att det finns en äganderättsligt skyddad (*proprietary*) användning av PERFORM SECURITY OPERATION / HASH.

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. Om ett företagskort eller ett kontrollkort har detta kommando infört, ska det vara infört enligt specifikationen i detta kapitel.

Kommandot kan vara, men måste inte vara, åtkomligt i huvudfilen (MF). Om så är fallet ska kommandot vara infört enligt specifikationen i detta kapitel, dvs. det ska inte möjliggöra beräkning av ett hashvärde, utan avbrytas med en lämplig felkod.

TCS_118 Kommandot PERFORM HASH of FILE används för att hasha dataarean hos den för närvarande valda transparenta elementfilen (EF).

TCS_119 Ett färdskrivarkort ska stödja detta kommando endast för de elementfiler som är förtecknade i kapitel 4 under DF_Tachograph och DF_Tachograph_G2 med undantaget att ett färdskrivarkort inte ska stödja kommandot för EF Sensor_Installation_Data i DF Tachograph_G2.

▼B

TCS_120 Resultatet från hashningen lagras tillfälligt i kortet. Det kan därefter användas för att få en digital signatur av filen, med hjälp av kommandot PSO: COMPUTE DIGITAL SIGNATURE.

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 PSO: HASH OF FILE, om en dedikerad fil (DF) väljs, och om färdskrivarkortet återställs.

TCS_122 Färdskrivartillämpningen (generation 1) ska stödja SHA-1.

TCS_123 Färdskrivartillämpningen (generation 2) ska stödja SHA-1 och SHA-2 (256, 384 och 512 bitar).

TCS_124 **Kommandomeddelande**

Byte	Längd	Värde	Beskrivning
CLA	1	‘80h’	CLA
INS	1	‘2Ah’	PERFORM SECURITY OPERATION
P1	1	‘90h’	Tagg: Hash
P2	1	‘XXh’	P2: Anger vilken algoritm som ska användas för hashning av data i den för närvarande valda transparenta filen: ‘00h’ för SHA-1 ‘01h’ för SHA-256 ‘02h’ för SHA-384 ‘03h’ för SHA-512

TCS_125 **Svarsmeddelande**

Byte	Längd	Värde	Beskrivning
SW	2	‘XXXXh’	Statusregister (SW1,SW2)

— Om kommandot lyckas återsänder kortet ‘**9000**’.

— Om den aktuella elementfilen inte tillåter detta kommando (EF Sensor_Installation_Data i DF Tachograph_G2) återsänds bearbetningsstatus ‘**6985**’.

— Om den valda elementfilen anses skadad (integritetsfel i filattributen eller lagrade data), återsänds bearbetningsstatus ‘**6400**’ eller ‘**6581**’.

— Om den valda filen inte är en transparent fil, eller om det inte finns någon aktuell elementfil, återsänds bearbetningsstatus ‘**6986**’.

3.5.14 *PSO: COMPUTE DIGITAL SIGNATURE*

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.

▼B

Andra typer av färdskrivarkort kan ha, men måste inte ha, detta kommando infört, men de ska inte ha någon signaturnyckel. Därför kan dessa kort inte utföra kommandot, utan kommandot avbryts med en lämplig felkod.

Kommandot kan vara, men måste inte vara, åtkomligt i huvudfilen (MF). I så ska fall ska kommandot avbrytas med en lämplig felkod.

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

TCS_126 Detta kommando ska inte beräkna en digital signatur hos tidigare beräknad hashkod med kommandot PSO: HASH.

TCS_127 Kortets privata nyckel används för att beräkna den digitala signaturen och är indirekt känd av kortet.

TCS_128 Färdskrivartillämpningen (generation 1) skapar en digital signatur med hjälp av en utfyllnadsmetod som överensstämmer med PKCS1 (se tillägg 11).

TCS_129 Färdskrivartillämpningen (generation 2) beräknar en digital signatur baserad på en elliptisk kurva (se tillägg 11).

TCS_130 **Kommandomeddelande**

Byte	Längd	Värde	Beskrivning
CLA	1	‘00h’	CLA
INS	1	‘2Ah’	PERFORM SECURITY OPERATION
P1	1	‘9Eh’	Digital signatur som ska återsändas
P2	1	‘9Ah’	Tagg: datafältet innehåller data som ska signeras. Eftersom inget datafält inbegrips är det meningen att data redan ska finnas i kortet (*hash of file*).
Le	1	‘NNh’	Längd på förväntad signatur

TCS_131 **Svarsmeddelande**

Byte	Längd	Värde	Beskrivning
#1-#L	L	‘XX..XXh’	Signatur hos tidigare beräknad hash
SW	2	‘XXXXh’	Statusregister (SW1,SW2)

— Om kommandot lyckas återsänder kortet ‘**9000**’.

— Om den indirekt valda privata nyckeln anses skadad, återsänds bearbetningsstatus ‘**6400**’ eller ‘**6581**’.

— Om den hash som beräknades i ett tidigare PERFORM HASH OF FILE-kommando inte är tillgänglig återsänds bearbetningsstatus ‘**6985**’.

▼B

3.5.15 *PSO: VERIFY DIGITAL SIGNATURE*

Detta kommando används för att verifiera den digitala signaturen som tillhandahålls som indata och vars hash är känd av kortet. Signaturalgoritmen är indirekt känd av kortet.

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

Endast kontrollkortet måste stödja detta kommando i DF Tachograph och DF Tachograph_G2.

Andra typer av färdskrivarkort kan ha, men måste inte ha, detta kommando infört. Kommandot kan vara, men måste inte vara, åtkomligt i huvudfilen (MF).

TCS_132 Kommandot VERIFY DIGITAL SIGNATURE använder alltid den öppna nyckel som valts av det tidigare givna MSE-kommandot (*Manage Security Environment*) MSE: SET DST och den tidigare hashkoden som angetts i ett PSO: HASH-kommando.

TCS_133 **Kommandomeddelande**

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	‘83h’	Längd Lc på efterföljande datafält
6	1	‘9Eh’	Tagg för digital signatur
#7-#8	2	‘81 XXh’	Längd på digital signatur: 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)
#9-#(8+L)	L	‘XX..XXh’	Innehåll i digital signatur

TCS_134 **Svarsmeddelande**

Byte	Längd	Värde	Beskrivning
SW	2	‘XXXXh’	Statusregister (SW1,SW2)

— Om kommandot lyckas återsänder kortet ‘**9000**’.

— Om verifieringen av signaturen misslyckas, återsänds bearbetningsstatus ‘**6688**’. Verifieringen beskrivs i tillägg 11.

— Om ingen öppen nyckel har valts återsänds bearbetningsstatus ‘**6A88**’.

— Om några förväntade dataobjekt (enligt specifikation ovan) saknas återsänds bearbetningsstatus ‘**6987**’. Detta kan inträffa om en av de nödvändiga taggarna saknas.

▼B

— Om ingen hashkod finns tillgänglig för att behandla kommandot (som ett resultat av ett tidigare PSO: HASH-kommando) återsänds bearbetningsstatus ‘**6985**’.

— Om några dataobjekt är inkorrekta, återsänds bearbetningsstatus ‘**6988**’. Detta kan inträffa om en av de begärda dataobjektlängderna är inkorrekt.

— Om den valda öppna nyckeln anses skadad, återsänds bearbetningsstatus ‘**6400**’ eller ‘**6581**’.

3.5.16 *PROCESS DSRC MESSAGE*

Detta kommando används för att kontrollera integriteten och autenticiteten hos DSRC-meddelandet och dechiffrera de data som översänts från en fordonsenhet till en kontrollmyndighet eller en verkstad via DSRC-länken. Kortet härleder krypteringsnyckeln och den MAC-nyckel som används för att skydda DSRC-meddelandet såsom beskrivs i kapitel 13 i del B i tillägg 11.

Endast kontrollkortet och verkstadskortet måste stödja detta kommando i DF Tachograph_G2.

Andra typer av färdskrivarkort kan ha, men måste inte ha, detta kommando infört, men de ska inte ha någon huvudnyckel till DSRC. Därför kan dessa kort inte utföra kommandot, utan kommandot avbryts med en lämplig felkod.

Kommandot kan vara, men måste inte vara, åtkomligt i huvudfilen (MF) och/eller DF Tachograph. I så ska fall ska kommandot avbrytas med en lämplig felkod.

TCS_135 Huvudnyckeln till DSRC är åtkomlig endast i DF Tachograph_G2, dvs. kontroll- och verkstadskortet ska stödja verkställandet av kommandot endast i DF Tachograph_G2.

TCS_136 Kommandot ska endast dekryptera DSRC-data och verifiera den kryptografiska kontrollsumman, men det ska inte tolka indata.

TCS_137 Dataobjektens ordningsföljd i kommandodatafältet fastställs i denna specifikation.

TCS_138 **Kommandomeddelande**

Byte	Längd	Värde	Beskrivning
CLA	1	‘80h’	Äganderättsligt skyddad (*proprietary*) CLA
INS	1	‘2Ah’	PERFORM SECURITY OPERATION
P1	1	‘80h’	Svarsdata: klarvärde
P2	1	‘B0h’	Kommandodata: BER-TVL-kodade data med klarvärde inklusive SM-dataobjekt (SM – säker meddelandehantering)
Lc	1	‘NNh’	Längd Lc på efterföljande datafält

▼B

Byte	Längd	Värde	Beskrivning
#6-#(5+L)	L	‘87h’ + L_{87} + ‘XX..XXh’	DER-TLV-kodad byte för utfyllnadsindikator, följd av krypterad nyttolast (*payload*) från färdskrivaren. För denna byte för utfyllnadsindikator ska värdet ‘00h’ (”ingen ytterligare indikering” i enlighet med ISO/IEC 7816-4:2013 tabell 52) användas. Information om krypteringsmekanismen finns i kapitel 13 i del B i tillägg 11. Tillåtna värden för längden L_{87} är multiplar av AES-blocklängden plus 1 för byte för utfyllnadsindikator, dvs. från 17 byte upp till och med 193 byte. *Anmärkning:* Se ISO/IEC 7816-4:2013 tabell 49 för SM-dataobjektet (SM – säker meddelandehantering) med taggen ‘87h’.
		‘81h’ + ‘10h’	DER-TLV-kodad kontrollreferensmall för konfidentialitet (*Control Reference Template for Confidentiality*) som kapslar följande konkatenerade dataelement (se tillägg 1 DSRCSecurityData och tillägg 11 del B kapitel 13): — Tidsstämpel (4 byte) — Räknare (3 byte) — Serienummer för fordonsenhet (VU) (8 byte) — Version för huvudnyckel till DSRC (1 byte) *Anmärkning:* Se ISO/IEC 7816-4:2013 tabell 49 för SM-dataobjektet (SM – säker meddelandehantering) med taggen ‘81h’.
		‘8Eh’ + L_{8E} + ‘XX..XXh’	DER-TLV-kodad MAC för DSRC-meddelandet. Information om MAC-algoritmen och MAC-beräkningen finns i kapitel 13 i del B i tillägg 11. *Anmärkning:* Se ISO/IEC 7816-4:2013 tabell 49 för SM-dataobjektet (SM – säker meddelandehantering) med taggen ‘8Eh’.

TCS_139 **Svarsmeddelande**

Byte	Längd	Värde	Beskrivning
#1-#L	L	‘XX..XXh’	Frånvarande (i händelse av ett fel) eller dechiffrerade data (utfyllnad borttagen)
SW	2	‘XXXXh’	Statusregister (SW1,SW2)

— Om kommandot lyckas återsänder kortet ‘9000’.

— ‘**6A80**’ anger felaktiga parametrar i kommandodatafältet (används också om dataobjekten inte sänds i den angivna ordningsföljden).

— ‘**6A88**’ anger att refererade data inte är tillgängliga, dvs den refererade huvudnyckeln till DSRC är inte tillgänglig.

— ‘**6900**’ anger att verifieringen av den kryptografiska kontrollsumman eller dekrypteringen av data misslyckades.

4. FÄRDSKRIVARKORTENS STRUKTUR

I denna punkt specificeras filstrukturerna i färdskrivarkort för lagring av åtkomliga data.

▼B

Här specificeras varken interna strukturer som är beroende av korttillverkare, exempelvis etikett för startdel (*header*) i en fil, eller lagring och hantering av dataelement som endast behövs för intern användning, exempelvis `EuropeanPublicKey`,`CardPrivateKey`,`TdesSessionKey` eller `WorkshopCardPin`.

TCS_140 Ett färdskrivarkort (generation 2) ska innehålla huvudfilen (MF) och en färdskrivarkortstillämpning (generation 1 och generation 2) av samma typ (t.ex. förarkortstillämpningar).

TCS_141 Ett färdskrivarkort ska stödja åtminstone det minsta antal poster som anges för motsvarande tillämpningar och ska inte stödja fler poster än det största antal poster som anges för motsvarande tillämpningar.

Största och minsta antal poster anges i detta kapitel för de olika tillämpningarna.

Information om de säkerhetsvillkor som används i tillträdesreglerna i hela detta kapitel återfinns i kapitel 3.3. I allmänhet betecknar åtkomstläget för läsning (*read*) kommandot READ BINARY med jämn och, om detta stöds, udda INS-byte med undantag för EF Sensor_Installation_Data i verkstadskortet (se TCS_156 och TCS_160). Åtkomstläget för uppdatering (*update*) betecknar kommandot UPDATE BINARY med jämn och, om detta stöds, udda INS-byte, och åtkomstläget för val (*select*) betecknar kommandot SELECT.

4.1. **Huvudfil (MF)**

TCS_142 Efter det att huvudfilen (MF) har användaranpassats ska den ha nedanstående permanenta filstruktur och filtillträdesvillkor.

Anmärkning: Den korta identifieraren (SFID) för elementfilen (EF) anges som ett decimaltal, t.ex. motsvaras värdet 30 av 11110 binärt.

			Tillträdesregler	
Fil	**Fil-ID**	**SFID**	**Läs/välj (Read/Select)**	**Uppdatera (*Update*)**
MF	'3F00h'			
├─ EF ICC	'0002h'		ALW	NEV
├─ EF IC	'0005h'		ALW	NEV
├─ EF DIR	'2F00h'	30	ALW	NEV
├─ EF ATR/INFO (conditional)	'2F01h'	29	ALW	NEV
├─ EF Extended_Length (conditional)	'0006h'	28	ALW	NEV
├─ DF Tachograph	'0500h'		SC1	
└─ DF Tachograph_G2			SC1	

Följande förkortning för säkerhetsvillkoret används i denna tabell:

SC1 ALW OR SM-MAC-G2

TCS_143 Alla EF-strukturer ska vara transparenta.

TCS_144 Huvudfilen (MF) ska ha följande datastruktur:

▼B

Fil/Dataelement	Antal poster	Storlek (byte) Min.	Max.	Standardvärden
MF		*63*	*184*	
├─EF ICC		*25*	*25*	
│ └─CardIccIdentification		*25*	*25*	
│ ├─clockStop		1	1	{00}
│ ├─cardExtendedSerialNumber		8	8	{00..00}
│ ├─cardApprovalNumber		8	8	{20..20}
│ ├─cardPersonaliserID		1	1	{00}
│ ├─embedderIcAssemblerId		5	5	{00..00}
│ └─icIdentifier		2	2	{00 00}
├─EF IC		*8*	*8*	
│ └─CardChipIdentification		*8*	*8*	
│ ├─icSerialNumber		4	4	{00..00}
│ └─icManufacturingReferences		4	4	{00..00}
├─EF DIR		*20*	*20*	
│ └─See TCS_145		*20*	*20*	{00..00}
├─EF ATR/INFO		*7*	*128*	
│ └─See TCS_146		*7*	*128*	{00..00}
├─EF EXTENDED_LENGTH		*3*	*3*	
│ └─See TCS_147		*3*	*3*	{00..00}
└─DF Tachograph				
└─DF Tachograph_G2				

TCS_145 Elementfilen EF DIR ska innehålla följande tillämpningsrelaterade dataobjekt: ‘61 08 4F 06 FF 54 41 43 48 4F 61 08 4F 06 FF 53 4D 52 44 54’

TCS_146 Elementfilen EF ATR/INFO ska vara närvarande om färdskrivarkortet indikerar i sitt ATR att det stödjer fält med utökad längd. I så fall ska EF ATR/INFO innehålla dataobjektet med information om utökad längd (DO‘7F66’) i enlighet med ISO/IEC 7816-4:2013 avsnitt 12.7.1.

TCS_147 Elementfilen EF Extended_Length ska vara närvarande om färdskrivarkortet indikerar i sitt ATR att det stödjer fält med utökad längd. I så fall ska elementfilen (EF) innehålla följande dataobjekt: ‘02 01 xx’ där värdet ‘xx’ anger om fält med utökad längd stöds för protokoll T=1 och/eller protokoll T=0.

Värdet ‘01’ anger att fält med utökad längd stöds för protokoll T=1.

Värdet ‘10’ anger att fält med utökad längd stöds för protokoll T=0.

Värdet ‘11’ anger att fält med utökad längd stöds för protokoll T=1 och protokoll T=0.

4.2. Förarkortstillämpningar

4.2.1 *Förarkortstillämpning (generation 1)*

TCS_148 Efter det att förarkortstillämpningen (generation 1) har användaranpassats ska den ha nedanstående permanenta filstruktur och filtillträdesvillkor.

Fil	Fil-ID	Tillträdesregler		
		Läs (*Read*)	Välj (*Select*)	Uppdatera (*Update*)
└─DF Tachograph	‘0500h’		SC1	
├─EF Application_Identification	‘0501h’	SC2	SC1	NEV
├─EF Card_Certificate	‘C100h’	SC2	SC1	NEV
├─EF CA_Certificate	‘C108h’	SC2	SC1	NEV
├─EF Identification	‘0520h’	SC2	SC1	NEV
├─EF Card_Download	‘050Eh’	SC2	SC1	SC1
├─EF Driving_Licence_Info	‘0521h’	SC2	SC1	NEV
├─EF Events_Data	‘0502h’	SC2	SC1	SC3
├─EF Faults_Data	‘0503h’	SC2	SC1	SC3
├─EF Driver_Activity_Data	‘0504h’	SC2	SC1	SC3
├─EF Vehicles_Used	‘0505h’	SC2	SC1	SC3
├─EF Places	‘0506h’	SC2	SC1	SC3
├─EF Current_Usage	‘0507h’	SC2	SC1	SC3
├─EF Control_Activity_Data	‘0508h’	SC2	SC1	SC3
└─EF Specific_Conditions	‘0522h’	SC2	SC1	SC3

▼B

Följande förkortningar för säkerhetsvillkoren används i denna tabell:

SC1 ALW OR SM-MAC-G2

SC2 ALW OR SM-MAC-G1 OR SM-MAC-G2

SC3 SM-MAC-G1 OR SM-MAC-G2

TCS_149 Alla EF-strukturer ska vara transparenta.

TCS_150 Förarkortstillämpningen (generation 1) ska ha följande datastruktur:

Fil/dataelement	Antal poster	Size (bytes) Min.	Size (bytes) Max.	Standard-värden
DF Tachograph		*11378*	*24926*	
EF Application_Identification		*10*	*10*	
DriverCardApplicationIdentification		*10*	*10*	
typeOfTachographCardId		1	1	{00}
cardStructureVersion		2	2	{00 00}
noOfEventsPerType		1	1	{00}
noOfFaultsPerType		1	1	{00}
activityStructureLength		2	2	{00 00}
noOfCardVehicleRecords		2	2	{00 00}
noOfCardPlaceRecords		1	1	{00}
EF Card_Certificate		*194*	*194*	
CardCertificate		194	194	{00..00}
EF CA_Certificate		*194*	*194*	
MemberStateCertificate		194	194	{00..00}
EF Identification		*143*	*143*	
CardIdentification		*65*	*65*	
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
cardIssuingAuthorityName		36	36	{20..20}
cardIssueDate		4	4	{00..00}
cardValidityBegin		4	4	{00..00}
cardExpiryDate		4	4	{00..00}
DriverCardHolderIdentification		*78*	*78*	
cardHolderName		*72*	*72*	
holderSurname		36	36	{00, 20..20}
holderFirstNames		36	36	{00, 20..20}
cardHolderBirthDate		4	4	{00..00}
cardHolderPreferredLanguage		2	2	{20 20}
EF Card_Download		*4*	*4*	
LastCardDownload		4	4	
EF Driving_Licence_Info		*53*	*53*	
CardDrivingLicenceInformation		*53*	*53*	
drivingLicenceIssuingAuthority		36	36	{00, 20..20}
drivingLicenceIssuingNation		1	1	{00}
drivingLicenceNumber		16	16	{20..20}
EF Events_Data		*864*	*1728*	
CardEventData		*864*	*1728*	
cardEventRecords	6	*144*	*288*	
CardEventRecord	n_1	*24*	*24*	
eventType		1	1	{00}
eventBeginTime		4	4	{00..00}
eventEndTime		4	4	{00..00}
eventVehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
EF Faults_Data		*576*	*1152*	
CardFaultData		*576*	*1152*	
cardFaultRecords	2	*288*	*576*	
CardFaultRecord	n_2	*24*	*24*	
faultType		1	1	{00}
faultBeginTime		4	4	{00..00}
faultEndTime		4	4	{00..00}
faultVehicleRegistration				

▼B

vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
EF Driver_Activity_Data		*5548*	*13780*	
CardDriverActivity		*5548*	*13780*	
activityPointerOldestDayRecord		2	2	{00 00}
activityPointerNewestRecord		2	2	{00 00}
activityDailyRecords	n_6	5544	13776	{00..00}
EF Vehicles_Used		*2606*	*6202*	
CardVehiclesUsed		*2606*	*6202*	
vehiclePointerNewestRecord		2	2	{00 00}
cardVehicleRecords		*2604*	*6200*	
CardVehicleRecord	n_3	*31*	*31*	
vehicleOdometerBegin		3	3	{00..00}
vehicleOdometerEnd		3	3	{00..00}
vehicleFirstUse		4	4	{00..00}
vehicleLastUse		4	4	{00..00}
vehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
vuDataBlockCounter		2	2	{00 00}
EF Places		*841*	*1121*	
CardPlaceDailyWorkPeriod		*841*	*1121*	
placePointerNewestRecord		1	1	{00}
placeRecords		*840*	*1120*	
PlaceRecord	n_4	*10*	*10*	
entryTime		4	4	{00..00}
entryTypeDailyWorkPeriod		1	1	{00}
dailyWorkPeriodCountry		1	1	{00}
dailyWorkPeriodRegion		1	1	{00}
vehicleOdometerValue		3	3	{00..00}
EF Current_Usage		*19*	*19*	
CardCurrentUse		*19*	*19*	
sessionOpenTime		4	4	{00..00}
sessionOpenVehicle				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
EF Control_Activity_Data		*46*	*46*	
CardControlActivityDataRecord		*46*	*46*	
controlType		1	1	{00}
controlTime		4	4	{00..00}
controlCardNumber				
cardType		1	1	{00}
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
controlVehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
controlDownloadPeriodBegin		4	4	{00..00}
controlDownloadPeriodEnd		4	4	{00..00}
EF Specific_Conditions		*280*	*280*	
SpecificConditionRecord	56	*5*	*5*	
entryTime		4	4	{00..00}
SpecificConditionType		1	1	{00}

▼B

TCS_151 Nedanstående värden, som används för att tillhandahålla storlekar i tabellen ovan, är de minsta och största numeriska värden som förarkortets datastruktur enligt generation 1 måste använda för posterna.

		Min.	Max.
n_1	NoOfEventsPerType	6	12
n_2	NoOfFaultsPerType	12	24
n_3	NoOfCardVehicleRecords	84	200
n_4	NoOfCardPlaceRecords	84	112
n_6	CardActivityLengthRange	5544 byte (28 dagar * 93 aktivitetsändringar)	13776 byte (28 dagar * 240 aktivitetsändringar)

4.2.2 *Förarkortstillämpning (generation 2)*

TCS_152 Efter det att förarkortstillämpningen (generation 2) har användaranpassats ska den ha nedanstående permanenta filstruktur och filtillträdesvillkor.

Anmärkning: Den korta identifieraren (SFID) för elementfilen (EF) anges som ett decimaltal, t.ex. motsvaras värdet 30 av 11110 binärt.

Fil	Fil-ID	SFID	Tillträdesregler	
			Läs/välj (Read/Select)	Uppdatera (*Update*)
└─DF Tachograph_G2			SC1	
├─EF Application_Identification	'0501h'	1	SC1	NEV
├─EF CardMA_Certificate	'C100h'	2	SC1	NEV
├─EF CardSignCertificate	'C101h'	3	SC1	NEV
├─EF CA_Certificate	'C108h'	4	SC1	NEV
├─EF Link_Certificate	'C109h'	5	SC1	NEV
├─EF Identification	'0520h'	6	SC1	NEV
├─EF Card_Download	'050Eh'	7	SC1	SC1
├─EF Driving_Licence_Info	'0521h'	10	SC1	NEV
├─EF Events_Data	'0502h'	12	SC1	SM-MAC-G2
├─EF Faults_Data	'0503h'	13	SC1	SM-MAC-G2
├─EF Driver_Activity_Data	'0504h'	14	SC1	SM-MAC-G2
├─EF Vehicles_Used	'0505h'	15	SC1	SM-MAC-G2
├─EF Places	'0506h'	16	SC1	SM-MAC-G2
├─EF Current_Usage	'0507h'	17	SC1	SM-MAC-G2
├─EF Control_Activity_Data	'0508h'	18	SC1	SM-MAC-G2
├─EF Specific_Conditions	'0522h'	19	SC1	SM-MAC-G2
├─EF VehicleUnits_Used	'0523h'	20	SC1	SM-MAC-G2
└─EF GNSS_Places	'0524h'	21	SC1	SM-MAC-G2

Följande förkortning för säkerhetsvillkoret används i denna tabell:

SC1 ALW OR SM-MAC-G2

TCS_153 Alla EF-strukturer ska vara transparenta.

TCS_154 Förarkortstillämpningen (generation 2) ska ha följande datastruktur:

▼B

Fil/dataelement	Antal poster	Storlek (byte) Min.	Max.	Standard-värden
DF Tachograph_G2		*19510*	*39306*	
EF Application_Identification		*15*	*15*	
DriverCardApplicationIdentification		*15*	*15*	
typeOfTachographCardId		1	1	{00}
cardStructureVersion		2	2	{00 00}
noOfEventsPerType		1	1	{00}
noOfFaultsPerType		1	1	{00}
activityStructureLength		2	2	{00 00}
noOfCardVehicleRecords		2	2	{00 00}
noOfCardPlaceRecords		2	2	{00}
noOfGNSSCDRecords		2	2	{00 00}
noOfSpecificConditionRecords		2	2	{00}
EF CardMA_Certificate		*204*	*341*	
CardMACertificate		204	341	{00..00}
EF CardSignCertificate		*204*	*341*	
CardSignCertificate		204	341	{00..00}
EF CA_Certificate		*204*	*341*	
MemberStateCertificate		204	341	{00..00}
EF Link_Certificate		*204*	*341*	
LinkCertificate		204	341	{00..00}
EF Identification		*143*	*143*	
CardIdentification		*65*	*65*	
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
cardIssuingAuthorityName		36	36	{20..20}
cardIssueDate		4	4	{00..00}
cardValidityBegin		4	4	{00..00}
cardExpiryDate		4	4	{00..00}
DriverCardHolderIdentification		*78*	*78*	
cardHolderName		*72*	*72*	
holderSurname		36	36	{00, 20..20}
holderFirstNames		36	36	{00, 20..20}
cardHolderBirthDate		4	4	{00..00}
cardHolderPreferredLanguage		2	2	{20 20}
EF Card_Download		*4*	*4*	
LastCardDownload		4	4	
EF Driving_Licence_Info		*53*	*53*	
CardDrivingLicenceInformation		*53*	*53*	
drivingLicenceIssuingAuthority		36	36	{00, 20..20}
drivingLicenceIssuingNation		1	1	{00}
drivingLicenceNumber		16	16	{20..20}
EF Events_Data		*1584*	*3168*	
CardEventData		*1584*	*3168*	
cardEventRecords	11	*144*	*288*	
CardEventRecord	n_1	*24*	*24*	
eventType		1	1	{00}
eventBeginTime		4	4	{00..00}
eventEndTime		4	4	{00..00}
eventVehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
EF Faults_Data		*576*	*1152*	
CardFaultData		*576*	*1152*	
cardFaultRecords	2	*288*	*576*	
CardFaultRecord	n_2	*24*	*24*	

▼B

├─faultType		1	1	{00}
├─faultBeginTime		4	4	{00..00}
├─faultEndTime		4	4	{00..00}
└─faultVehicleRegistration				
├─vehicleRegistrationNation		1	1	{00}
└─vehicleRegistrationNumber		14	14	{00, 20..20}
EF Driver_Activity_Data		*5548*	*13780*	
└CardDriverActivity		*5548*	*13780*	
├─activityPointerOldestDayRecord		2	2	{00 00}
├─activityPointerNewestRecord		2	2	{00 00}
└─activityDailyRecords	n_6	5544	13776	{00..00}
EF Vehicles_Used		*4034*	*9602*	
└CardVehiclesUsed		*4034*	*9602*	
├─vehiclePointerNewestRecord		2	2	{00 00}
└─cardVehicleRecords		*4032*	*9600*	
└─CardVehicleRecord	n_3	*48*	*48*	
├─vehicleOdometerBegin		3	3	{00..00}
├─vehicleOdometerEnd		3	3	{00..00}
├─vehicleFirstUse		4	4	{00..00}
├─vehicleLastUse		4	4	{00..00}
├─vehicleRegistration				
├─vehicleRegistrationNation		1	1	{00}
└─vehicleRegistrationNumber		14	14	{00, 20..20}
├─vuDataBlockCounter		2	2	{00 00}
└─vehicleIdentificationNumber		17	17	{20..20}
EF Places		*1766*	*2354*	
└CardPlaceDailyWorkPeriod		*1766*	*2354*	
├─placePointerNewestRecord		2	2	{00 00}
└─placeRecords		*1764*	*2352*	
└─PlaceRecord	n_4	*21*	*21*	
├─entryTime		4	4	{00..00}
├─entryTypeDailyWorkPeriod		1	1	{00}
├─dailyWorkPeriodCountry		1	1	{00}
├─dailyWorkPeriodRegion		1	1	{00}
├─vehicleOdometerValue		3	3	{00..00}
└─entryGNSSPlaceRecord		11	11	
├─timeStamp		4	4	{00..00}
├─gnssAccuracy		1	1	{00}
└─geoCoordinates		6	6	{00..00}
EF Current_Usage		*19*	*19*	
└CardCurrentUse		*19*	*19*	
├─sessionOpenTime		4	4	{00..00}
└─sessionOpenVehicle				
├─vehicleRegistrationNation		1	1	{00}
└─vehicleRegistrationNumber		14	14	{00, 20..20}
EF Control_Activity_Data		*46*	*46*	
└CardControlActivityDataRecord		*46*	*46*	
├─controlType		1	1	{00}
├─controlTime		4	4	{00..00}
├─controlCardNumber				
├─cardType		1	1	{00}
├─cardIssuingMemberState		1	1	{00}
└─cardNumber		16	16	{20..20}
├─controlVehicleRegistration				
├─vehicleRegistrationNation		1	1	{00}
└─vehicleRegistrationNumber		14	14	{00, 20..20}
├─controlDownloadPeriodBegin		4	4	{00..00}
└─controlDownloadPeriodEnd		4	4	{00..00}

▼B

EF Specific_Conditions		*282*	*562*	
SpecificConditions		*282*	*562*	
conditionPointerNewestRecord		2	2	{00 00}
specificConditionRecords		*280*	*560*	
SpecificConditionRecord	n_9	*5*	*5*	
entryTime		4	4	{00..00}
specificConditionType		1	1	{00}
EF VehicleUnits_Used		*842*	*2002*	
CardVehicleUnitsUsed		*842*	*2002*	
vehicleUnitPointerNewestRecord		2	2	{00 00}
cardVehicleUnitRecords		*840*	*2000*	
CardVehicleUnitRecord	n_7	*10*	*10*	
timeStamp		4	4	{00..00}
manufacturerCode		1	1	{00}
deviceID		1	1	{00}
vuSoftwareVersion		4	4	{00..00}
EF GNSS_Places		*3782*	*5042*	
GNSSContinuousDriving		*3782*	*5042*	
gnssCDPointerNewestRecord		2	2	{00 00}
gnssContinuousDrivingRecords		3780	5040	{00}
GNSSContinuousDrivingRecord	n_8	*15*	*15*	
timeStamp		4	4	{00..00}
gnssPlaceRecord		11	11	
timeStamp		4	4	{00..00}
gnssAccuracy		1	1	{00}
geoCoordinates		6	6	{00..00}

TCS_155 Nedanstående värden, som används för att tillhandahålla storlekar i tabellen ovan, är de minsta och största numeriska värden som förarkortets datastruktur enligt generation 2 måste använda för posterna.

		Min.	Max.
n_1	NoOfEventsPerType	6	12
n_2	NoOfFaultsPerType	12	24
n_3	NoOfCardVehicleRecords	84	200
n_4	NoOfCardPlaceRecords	84	112
n_6	CardActivityLengthRange	5544 byte (28 dagar * 93 aktivitetsändringar)	13776 byte (28 dagar * 240 aktivitetsändringar)
n_7	NoOfCardVehicleUnitRecords	84	200
n_8	NoOfGNSSCDRecords	252	336
n_9	NoOfSpecificConditionRecords	56	112

4.3. **Verkstadskortstillämpningar**

4.3.1 *Verkstadskortstillämpning (generation 1)*

TCS_156 Efter det att verkstadskortstillämpningen (generation 1) har användaranpassats ska den ha nedanstående permanenta filstruktur och filtillträdesvillkor.

▼B

Fil	Fil-ID	Tillträdesregler		
		Läs (*Read*)	Välj (*Select*)	Uppdatera (*Update*)
└─DF Tachograph	'0500h'		SC1	
├─EF Application_Identification	'0501h'	SC2	SC1	NEV
├─EF Card_Certificate	'C100h'	SC2	SC1	NEV
├─EF CA_Certificate	'C108h'	SC2	SC1	NEV
├─EF Identification	'0520h'	SC2	SC1	NEV
├─EF Card_Download	'0509h'	SC2	SC1	**SC1**
├─EF Calibration	'050Ah'	SC2	SC1	SC3
├─EF Sensor_Installation_Data	'050Bh'	**SC4**	SC1	NEV
├─EF Events_Data	'0502h'	SC2	SC1	SC3
├─EF Faults_Data	'0503h'	SC2	SC1	SC3
├─EF Driver_Activity_Data	'0504h'	SC2	SC1	SC3
├─EF Vehicles_Used	'0505h'	SC2	SC1	SC3
├─EF Places	'0506h'	SC2	SC1	SC3
├─EF Current_Usage	'0507h'	SC2	SC1	SC3
├─EF Control_Activity_Data	'0508h'	SC2	SC1	SC3
└─EF Specific_Conditions	'0522h'	SC2	SC1	SC3

Följande förkortningar för säkerhetsvillkoren används i denna tabell:

SC1 ALW OR SM-MAC-G2

SC2 ALW OR SM-MAC-G1 OR SM-MAC-G2

SC3 SM-MAC-G1 OR SM-MAC-G2

SC4 För kommandot READ BINARY med jämn INS-byte:

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

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

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

TCS_157 Alla EF-strukturer ska vara transparenta.

TCS_158 Verkstadskortstillämpningen (generation 1) ska ha följande datastruktur:

▼B

Fil/dataelementt	Antal poster	Storlek (byte) Min.	Max.	Standardvärden
DF Tachograph		*11055*	*29028*	
EF Application_Identification		*11*	*11*	
WorkshopCardApplicationIdentification		*11*	*11*	
typeOfTachographCardId		1	1	{00}
cardStructureVersion		2	2	{00 00}
noOfEventsPerType		1	1	{00}
noOfFaultsPerType		1	1	{00}
activityStructureLength		2	2	{00 00}
noOfCardVehicleRecords		2	2	{00 00}
noOfCardPlaceRecords		1	1	{00}
noOfCalibrationRecords		1	1	{00}
EF Card_Certificate		*194*	*194*	
CardCertificate		194	194	{00..00}
EF CA_Certificate		*194*	*194*	
MemberStateCertificate		194	194	{00..00}
EF Identification		*211*	*211*	
CardIdentification		65	65	
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
cardIssuingAuthorityName		36	36	{00, 20..20}
cardIssueDate		4	4	{00..00}
cardValidityBegin		4	4	{00..00}
cardExpiryDate		4	4	{00..00}
WorkshopCardHolderIdentification		*146*	*146*	
workshopName		36	36	{00, 20..20}
workshopAddress		36	36	{00, 20..20}
cardHolderName				
holderSurname		36	36	{00, 20..20}
holderFirstNames		36	36	{00, 20..20}
cardHolderPreferredLanguage		2	2	{20 20}
EF Card_Download		*2*	*2*	
NoOfCalibrationsSinceDownload		2	2	{00 00}
EF Calibration		*9243*	*26778*	
WorkshopCardCalibrationData		*9243*	*26778*	
calibrationTotalNumber		2	2	{00 00}
calibrationPointerNewestRecord		1	1	{00}
calibrationRecords		*9240*	*26775*	
WorkshopCardCalibrationRecord	n_5	*105*	*105*	
calibrationPurpose		1	1	{00}
vehicleIdentificationNumber		17	17	{20..20}
vehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
wVehicleCharacteristicConstant		2	2	{00 00}
kConstantOfRecordingEquipment		2	2	{00 00}
lTyreCircumference		2	2	{00 00}
tyreSize		15	15	{20..20}
authorisedSpeed		1	1	{00}
oldOdometerValue		3	3	{00..00}
newOdometerValue		3	3	{00..00}
oldTimeValue		4	4	{00..00}
newTimeValue		4	4	{00..00}
nextCalibrationDate		4	4	{00..00}
vuPartNumber		16	16	{20..20}
vuSerialNumber		8	8	{00..00}
sensorSerialNumber		8	8	{00..00}

▼B

EF Sensor_Installation_Data		*16*	*16*	
SensorInstallationSecData		16	16	{00..00}
EF Events_Data		*432*	*432*	
CardEventData		*432*	*432*	
cardEventRecords	6	*72*	*72*	
CardEventRecord	n_1	*24*	*24*	
eventType		1	1	{00}
eventBeginTime		4	4	{00..00}
eventEndTime		4	4	{00..00}
eventVehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
EF Faults_Data		*288*	*288*	
CardFaultData		*288*	*288*	
cardFaultRecords	2	*144*	*144*	
CardFaultRecord	n_2	*24*	*24*	
faultType		1	1	{00}
faultBeginTime		4	4	{00..00}
faultEndTime		4	4	{00..00}
faultVehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
EF Driver_Activity_Data		*202*	*496*	
CardDriverActivity		*202*	*496*	
activityPointerOldestDayRecord		2	2	{00 00}
activityPointerNewestRecord		2	2	{00 00}
activityDailyRecords	n_6	198	492	{00..00}
EF Vehicles_Used		*126*	*250*	
CardVehiclesUsed		*126*	*250*	
vehiclePointerNewestRecord		2	2	{00 00}
cardVehicleRecords		*124*	*248*	
CardVehicleRecord	n_3	*31*	*31*	
vehicleOdometerBegin		3	3	{00..00}
vehicleOdometerEnd		3	3	{00..00}
vehicleFirstUse		4	4	{00..00}
vehicleLastUse		4	4	{00..00}
vehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
vuDataBlockCounter		2	2	{00 00}
EF Places		*61*	*81*	
CardPlaceDailyWorkPeriod		*61*	*81*	
placePointerNewestRecord		1	1	{00}
placeRecords		*60*	*80*	
PlaceRecord	n_4	*10*	*10*	
entryTime		4	4	{00..00}
entryTypeDailyWorkPeriod		1	1	{00}
dailyWorkPeriodCountry		1	1	{00}
dailyWorkPeriodRegion		1	1	{00}
vehicleOdometerValue		3	3	{00..00}
EF Current_Usage		*19*	*19*	
CardCurrentUse		*19*	*19*	
sessionOpenTime		4	4	{00..00}
sessionOpenVehicle				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}

▼B

EF Control_Activity_Data		*46*	*46*	
CardControlActivityDataRecord	2	*46*	*46*	
controlType		1	1	{00}
controlTime		4	4	{00..00}
controlCardNumber				
cardType		1	1	{00}
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
controlVehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
controlDownloadPeriodBegin		4	4	{00..00}
controlDownloadPeriodEnd		4	4	{00..00}
EF Specific_Conditions		*10*	*10*	
SpecificConditionRecord	2	*5*	*5*	
entryTime		4	4	{00..00}
SpecificConditionType		1	1	{00}

TCS_159 Nedanstående värden, som används för att tillhandahålla storlekar i tabellen ovan, är de minsta och största numeriska värden som verkstadskortets datastruktur enligt generation 1 måste använda för posterna.

		Min.	Max.
n_1	NoOfEventsPerType	3	3
n_2	NoOfFaultsPerType	6	6
n_3	NoOfCardVehicleRecords	4	8
n_4	NoOfCardPlaceRecords	6	8
n_5	NoOfCalibrationRecords	88	255
n_6	CardActivityLengthRange	198 byte (1 dag * 93 aktivitetsändringar)	492 byte (1 dag * 240 aktivitetsändringar)

4.3.2 *Verkstadskortstillämpning (generation 2)*

TCS_160 Efter det att verkstadskortstillämpningen (generation 2) har användaranpassats ska den ha nedanstående permanenta filstruktur och filtillträdesvillkor.

Anmärkning: Den korta identifieraren (SFID) för elementfilen (EF) anges som ett decimaltal, t.ex. motsvaras värdet 30 av 11110 binärt.

			Tillträdesregler		
Fil	**Fil-ID**	**SFID**	**Läs (*Read*)**	**Välj (*Select*)**	**Uppdatera (*Update*)**
DF Tachograph_G2			SC1	SC1	
EF Application_Identification	'0501h'	1	SC1	SC1	NEV
EF CardMA_Certificate	'C100h'	2	SC1	SC1	NEV
EF CardSignCertificate	'C101h'	3	SC1	SC1	NEV
EF CA_Certificate	'C108h'	4	SC1	SC1	NEV
EF Link_Certificate	'C109h'	5	SC1	SC1	NEV
EF Identification	'0520h'	6	SC1	SC1	NEV
EF Card_Download	'0509h'	7	SC1	SC1	SC1
EF Calibration	'050Ah'	10	SC1	SC1	SM-MAC-G2
EF Sensor_Installation_Data	'050Bh'	11	**SC5**	SM-MAC-G2	NEV
EF Events_Data	'0502h'	12	SC1	SC1	SM-MAC-G2
EF Faults_Data	'0503h'	13	SC1	SC1	SM-MAC-G2
EF Driver_Activity_Data	'0504h'	14	SC1	SC1	SM-MAC-G2
EF Vehicles_Used	'0505h'	15	SC1	SC1	SM-MAC-G2
EF Places	'0506h'	16	SC1	SC1	SM-MAC-G2
EF Current_Usage	'0507h'	17	SC1	SC1	SM-MAC-G2
EF Control_Activity_Data	'0508h'	18	SC1	SC1	SM-MAC-G2
EF Specific_Conditions	'0522h'	19	SC1	SC1	SM-MAC-G2
EF VehicleUnits_Used	'0523h'	20	SC1	SC1	SM-MAC-G2
EF GNSS_Places	'0524h'	21	SC1	SC1	SM-MAC-G2

▼B

Följande förkortningar för säkerhetsvillkoren används i denna tabell:

SC1 ALW OR SM-MAC-G2

SC5 För kommandot READ BINARY med jämn INS-byte: SM-C-MAC-G2 AND SM-R-ENC-MAC-G2

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

TCS_161 Alla elementfilers strukturer ska vara transparenta.

TCS_162 Verkstadskortstillämpningen (generation 2) ska ha följande datastruktur:

Fil/dataelement	Antal poster	Storlek (byte) Min.	Max.	Standard-värden
DF Tachograph_G2		*17837*	*47163*	
EF Application_Identification		*17*	*17*	
WorkshopCardApplicationIdentification		*17*	*17*	
typeOfTachographCardId		1	1	{00}
cardStructureVersion		2	2	{00 00}
noOfEventsPerType		1	1	{00}
noOfFaultsPerType		1	1	{00}
activityStructureLength		2	2	{00 00}
noOfCardVehicleRecords		2	2	{00 00}
noOfCardPlaceRecords		2	2	{00}
noOfCalibrationRecords		2	2	{00}
noOfGNSSCDRecords		2	2	{00..00}
noOfSpecificConditionRecords		2	2	{00..00}
EF CardMA_Certificate		*204*	*341*	
CardMACertificate		204	341	{00..00}
EF CardSignCertificate		*204*	*341*	
CardSignCertificate		204	341	{00..00}
EF CA_Certificate		*204*	*341*	
MemberStateCertificate		204	341	{00..00}
EF Link_Certificate		*204*	*341*	
LinkCertificate		204	341	{00..00}
EF Identification		*211*	*211*	
CardIdentification		*65*	*65*	
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
cardIssuingAuthorityName		36	36	{00, 20..20}
cardIssueDate		4	4	{00..00}
cardValidityBegin		4	4	{00..00}
cardExpiryDate		4	4	{00..00}
WorkshopCardHolderIdentification		*146*	*146*	
workshopName		36	36	{00, 20..20}
workshopAddress		36	36	{00, 20..20}
cardHolderName				
holderSurname		36	36	{00, 20..20}
holderFirstNames		36	36	{00, 20..20}
cardHolderPreferredLanguage		2	2	{20 20}
EF Card_Download		*2*	*2*	
NoOfCalibrationsSinceDownload		2	2	{00 00}
EF Calibration		*14788*	*42844*	
WorkshopCardCalibrationData		*14788*	*42844*	
calibrationTotalNumber		2	2	{00 00}
calibrationPointerNewestRecord		2	2	{00}
calibrationRecords		*14784*	*42840*	
WorkshopCardCalibrationRecord	n_5	*168*	*168*	
calibrationPurpose		1	1	{00}
vehicleIdentificationNumber		17	17	{20..20}
vehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
wVehicleCharacteristicConstant		2	2	{00 00}
kConstantOfRecordingEquipment		2	2	{00 00}
lTyreCircumference		2	2	{00 00}
tyreSize		15	15	{20..20}
authorisedSpeed		1	1	{00}
oldOdometerValue		3	3	{00..00}
newOdometerValue		3	3	{00..00}

▼B

├─oldTimeValue		4	4	{00..00}
├─newTimeValue		4	4	{00..00}
├─nextCalibrationDate		4	4	{00..00}
├─vuPartNumber		16	16	{20..20}
├─vuSerialNumber		8	8	{00..00}
├─sensorSerialNumber		8	8	{00..00}
├─sensorGNSSSerialNumber		8	8	{00..00}
├─rcmSerialNumber		8	8	{00..00}
├─vuAbility		1	1	{00}
└─sealDataCard		46	46	
├─noOfSealRecords		1	1	{00}
└─SealRecords		45	45	
└─SealRecord	5	9	9	
├─equipmentType		1	1	{00}
└─extendedSealIdentifier		8	8	{00..00}
EF Sensor_Installation_Data		*18*	*102*	
└─SensorInstallationSecData		18	102	{00..00}
EF Events_Data		*792*	*792*	
└─CardEventData		*792*	*792*	
└─cardEventRecords	11	*72*	*72*	
└─CardEventRecord	n_1	*24*	*24*	
├─eventType		1	1	{00}
├─eventBeginTime		4	4	{00..00}
├─eventEndTime		4	4	{00..00}
└─eventVehicleRegistration				
├─vehicleRegistrationNation		1	1	{00}
└─vehicleRegistrationNumber		14	14	{00, 20..20}
EF Faults_Data		*288*	*288*	
└─CardFaultData		*288*	*288*	
└─cardFaultRecords	2	*144*	*144*	
└─CardFaultRecord	n_2	*24*	*24*	
├─faultType		1	1	{00}
├─faultBeginTime		4	4	{00..00}
├─faultEndTime		4	4	{00..00}
└─faultVehicleRegistration				
├─vehicleRegistrationNation		1	1	{00}
└─vehicleRegistrationNumber		14	14	{00, 20..20}
EF Driver_Activity_Data		*202*	*496*	
└─CardDriverActivity		*202*	*496*	
├─activityPointerOldestDayRecord		2	2	{00 00}
├─activityPointerNewestRecord		2	2	{00 00}
└─activityDailyRecords	n_6	198	492	{00..00}
EF Vehicles_Used		*194*	*386*	
└─CardVehiclesUsed		*194*	*386*	
├─vehiclePointerNewestRecord		2	2	{00 00}
└─cardVehicleRecords		*192*	*384*	
└─CardVehicleRecord	n_3	*48*	*48*	
├─vehicleOdometerBegin		3	3	{00..00}
├─vehicleOdometerEnd		3	3	{00..00}
├─vehicleFirstUse		4	4	{00..00}
├─vehicleLastUse		4	4	{00..00}
├─vehicleRegistration				
├─vehicleRegistrationNation		1	1	{00}
└─vehicleRegistrationNumber		14	14	{00, 20..20}
├─vuDataBlockCounter		2	2	{00 00}
└─vehicleIdentificationNumber		*17*	17	{20..20}
EF Places		*128*	*170*	

▼B

└CardPlaceDailyWorkPeriod		*128*	*170*	
├placePointerNewestRecord		2	2	{00 00}
└placeRecords		*126*	*168*	
└PlaceRecord	n_4	*21*	*21*	
├entryTime		4	4	{00..00}
├entryTypeDailyWorkPeriod		1	1	{00}
├dailyWorkPeriodCountry		1	1	{00}
├dailyWorkPeriodRegion		1	1	{00}
├vehicleOdometerValue		3	3	{00..00}
└entryGNSSPlaceRecord		11	11	{00..00}
├timeStamp		4	4	{00..00}
├gnssAccuracy		1	1	{00}
└geoCoordinates		6	6	{00..00}
EF Current_Usage		*19*	*19*	
└CardCurrentUse		*19*	*19*	
├sessionOpenTime		4	4	{00..00}
└sessionOpenVehicle				
├vehicleRegistrationNation		1	1	{00}
└vehicleRegistrationNumber		14	14	{00, 20..20}
EF Control_Activity_Data		*46*	*46*	
└CardControlActivityDataRecord		*46*	*46*	
├controlType		1	1	{00}
├controlTime		4	4	{00..00}
├controlCardNumber				
├cardType		1	1	{00}
├cardIssuingMemberState		1	1	{00}
└cardNumber		16	16	{20..20}
├controlVehicleRegistration				
├vehicleRegistrationNation		1	1	{00}
└vehicleRegistrationNumber		14	14	{00, 20..20}
├controlDownloadPeriodBegin		4	4	{00..00}
└controlDownloadPeriodEnd		4	4	{00..00}
EF VehicleUnits_Used		*42*	*42*	
└CardVehicleUnitsUsed		*42*	*82*	
├vehicleUnitPointerNewestRecord		2	2	{00 00}
└cardVehicleUnitRecords		*40*	*80*	
└CardVehicleUnitRecord	n_7	*10*	*10*	
├timeStamp		4	4	{00..00}
├manufacturerCode		1	1	{00..00}
├deviceID		1	1	{00..00}
└vuSoftwareVersion		4	4	{00..00}
EF GNSS_Places		*262*	*362*	
└GNSSContinuousDriving		*262*	*362*	
├gnssCDPointerNewestRecord		2	2	{00 00}
└gnssContinuousDrivingRecords		*260*	*360*	
└GNSSContinuousDrivingRecord	n_8	*15*	*15*	
├timeStamp		4	4	{00..00}
└gnssPlaceRecord		11	11	
├timeStamp		4	4	{00..00}
├gnssAccuracy		1	1	{00}
└geoCoordinates		6	6	{00..00}
EF Specific_Conditions		*12*	*22*	
└SpecificConditions		*12*	*22*	
├conditionPointerNewestRecord		2	2	{00 00}
└specificConditionRecords		10	20	
└SpecificConditionRecord	n_9	*5*	*5*	
├entryTime		4	4	{00..00}
└specificConditionType		1	1	{00}

▼B

TCS_163 Nedanstående värden, som används för att tillhandahålla storlekar i tabellen ovan, är de minsta och största numeriska värden som verkstadskortets datastruktur enligt generation 2 måste använda för posterna.

		Min.	Max.
n_1	NoOfEventsPerType	3	3
n_2	NoOfFaultsPerType	6	6
n_3	NoOfCardVehicleRecords	4	8
n_4	NoOfCardPlaceRecords	6	8
n_5	NoOfCalibrationRecords	88	255
n_6	CardActivityLengthRange	198 byte (1 dag * 93 aktivitetsändringar)	492 byte (1 dag * 240 aktivitetsändringar)
n_7	NoOfCardVehicleUnitRecords	4	8
n_8	NoOfGNSSCDRecords	18	24
n_9	NoOfSpecificConditionRecords	2	4

4.4. Kontrollkortstillämpningar

4.4.1 *Kontrollkortstillämpning (generation 1)*

TCS_164 Efter det att kontrollkortstillämpningen (generation 1) har användaranpassats ska den ha nedanstående permanenta filstruktur och filtillträdesvillkor.

		Tillträdesregler		
Fil	**Fil-ID**	**Läs (*Read*)**	**Välj (*Select*)**	**Uppdatera (*Update*)**
└─DF Tachograph	'0500h'			
├─EF Application_Identification	'0501h'	SC2	SC1	NEV
├─EF Card_Certificate	'C100h'	SC2	SC1	NEV
├─EF CA_Certificate	'C108h'	SC2	SC1	NEV
├─EF Identification	'0520h'	**SC6**	SC1	NEV
└─EF Controller_Activity_Data	'050Ch'	SC2	SC1	SC3

Följande förkortningar för säkerhetsvillkoren används i denna tabell:

SC1 ALW OR SM-MAC-G2

SC2 ALW OR SM-MAC-G1 OR SM-MAC-G2

SC3 SM-MAC-G1 OR SM-MAC-G2

SC6 EXT-AUT-G1 OR SM-MAC-G1 OR SM-MAC-G2

TCS_165 Alla EF-strukturer ska vara transparenta.

TCS_166 Kontrollkortstillämpningen (generation 1) ska ha följande datastruktur:

▼B

Fil/dataelement	Antal poster	Storlek (byte) Min.	Max.	
DF Tachograph		*11186*	*24526*	
EF Application_Identification		*5*	*5*	
ControlCardApplicationIdentification		*5*	*5*	
typeOfTachographCardId		1	1	{00}
cardStructureVersion		2	2	{00 00}
noOfControlActivityRecords		2	2	{00 00}
EF Card_Certificate		*194*	*194*	
CardCertificate		194	194	{00..00}
EF CA_Certificate		*194*	*194*	
MemberStateCertificate		194	194	{00..00}
EF Identification		*211*	*211*	
CardIdentification		*65*	*65*	
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
cardIssuingAuthorityName		36	36	{00, 20..20}
cardIssueDate		4	4	{00..00}
cardValidityBegin		4	4	{00..00}
cardExpiryDate		4	4	{00..00}
ControlCardHolderIdentification		*146*	*146*	
controlBodyName		36	36	{00, 20..20}
controlBodyAddress		36	36	{00, 20..20}
cardHolderName				
holderSurname		36	36	{00, 20..20}
holderFirstNames		36	36	{00, 20..20}
cardHolderPreferredLanguage		2	2	{20 20}
EF Controller_Activity_Data		*10582*	*23922*	
ControlCardControlActivityData		*10582*	*23922*	
controlPointerNewestRecord		2	2	{00 00}
controlActivityRecords		*10580*	*23920*	
controlActivityRecord	n_7	*46*	*46*	
controlType		1	1	{00}
controlTime		4	4	{00..00}
controlledCardNumber				
cardType		1	1	{00}
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
controlledVehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
controlDownloadPeriodBegin		4	4	{00..00}
controlDownloadPeriodEnd		4	4	{00..00}

TCS_167 Nedanstående värden, som används för att tillhandahålla storlekar i tabellen ovan, är de minsta och största numeriska värden som kontrollkortets datastruktur enligt generation 1 måste använda för posterna.

		Min.	Max.
n_7	NoOfControlActivityRecords	230	520

4.4.2 *Kontrollkortstillämpning (generation 2)*

TCS_168 Efter det att kontrollkortstillämpningen (generation 2) har användaranpassats ska den ha nedanstående permanenta filstruktur och filtillträdesvillkor.

Anmärkning: Den korta identifieraren (SFID) för elementfilen (EF) anges som ett decimaltal, t.ex. motsvaras värdet 30 av 11110 binärt.

▼B

Fil	Fil-ID	SFID	Tillträdesregler: Läs/välj (Read/Select)	Tillträdesregler: Uppdatera (*Update*)
└─DF Tachograph_G2			SC1	
├─EF Application_Identification	'0501h'	1	SC1	NEV
├─EF CardMA_Certificate	'C100h'	2	SC1	NEV
├─EF CA_Certificate	'C108h'	4	SC1	NEV
├─EF Link_Certificate	'C109h'	5	SC1	NEV
├─EF Identification	'0520h'	6	SC1	NEV
└─EF Controller_Activity_Data	'050Ch'	14	SC1	SM-MAC-G2

Följande förkortning för säkerhetsvillkoret används i denna tabell:

SC1 ALW OR SM-MAC-G2

TCS_169 Alla EF-strukturer ska vara transparenta.

TCS_170 Kontrollkortstillämpningen (generation 2) ska ha följande datastruktur:

Fil/dataelement	Antal poster	Storlek (byte) Min.	Max.	
└─DF Tachograph_G2		*11410*	*25161*	
├─EF Application_Identification		*5*	*5*	
└─ControlCardApplicationIdentification		*5*	*5*	
├─typeOfTachographCardId		1	1	{00}
├─cardStructureVersion		2	2	{00 00}
└─noOfControlActivityRecords		2	2	{00 00}
├─EF CardMA_Certificate		*204*	*341*	
└─CardMACertificate		204	341	{00..00}
├─EF CA_Certificate		*204*	*341*	
└─MemberStateCertificate		204	341	{00..00}
├─EF Link_Certificate		*204*	*341*	
└─LinkCertificate		204	341	{00..00}
├─EF Identification		*211*	*211*	
├─CardIdentification		*65*	*65*	
├─cardIssuingMemberState		1	1	{00}
├─cardNumber		16	16	{20..20}
├─cardIssuingAuthorityName		36	36	{00, 20..20}
├─cardIssueDate		4	4	{00..00}
├─cardValidityBegin		4	4	{00..00}
└─cardExpiryDate		4	4	{00..00}
└─ControlCardHolderIdentification		*146*	*146*	
├─controlBodyName		36	36	{00, 20..20}
├─controlBodyAddress		36	36	{00, 20..20}
├─cardHolderName				
├─holderSurname		36	36	{00, 20..20}
└─holderFirstNames		36	36	{00, 20..20}
└─cardHolderPreferredLanguage		2	2	{20 20}
└─EF Controller_Activity_Data		*10582*	*23922*	
└─ControlCardControlActivityData		*10582*	*23922*	
├─controlPointerNewestRecord		2	2	{00 00}
└─controlActivityRecords		*10580*	*23920*	
└─controlActivityRecord	n_7	*46*	*46*	
├─controlType		1	1	{00}
├─controlTime		4	4	{00..00}
├─controlledCardNumber				
├─cardType		1	1	{00}
├─cardIssuingMemberState		1	1	{00}
└─cardNumber		16	16	{20..20}
├─controlledVehicleRegistration				
├─vehicleRegistrationNation		1	1	{00}
└─vehicleRegistrationNumber		14	14	{00, 20..20}
├─controlDownloadPeriodBegin		4	4	{00..00}
└─controlDownloadPeriodEnd		4	4	{00..00}

TCS_171 Nedanstående värden, som används för att tillhandahålla storlekar i tabellen ovan, är de minsta och största numeriska värden som kontrollkortets datastruktur enligt generation 2 måste använda för posterna.

▼B

		Min.	Max.
n_7	NoOfControlActivityRecords	230	520

4.5. **Företagskortstillämpningar**

4.5.1 *Företagskortstillämpning (generation 1)*

TCS_172 Efter det att företagskortstillämpningen (generation 1) har användaranpassats ska den ha nedanstående permanenta filstruktur och filtillträdesvillkor.

		Tillträdesregler		
Fil	**Fil-ID**	**Läs (*Read*)**	**Välj (*Select*)**	**Uppdatera (*Update*)**
└DF Tachograph	'0500h'		SC1	
├EF Application_Identification	'0501h'	SC2	SC1	NEV
├EF Card_Certificate	'C100h'	SC2	SC1	NEV
├EF CA_Certificate	'C108h'	SC2	SC1	NEV
├EF Identification	'0520h'	**SC6**	SC1	NEV
└EF Company_Activity_Data	'050Dh'	SC2	SC1	SC3

Följande förkortningar för säkerhetsvillkoren används i denna tabell:

SC1 ALW OR SM-MAC-G2

SC2 ALW OR SM-MAC-G1 OR SM-MAC-G2

SC3 SM-MAC-G1 OR SM-MAC-G2

SC6 EXT-AUT-G1 OR SM-MAC-G1 OR SM-MAC-G2

TCS_173 Alla EF-strukturer ska vara transparenta.

TCS_174 Företagskortstillämpningen (generation 1) ska ha följande datastruktur:

Fil/dataelement	Antal poster	Storlek (byte) Min.	Max.	Standard-värden
└DF Tachograph		*11114*	*24454*	
├EF Application_Identification		*5*	*5*	
│└CompanyCardApplicationIdentification		*5*	*5*	
│├typeOfTachographCardId		1	1	{00}
│├cardStructureVersion		2	2	{00 00}
│└noOfCompanyActivityRecords		2	2	{00 00}
├EF Card_Certificate		*194*	*194*	
│└CardCertificate		194	194	{00..00}
├EF CA_Certificate		*194*	*194*	
│└MemberStateCertificate		194	194	{00..00}
├EF Identification		*139*	*139*	
│├CardIdentification		*65*	*65*	
││├cardIssuingMemberState		1	1	{00}
││├cardNumber		16	16	{20..20}
││├cardIssuingAuthorityName		36	36	{00, 20..20}
││├cardIssueDate		4	4	{00..00}
││├cardValidityBegin		4	4	{00..00}
││└cardExpiryDate		4	4	{00..00}
│└CompanyCardHolderIdentification		*74*	*74*	
│├companyName		36	36	{00, 20..20}
│├companyAddress		36	36	{00, 20..20}
│└cardHolderPreferredLanguage		2	2	{20 20}
├EF Company_Activity_Data		*10582*	*23922*	
│└CompanyActivityData		*10582*	*23922*	
│├companyPointerNewestRecord		2	2	{00 00}
│└companyActivityRecords		*10580*	*23920*	
│└companyActivityRecord	n_8	*46*	*46*	
│├companyActivityType		1	1	{00}
│├companyActivityTime		4	4	{00..00}
│├cardNumberInformation				
││├cardType		1	1	{00}
││├cardIssuingMemberState		1	1	{00}
││└cardNumber		16	16	{20..20}
│├vehicleRegistrationInformation				
││├vehicleRegistrationNation		1	1	{00}
││└vehicleRegistrationNumber		14	14	{00, 20..20}
│├downloadPeriodBegin		4	4	{00..00}
│└downloadPeriodEnd		4	4	{00..00}

▼B

TCS_175 Nedanstående värden, som används för att tillhandahålla storlekar i tabellen ovan, är de minsta och största numeriska värden som företagskortets datastruktur enligt generation 1 måste använda för posterna.

		Min.	Max.
n_8	NoOfCompanyActivityRecords	230	520

4.5.2 *Företagskortstillämpning (generation 2)*

TCS_176 Efter det att företagskortstillämpningen (generation 2) har användaranpassats ska den ha nedanstående permanenta filstruktur och filtillträdesvillkor.

Anmärkning: Den korta identifieraren (SFID) för elementfilen (EF) anges som ett decimaltal, t.ex. motsvaras värdet 30 av 11110 binärt.

			Tillträdesregler	
Fil	**Fil-ID**	**SFID**	**Läs/välj (Read/Select)**	**Uppdatera (*Update*)**
└DF Tachograph_G2			SC1	
├EF Application_Identification	'0501h'	1	SC1	NEV
├EF CardMA_Certificate	'C100h'	2	SC1	NEV
├EF CA_Certificate	'C108h'	4	SC1	NEV
├EF Link_Certificate	'C109h'	5	SC1	NEV
├EF Identification	'0520h'	6	SC1	NEV
└EF Company_Activity_Data	'050Dh'	14	SC1	SM-MAC-G2

Följande förkortning för säkerhetsvillkoret används i denna tabell:

SC1 ALW OR SM-MAC-G2

TCS_177 Alla EF-strukturer ska vara transparenta.

TCS_178 Företagskortstillämpningen (generation 2) ska ha följande datastruktur:

Fil/dataelement	Antal poster	Storlek (byte) Min.	Max.	Standardvärden
└DF Tachograph_G2		*11338*	*25089*	
├EF Application_Identification		*5*	*5*	
│└CompanyCardApplicationIdentification		*5*	*5*	
│├typeOfTachographCardId		1	1	{00}
│├cardStructureVersion		2	2	{00 00}
│└noOfCompanyActivityRecords		2	2	{00 00}
├EF CardMA_Certificate		*204*	*341*	
│└CardMACertificate		204	341	{00..00}
├EF CA_Certificate		*204*	*341*	
│└MemberStateCertificate		204	341	{00..00}
├EF Link_Certificate		*204*	*341*	
│└LinkCertificate		204	341	{00..00}
├EF Identification		*139*	*139*	
│├CardIdentification		*65*	*65*	
││├cardIssuingMemberState		1	1	{00}
││├cardNumber		16	16	{20..20}
││├cardIssuingAuthorityName		36	36	{00, 20..20}
││├cardIssueDate		4	4	{00..00}
││├cardValidityBegin		4	4	{00..00}
││└cardExpiryDate		4	4	{00..00}
│└CompanyCardHolderIdentification		*74*	*74*	
│├companyName		36	36	{00, 20..20}
│├companyAddress		36	36	{00, 20..20}
│└cardHolderPreferredLanguage		2	2	{20 20}
└EF Company_Activity_Data		*10582*	*23922*	
└CompanyActivityData		*10582*	*23922*	
├companyPointerNewestRecord		2	2	{00 00}
└companyActivityRecords		*10580*	*23920*	
└companyActivityRecord	n_8	*46*	*46*	
├companyActivityType		1	1	{00}
├companyActivityTime		4	4	{00..00}
├cardNumberInformation				
├cardType		1	1	{00}
├cardIssuingMemberState		1	1	{00}
└cardNumber		16	16	{20..20}
├vehicleRegistrationInformation				
├vehicleRegistrationNation		1	1	{00}
└vehicleRegistrationNumber		14	14	{00, 20..20}
├downloadPeriodBegin		4	4	{00..00}
└downloadPeriodEnd		4	4	{00..00}

▼B

TCS_179 Nedanstående värden, som används för att tillhandahålla storlekar i tabellen ovan, är de minsta och största numeriska värden som företagskortets datastruktur enligt generation 2 måste använda för posterna.

		Min.	Max.
n_8	NoOfCompanyActivityRecords	230	520

▼B

Tillägg 3

PIKTOGRAM

PIC_001 Färdskrivaren får som alternativ använda följande piktogram och kombinationer av piktogram (eller piktogram och sådana kombinationer av piktogram som är tillräckligt lika för att otvetydigt kunna identifieras med dessa).

1. GRUNDLÄGGANDE PIKTOGRAM

	Aktörer	**Verksamhet**	**Driftlägen**
	Företag		Företagsläge
	Kontrollant	Kontroll	Kontrolläge
	Förare	Körning	Driftläge
	Verkstad/provningsstation	Besiktning/kalibrering	Kalibreringsläge
	Tillverkare		

	Aktiviteter	**Varaktighet**
	Tillgänglig	Innevarande tillgänglighetsperiod
	Körning	Sammanhängande körtid
	Vila	Innevarande viloperiod
	Annat arbete	Innevarande arbetsperiod
	Rast	Sammanlagd avbrottstid
	Okänd	

	Utrustning	**Funktioner**
	Förarens kortplats	
	Medförarens kortplats	
	Kort	
	Klocka	
	Bildskärm	Visning
	Extern lagring	Överföring
	Strömtillförsel	
	Skrivare/utskrift	Utskrift
	Sensor	
	Däcksdimension	
	Fordon/fordonsenhet	
	GNSS-anordning	
	Anordning för fjärravläst tidig upptäckt	
	ITS-gränssnitt	

▼B

Särskilda omständigheter

OUT	Omfattas ej
	Transport med färja/tåg

Övrigt

	Händelser		Fel
	Start för arbetsperiod		Slut för arbetsperiod
	Plats		
	Manuell angivelse av föraraktiviteter		
	Säkerhet		
	Hastighet		
	Tidpunkt		
	Totalt/sammanfattning		

Precisering

24h	Gäller en dag
	Gäller en vecka
	Gäller två veckor
	Från eller till

2. KOMBINATIONER AV PIKTOGRAM

Övrigt

	Kontrollplats		
	Startplats för arbetsperiod		Slutplats för arbetsperiod
	Från (tidpunkt)		Till (tidpunkt)
	Från (fordon)		
	Perioden ”omfattas ej” börjar		Perioden ”omfattas ej” slutar

Kort

	Förarkort
	Företagskort
	Kontrollkort
	Verkstadskort
	Inget kort

Körning

	Körning med flera förare
	Körtid för en vecka
	Körtid för två veckor

▼B

	Utskrifter
24h	Dagsutskrift från kort av föraraktiviteter
24h	Dagsutskrift från fordonsenhet av föraraktiviteter
	Utskrift från kort av händelser och fel
	Utskrift från fordonsenhet av händelser och fel
	Utskrift av tekniska data
	Utskrift av hastighetsöverträdelse
	Händelser
	Insättning av ogiltigt kort
	Kortkonflikt
	Tidsöverlappning
	Körning utan korrekt kort
	Insättning av kort under körning
	Senaste kortsession ej korrekt avslutad
	Hastighetsöverträdelse
	Avbrott i strömtillförseln
	Fel i rörelsedata
	Konflikt i fordonets rörelsedata
	Säkerhetsöverträdelse
	Tidsinställning (av verkstad)
	Kontroll av hastighetsöverträdelse
	Fel
1	Kortfel (förarens kortplats)
2	Kortfel (medförarens kortplats)
	Bildskärmsfel
	Överföringsfel
	Skrivarfel
	Sensorfel
	Internt fel i fordonsenheten
	GNSS-fel
	Fel avseende fjärravläsning
	Manuella angivelser
?	Fortfarande samma arbetsperiod?
?	Slut på föregående arbetsperiod?
?	Bekräfta eller ange slutplats för arbetsperiod
?	Ange starttid
?	Ange startplats för arbetsperiod

Anmärkning: Ytterligare kombinationer av piktogram för att skapa utskriftsblock eller postidentifierare definieras i tillägg 4.

▼B

Tillägg 4

UTSKRIFTER

INNEHÅLLSFÖRTECKNING

1. ALLMÄNT

2. SPECIFIKATION FÖR DATABLOCK

3. SPECIFIKATIONER FÖR UTSKRIFTER

3.1. Dagsutskrift av föraraktiviteter från kort

3.2. Dagsutskrift av föraraktiviteter från fordonsenhet

3.3. Utskrift av händelser och fel från kort

3.4. Utskrift av händelser och fel från fordonsenhet

3.5. Utskrift av tekniska data

3.6. Utskrift av hastighetsöverträdelser

3.7. Historik över insatta kort

1. ALLMÄNT

Varje utskrift byggs upp genom sammankedjning av olika datablock, som eventuellt identifieras genom en blockidentifierare.

Ett datablock innehåller en eller flera poster, som eventuellt identifieras genom en postidentifierare.

PRT_001 När en blockidentifierare omedelbart föregår en postidentifierare skrivs postidentifieraren inte ut.

PRT_002 Om ett dataelement inte är känt, eller inte får skrivas ut på grund av rättigheter till datatillträde skrivs blanksteg ut i stället.

PRT_003 Om innehållet i en hel rad är okänt eller inte behöver skrivas ut utelämnas hela raden.

PRT_004 Numeriska datafält skrivs ut högerjusterade, med blanksteg för tusental och miljontal, och utan inledande nollor.

PRT_005 Strängdataelement skrivs ut vänsterjusterade och fylls med blanksteg till dataelementets längd, eller trunkeras vid behov till dataelementets längd (namn och adresser).

PRT_006 Vid radbrytning i en lång textsträng bör ett specialtecken (punkt mitt emellan baslinje och topplinje: ”•”) skrivas ut som första tecken på den nya raden.

2. SPECIFIKATION FÖR DATABLOCK

I detta kapitel används följande format och beteckningssätt:

— Tecken i **fetstil** anger vanlig text som ska skrivas ut som den visas.

▼B

— Vanliga tecken anger variabler (piktogram eller data) som ska ersättas med sina värden vid utskrift.

— Variabelnamn har strukits under för att visa den dataelementlängd som finns tillgänglig för variabeln.

— Data anges i formatet ”dd/mm/yyyy” (dag, månad, år). Formatet ”dd.mm.yyyy” får också användas.

— Termen ”kortidentifiering” (*card identification*) avser en sammansättning av korttypen (genom en kombination av piktogram), koden för den medlemsstat som utfärdat kortet, ett snedstreck och kortnummer med ersättningsindex och förnyelseindex, åtskilda med ett blanksteg.

P	■	x	x	x	/	x	x	x	x	x	x	x	x	x	x	x	x	x	x		x		x
Kombination av piktogram		Kod för utfärdande medlemsstat				Kortnumrets 14 första tecken (eventuellt med löpnummer)															Ersättningsindex		Förnyelseindex

▼B

PRT_007 Vid utskrift ska följande datablock och/eller dataposter användas, med följande betydelser och format:

Nummer på block eller post Betydelse	Dataformat
1 ***Datum och tidpunkt för utskrift av dokumentet***	▼ dd/mm/yyyy hh:mm **(UTC)**
2 ***Typ av utskrift*** Blockidentifierare Kombination av piktogram i utskriften (se tillägg 3): den hastighetsbegränsande anordningens inställning (endast vid utskrift av hastighetsöverträdelse)	----------▼---------- Picto xxx **km/h**
3 ***Identifiering av kortinnehavare*** Blockidentifierare P = piktogram för ”aktör” (*people*) Kortinnehavarens efternamn Kortinnehavarens förnamn (i förekommande fall) Kortidentifiering Kortets sista giltighetsdag (i förekommande fall) och generationsnummer (GEN 1 eller GEN 2) (*)	----------P---------- P Last_Name_____ First_Name_____ Card_Identification_____ dd/mm/yyyy - GEN 2

Om kortet är opersonligt och inte innehåller något efternamn på innehavaren, ska företagets, verkstadens eller kontrollorganets namn skrivas ut i stället.

(*) Kortets generationsnummer kan endast skrivas ut av en smart färdskrivare.

4 ***Fordonsidentifiering*** Blockidentifierare Fordonets identifieringsnummer (VIN) Registrerande medlemsstat och fordonets registreringsnummer (VRN)	----------▲---------- ▲ VIN_____ Nat/VRN_____
5 ***Identifiering av fordonsenhet*** Blockidentifierare Namn på fordonsenhetens tillverkare Fordonsenhetens artikelnummer Fordonsenhetens generationsnummer (*)	----------⊟---------- ⊟ VU_Manufacturer_____ VU_Part_Number__ GEN 2

(*) Kortets generationsnummer kan endast skrivas ut av en smart färdskrivare.

6 ***Senaste kalibrering av färdskrivaren*** Blockidentifierare Verkstadens namn Identifiering av verkstadskort Datum för kalibrering	----------▼---------- ▼ Last_Name_____ Card_Identification_____ ▼ dd/mm/yyyy

▼B

7 ***Senaste kontroll (av en kontrolltjänsteman)***

Blockidentifierare

Identifiering av kontrollantens (kontrolltjänstemannens) kort

Datum och tidpunkt för kontroll samt typ av kontroll

```
----------T----------
Card_Identification_____
T dd/mm/yyyy hh:mm ppppp
```

Typ av kontroll: Upp till fem piktogram. Kontrolltypen kan vara (en kombination av) följande:
▟: överföring från kort, ▼: överföring från fordonsenhet, T: utskrift, □: visning, ⊺: kalibreringskontroll på väg

8 ***Föraraktiviteter som finns lagrade på ett kort i den ordning de inträffat***

Blockidentifierare

Datum för förfrågan (kalenderdag för utskriften) + daglig närvaroräknare för kortet

```
----------⊙----------
    dd/mm/yyyy  xxx
```

8a Omständighet av typen ”omfattas ej” (*out of scope*) i början av den här dagen (lämnas tom om ingen omständighet av typen ”omfattas ej” har påbörjats)

```
----------OUT----------
```

8.1 *Period då kortet inte var insatt*

8,1 a Postidentifierare (periodens början)

8.1b *Okänd period* Starttid, varaktighet

8.1c *Manuellt angiven aktivitet*

Aktivitetspiktogram, starttid, varaktighet

```
  --------------------
?       hh:mm hhhmm
A       hh:mm hhhmm
```

8.2 *Insättning av kort i kortplats S*

Postidentifierare, S = piktogram för kortplats

Medlemsstat där fordonet är registrerat och fordonets registreringsnummer

Fordonets vägmätarvärde vid insättning av kortet

```
  ---------S---------
Nat/VRN___________

  x xxx xxx km
```

8.3 *Aktivitet (medan kortet var insatt)*

Aktivitetspiktogram, starttid, varaktighet, status för antal förare: piktogram för flera förare (för CREW) eller tomt (för SINGLE)

```
A       hh:mm hhhmm ⊙⊙
```

8,3 a *Särskild omständighet* Tidpunkt för angivelse, piktogram för särskild omständighet (eller kombination av piktogram)

```
        hh:mm ---pppp---
```

8.4 *Uttag av kort*

Fordonets vägmätarvärde och tillryggalagd sträcka sedan senaste insättning för vilken vägmätarvärdet är känt

```
  x xxx xxx km; x xxx km
```

9 ***Föraraktiviteter som finns lagrade i en fordonsenhet, per kortplats och i kronologisk följd***

Blockidentifierare

Datum för förfrågan (kalenderdag för utskriften)

Fordonets vägmätarvärde klockan 00:00 och 24:00

```
----------⊙----------
       dd/mm/yyyy
x xxx xxx - x xxx xxx km
```

10 ***Aktiviteter utförda i kortplats S***

Blockidentifierare

```
----------S----------
```

10 a Omständighet av typen ”omfattas ej” (*out of scope*) i början av den här dagen (lämnas tom om ingen omständighet av typen ”omfattas ej” har påbörjats)

```
----------OUT----------
```

10.1 *Period då inget kort var insatt i kortplats S*

Postidentifierare

Inget kort insatt

Fordonets vägmätarvärde i början av perioden

```
  --------------------
⊙▟---
  x xxx xxx km
```

10.2 *Insättning av kort*

Postidentifierare för insättning av kort

Förarens efternamn

```
  --------------------
⊙ Last_Name_____________
```

▼B

	Förarens förnamn	First_Name_____
	Identifiering av förarkort	Card_Identification_____
	Kortets sista giltighetsdag (i förekommande fall) och generationsnummer (GEN 1 eller GEN 2) (*)	dd/mm/yyyy - GEN 2
	Registrerande medlemsstat och registreringsnummer för föregående fordon som använts	Nat/VRN_____
	Datum och tidpunkt för uttag av kort i föregående fordon	dd/mm/yyyy hh:mm
	Tom rad	
	Fordonets vägmätarvärde vid insättning av kortet, markering för manuell angivelse av föraraktivitet (M för ja, tom för nej)	x xxx xxx **km** M
	Om inget förarkort sattes in under dagen för utskriften ska avläsningen av vägmätardata vid den senast tillgängliga kortinsättningen före den dagen användas för block 10.2.	
10.3	*Aktivitet*	
	Aktivitetspiktogram, starttid, varaktighet, status för antal förare: piktogram för flera förare (för CREW) eller tomt (för SINGLE)	A hh:mm hh**h**mm ⊙⊙
10,3 a	*Särskild omständighet* Tidpunkt för angivelse, piktogram för särskild omständighet (eller kombination av piktogram)	hh:mm ---pppp---
10.4	*Uttag av kort eller slut på period med "inget kort"*	
	Fordonets vägmätarvärde vid uttag av kort eller i slutet av period med "inget kort" och sträcka som tillryggalagts sedan insättning, eller sedan början av period med "inget kort"	x xxx xxx **km**; x xxx **km**

(*) Kortets generationsnummer kan endast skrivas ut av en smart färdskrivare.

11	***Dagssammanfattning***	
	Blockidentifierare	----------Σ----------
11.1	***Sammanfattning av fordonsenhetens perioder utan kort i förarens kortplats***	
	Blockidentifierare	1⊙▬---
11.2	***Sammanfattning av fordonsenhetens perioder utan kort i medförarens kortplats***	
	Blockidentifierare	2⊙▬---
11.3	***Dagssammanfattning för fordonsenheten, per förare***	
	Postidentifierare	----------
	Förarens efternamn	⊙ Last_Name_____
	Förarens förnamn	First_Name_____
	Identifiering av förarkort	Card_Identification_____
11.4	*Angivelse av plats där en arbetsperiod påbörjas och/eller avslutas*	
	pi = piktogram för plats för påbörjande/avslutande, tid, land, region	pihh:mm Cou Reg
	Vägmätarvärde	x xxx xxx **km**
11.5	*Angivelse av plats där en arbetsperiod påbörjas och/eller avslutas*	
	och efter tre timmars sammanhängande körtid	⁘ hh:mm
	Vägmätarvärde	x xxx xxx **km**

11.6	*Aktivitetssammanfattning (från ett kort)*	
	Sammanlagd varaktighet för körning, tillryggalagd sträcka	⊙ hh**h**mm x xxx **km**
	Total varaktighet för arbete och närvaro	⚒ hh**h**mm ⧈ hh**h**mm
	Total varaktighet för vila och okänd aktivitet	⊢ hh**h**mm ? hh**h**mm
	Total varaktighet för förarnas (*crew*) aktiviteter	⊙⊙ hh**h**mm
11.7	*Aktivitetssammanfattning (perioder utan kort, förarens kortplats)*	
	Sammanlagd varaktighet för körning, tillryggalagd sträcka	⊙ hh**h**mm x xxx **km**
	Total varaktighet för arbete och närvaro	⚒ hh**h**mm ⧈ hh**h**mm
	Total varaktighet för vila	⊢ hh**h**mm

▼B

11.8	*Aktivitetssammanfattning (perioder utan kort, medförarens kortplats)*	
	Total varaktighet för arbete och närvaro	`hhhmm  hhhmm`
	Total varaktighet för vila	`hhhmm`
11.9	*Aktivitetssammanfattning (per förare, båda kortplatserna medtagna)*	
	Sammanlagd varaktighet för körning, tillryggalagd sträcka	`hhhmm  x xxx km`
	Total varaktighet för arbete och närvaro	`hhhmm  hhhmm`
	Total varaktighet för vila	`hhhmm`
	Total varaktighet för förarnas (*crew*) aktiviteter	`hhhmm`

När en dagsutskrift begärs för innevarande dag beräknas informationen i sammanfattningen för dagen med hjälp av de data som finns tillgängliga vid tidpunkten för utskriften.

12	***Händelser och/eller fel som finns lagrade på ett kort***	
12.1	Blockidentifierare, senaste fem ”händelser och fel” från ett kort	`----------!×----------`
12.2	Blockidentifierare, alla registrerade ”händelser” på ett kort	`----------!----------`
12.3	Blockidentifierare, alla registrerade ”fel” på ett kort	`----------×----------`
12.4	*Post för händelse och/eller fel*	
	Postidentifierare	`----------`
	Piktogram för händelse/fel, postens syfte, datum och starttid	`Pic (p) dd/mm/yyyy hh:mm`
	Kod för ytterligare händelse/fel (i förekommande fall), varaktighet	`!xx  hhhmm`
	Registreringsnummer (VRN) och registrerande medlemsstat för det fordon där händelsen eller felet ägde rum	`Nat/VRN_____`

13	***Händelser och/eller fel som finns lagrade eller pågår i en fordonsenhet***	
13.1	Blockidentifierare, senaste fem ”händelser och fel” från en fordonsenhet	`----------!×----------`
13.2	Blockidentifierare, alla registrerade eller pågående ”händelser” i en fordonsenhet	`----------!----------`
13.3	Blockidentifierare, alla registrerade eller pågående ”fel” i en fordonsenhet	`----------×----------`
13.4	*Post för händelse och/eller fel*	
	Postidentifierare	`----------`
	Piktogram för händelse/fel, postens syfte, datum och starttid	`Pic (p) dd/mm/yyyy hh:mm`
	Ytterligare kod för händelse/fel (i förekommande fall), antal liknande händelser den här dagen, varaktighet	`!xx  (xxx)  hhhmm`
	Identifiering av insatta kort vid händelsens eller felets början eller slut (högst fyra rader utan repetition av kortnummer)	`Card_Identification_____`
		`Card_Identification_____`
		`Card_Identification_____`
		`Card_Identification_____`
	Om inget kort var insatt	`---`
	Tillverkarspecifika data	`< Literal><ErrorCode>`

Postens syfte (p) är en numerisk kod som förklarar varför händelsen eller felet registrerades och som kodas i enlighet med dataelementet `EventFaultRecordPurpose`.

`Literal` är en textsträng på högst 12 tecken som är specifik för färdskrivarens tillverkare.

`ErrorCode` är en felkod på högst 12 tecken som är specifik för färdskrivarens tillverkare.

▼B

14	***Identifiering av fordonsenhet***	
	Blockidentifierare	----------⊟----------
	Namn på fordonsenhetens tillverkare	⊟ Name_____
	Adress till fordonsenhetens tillverkare	Address_____
	Fordonsenhetens artikelnummer	PartNumber_____
	Fordonsenhetens typggodkännandenummer	Apprv_____
	Fordonsenhetens serienummer	S/N_____
	Fordonsenhetens tillverkningsår	yyyy
	Version och installationsdatum för fordonsenhetens programvara	V xxxx dd/mm/yyyy
15	***Identifiering av sensor***	
	Blockidentifierare	----------⅄----------
15.1	*Parningspost*	
	Sensorns serienummer	⅄ S/N_____
	Sensorns typgodkännandenummer	Apprv_____
	Sensorns parningsdatum	dd/mm/yyyy hh:mm
16	***Identifiering av GNSS***	
	Blockidentifierare	----------▚----------
16.1	*Kopplingspost*	
	Den externa GNSS-anordningens serienummer	▚ S/N_____
	Den externa GNSS-anordningens typgodkännandenummer	Apprv_____
	Den externa GNSS-anordningens kopplingsdatum	dd/mm/yyyy hh:mm
17	***Kalibreringsdata***	
	Blockidentifierare	----------⊤----------
17.1	*Kalibreringspost*	
	Postidentifierare	----------
	Verkstad som utfört kalibreringen	⊤ Workshop_name_____
	Verkstadens adress	Workshop_address_____
	Identifiering av verkstadskort	Card_Identification_____
	Verkstadskortets sista giltighetsdag	dd/mm/yyyy
	Tom rad	
	Kalibreringens datum och syfte	⊤ dd/mm/yyyy (p)
	Fordonets identifieringsnummer (VIN)	⅄ VIN_____
	Registrerande medlemsstat och fordonets registreringsnummer (VRN)	Nat/VRN_____
	Fordonets karakteristiska koefficient	w xx xxx Imp/km
	Färdskrivarens konstant	k xx xxx Imp/km
	Effective circumference of wheel tyres	l xx xxx mm
	Dimension för monterade däck	● TyreSize_____
	Inställning för hastighetsbegränsande anordning	› xxx km/h
	Vägmätarställning (gammal och ny)	x xxx xxx – x xxx xxx km

Kalibreringssyftet (p) är en numerisk kod som förklarar varför dessa kalibreringsparametrar registrerades och som kodas i enlighet med dataelementet `CalibrationPurpose`.

▼B

18	***Tidsinställning***	
	Blockidentifierare	`----------◷----------`
18.1	*Post för tidsinställning*	
	Postidentifierare	`--------------------`
	Datum och tidpunkt (gammal)	`!◷ dd/mm/yyyy hh:mm`
	Datum och tidpunkt (ny)	`◷ dd/mm/yyyy hh:mm`
	Verkstad som utfört tidsinställningen	`⍑ Workshop_name_____`
	Verkstadens adress	`Workshop_address_____`
	Identifiering av verkstadskort	`Card_Identification_____`
	Verkstadskortets sista giltighetsdag	`dd/mm/yyyy`
19	***Senaste händelse/fel som registrerats i fordonsenheten***	
	Blockidentifierare	`----------!×Д----------`
	Senaste händelse (datum och tidpunkt)	`! dd/mm/yyyy hh:mm`
	Senaste fel (datum och tidpunkt)	`× dd/mm/yyyy hh:mm`
20	***Information om kontroll av hastighetsöverträdelse***	
	Blockidentifierare	`----------»»----------`
	Datum och tidpunkt för senaste kontroll av hastighetsöverträdelse (*OVER SPEEDING CONTROL*)	`»▫dd/mm/yyyy hh:mm`
	Datum och tidpunkt för första hastighetsöverträdelse och antal hastighetsöverträdelser sedan dess	`»»dd/mm/yyyy hh:mm (nnn)`
21	***Post för hastighetsöverträdelse***	
21.1	Blockidentifierare: ”Första hastighetsöverträdelse efter senaste kalibrering”	`--------»»⍑---------`
21.2	Blockidentifierare: ”De fem mest allvarliga under de senaste 365 dygnen”	`-------»»(365)------`
21.3	Blockidentifierare: ”Den mest allvarliga för vart och ett av de senaste tio dygn där händelsen inträffat”	`-------»»(10)-------`
21.4	Postidentifierare	`--------------------`
	Datum, tidpunkt och varaktighet	`»»dd/mm/yyyy hh:mm hhhmm`
	Högsta hastighet och medelhastighet, antal liknande händelser den här dagen	`xxx km/h xxx km/h(xxx)`
	Förarens efternamn	`◙ Last_Name_____`
	Förarens förnamn	`First_Name_____`
	Identifiering av förarkort	`Card_Identification_____`
21.5	Om ingen post för hastighetsöverträdelse finns i ett block	`»»---`
22	***Handskriven information***	
	Blockidentifierare	`------------------------`
22.1	Kontrollplats	`▫• ..................`
22.2	Kontrollantens (kontrolltjänstemannens) namnteckning	`▫ ..................`
22.3	Från tidpunkt	`◷+ ..................`
22.4	Till tidpunkt	`+◷ ..................`
22.5	Förarens namnteckning	`◙ ..................`

Handskriven information: Inför tillräckligt många tomma rader ovanför en handskriven post så att det faktiskt går att ange den information som krävs eller att skriva en namnteckning.

▼B

23 ***Senaste kort (ett eller flera) som varit insatta i fordonsenheten***

Blockidentifierare

23.1 Insatt kort

Postidentifierare

Kortets typ, generation, version, tillverkare (*)

Kortidentifiering

Kortets serienummer

Datum och tidpunkt för senaste insättning av kortet

```
-------- ▯▮◔ --------


----
⍑ <gen> <version> <MC>
Card Identification
Card Serial Number
dd/mm/yyyy hh:mm
```

(*) (allt på en rad)

med

kortets typ: Piktogram, ett tecken + blanksteg

gen: GEN1 eller GEN2, 4 tecken + blanksteg

version: max. 10 tecken

MC: tillverkarens kod, 3 tecken

3. SPECIFIKATIONER FÖR UTSKRIFTER

I detta kapitel används följande beteckningssätt:

N	Utskriftsblock eller utskriftspost med nummer ”N”
N	Utskriftsblock eller utskriftspost med nummer ”N”, upprepad så många gånger som behövs
X/Y	Utskriftsblock eller utskriftsposter X och/eller Y efter behov, och upprepade så många gånger som behövs

3.1. **Dagsutskrift av föraraktiviteter från kort**

PRT_008 Dagsutskriften av föraraktiviteter från kort ska ske i följande format:

1	Datum och tidpunkt för utskrift av dokumentet
2	Typ av utskrift
3	Identifiering av kontrollant (kontrolltjänsteman) (om ett kontrollkort är insatt i fordonsenheten)
3	Identifiering av förare (från det kort som utskriften avser, 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 föraren
8	Gränstecken för föraraktiviteter
8a	Omständighet av typen ”omfattas ej” (OUT OF SCOPE) i början av den här dagen
8.1a / 8.1b / 8.1c / 8.2 / 8.3 / 8.3a / 8.4	Förarens aktiviteter i den ordning de inträffat
11	Gränstecken för dagssammanfattning

▼B

11.4	Angivna platser i kronologisk ordning
11.5	GNSS-data
11.6	Aktivitetssammanfattning
12.1	Gränstecken för händelser och fel från kort
12.4	Poster för händelser/fel (de fem senaste händelser eller fel som finns lagrade på kortet)
13.1	Gränstecken för händelser och fel från fordonsenhet
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
22.5	Förarens namnteckning

3.2. **Dagsutskrift av föraraktiviteter från fordonsenhet**

PRT_009 Dagsutskriften av föraraktiviteter från fordonsenhet ska ske i följande format:

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)
10 a	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)
10 a	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	GNSS-data

▼B

11.6	Aktivitetssammanfattning
11.2	Sammanfattning av perioder utan kort i medförarens kortplats
11.4	Angivna platser i kronologisk ordning
11.5	GNSS-data
11.7	Aktivitetssammanfattning
11.3	Sammanfattning av aktiviteter för en förare, båda kortplatserna
11.4	Platser som denna förare angivit i kronologisk ordning
11.5	GNSS-data
11.8	Aktivitetssammanfattning för denna förare
13.1	Gränstecken för händelser/fel
12.4	Poster för händelser/fel (de fem senaste händelser eller fel som finns lagrade eller är pågående i fordonsenheten)
13.1	Kontrollplats
22.2	Kontrollantens (kontrolltjänstemannens) namnteckning
22.3	Från tidpunkt (utrymme där en förare utan kort kan ange vilka perioder som gäller honom själv)
22.4	Till tidpunkt
22.5	Förarens namnteckning

3.3. **Utskrift av händelser och fel från kort**

PRT_010 Utskriften av händelser och fel från kort ska ske i följande format:

1	Datum och tidpunkt för utskrift av dokumentet
2	Typ av utskrift
3	Identifiering av kontrollant (kontrolltjänsteman) (om ett kontrollkort är insatt i fordonsenheten, samt generation)
3	Identifiering av förare (från det kort som utskriften avser)
4	Identifiering av fordonet (från vilket utskrift görs)
12.2	Gränstecken för händelser
12.4	Poster för händelser (alla händelser som finns lagrade på kortet)
12.3	Gränstecken för fel
12.4	Poster för fel (alla fel som finns lagrade på kortet)
22.1	Kontrollplats
22.2	Kontrollantens (kontrolltjänstemannens) namnteckning
22.5	Förarens namnteckning

▼B

3.4. **Utskrift av händelser och fel från fordonsenhet**

PRT_011 Utskriften av händelser och fel från fordonsenhet ska ske i följande format:

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)
13.2	Gränstecken för händelser
13.4	Poster för händelser (alla händelser som finns lagrade eller är pågående i fordonsenheten)
13.3	Gränstecken för fel
13.4	Poster för fel (alla fel som finns lagrade eller är pågående i fordonsenheten)
22.1	Kontrollplats
22.2	Kontrollantens (kontrolltjänstemannens) namnteckning
22.5	Förarens namnteckning

3.5. **Utskrift av tekniska data**

PRT_012 Utskrift av tekniska data ska ske i följande format:

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)
14	Identifiering av fordonsenhet
15	Identifiering av sensor
15.1	Sensorns parningsdata (alla tillgängliga data i kronologisk ordning)
16	Identifiering av GNSS
16.1	Den externa GNSS-anordningen kopplingsdata (alla tillgängliga data i kronologisk ordning)
17	Gränstecken för kalibreringsdata
17.1	Kalibreringsposter (alla tillgängliga poster i kronologisk ordning)
18	Gränstecken för tidsinställning
18.1	Poster för tidsinställningar (alla tillgängliga poster från tidsinställningar och från kalibreringsposter)
19	Senaste händelse/fel som registrerats i fordonsenheten

▼B

3.6. **Utskrift av hastighetsöverträdelser**

PRT_013 Utskriften av hastighetsöverträdelser ska ske i följande format:

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)
20	Information om kontroll av hastighetsöverträdelse
21.1	Identifiering av data om hastighetsöverträdelser
21.4 / 21.5	Första hastighetsöverträdelse efter senaste kalibrering
21.2	Identifiering av data om hastighetsöverträdelser
21.4 / 21.5	De fem mest allvarliga hastighetsöverträdelserna under de senaste 365 dygnen
21.3	Identifiering av data om hastighetsöverträdelser
21.4 / 21.5	Den allvarligaste hastighetsöverträdelsen för vart och ett av de senaste tio dygn där en hastighetsöverträdelse inträffat
22.1	Kontrollplats
22.2	Kontrollantens (kontrolltjänstemannens) namnteckning
22.5	Förarens namnteckning

3.7. **Historik över insatta kort**

PRT_014 Utskriften av historik över insatta kort ska ske i följande format:

1	Datum och tidpunkt för utskrift av dokumentet
2	Typ av utskrift
3	Identifieringar av kortinnehavare (för alla kort som har satts in i fordonsenheten)
23	Senaste kort som varit insatt i fordonsenheten
23.1	Insatta kort (max. 88 poster)
12.3	Gränstecken för fel

▼B

Tillägg 5

BILDSKÄRM

I detta tillägg används följande format och beteckningssätt:

— Tecken i **fetstil** anger vanlig text som ska visas med vanliga tecken (inte i fetstil).

— Vanliga tecken anger variabler (piktogram eller data) som vid visning ska ersättas med sina värden.

  — dd mm yyyy: dag, månad, år

  — hh: timmar

  — mm: minuter

  — D: piktogram för varaktighet

  — EF: kombination av piktogram för händelser eller fel

  — O: piktogram för funktionsläge

DIS_001 Färdskrivaren ska visa data i följande format:

Data	Format
Standardvisning	
Lokal tid	hh:mm
Funktionsläge	O
Information om föraren:	1 Dhh**h**mm ▮▮hh**h**mm
Information om medföraren:	2 Dhh**h**mm
Omständigheten ”omfattas ej” påbörjad	OUT
Visning av varningar	
Sammanhängande körtid överskrids	1 ⊙hh**h**mm ▮▮hh**h**mm
Händelse eller fel	EF
Visning av övrig information	
UTC-datum Tid	UTC ⊙ dd/mm/yyyy eller UTC ⊙ dd.mm.yyyy hh:mm
Förarens sammanhängande körtid och sammanlagda avbrottstid	1 ⊙ hh**h**mm ▮▮hh**h**mm
Medförarens sammanhängande körtid och sammanlagda avbrottstid	2 ⊙ hh**h**mm ▮▮hh**h**mm
Förarens sammanlagda körtid för föregående och innevarande vecka	1 ⊙ ▮ hhh**h**mm
Medförarens sammanlagda körtid för föregående och innevarande vecka	2 ⊙ ▮ hhh**h**mm

▼B

Tillägg 6

FRONTANSLUTNING FÖR KALIBRERING OCH DATAÖVERFÖRING

INNEHÅLLSFÖRTECKNING

1 MASKINVARA

1.1 Anslutning

1.2 Tilldelning av kontakter

1.3 Blockdiagram

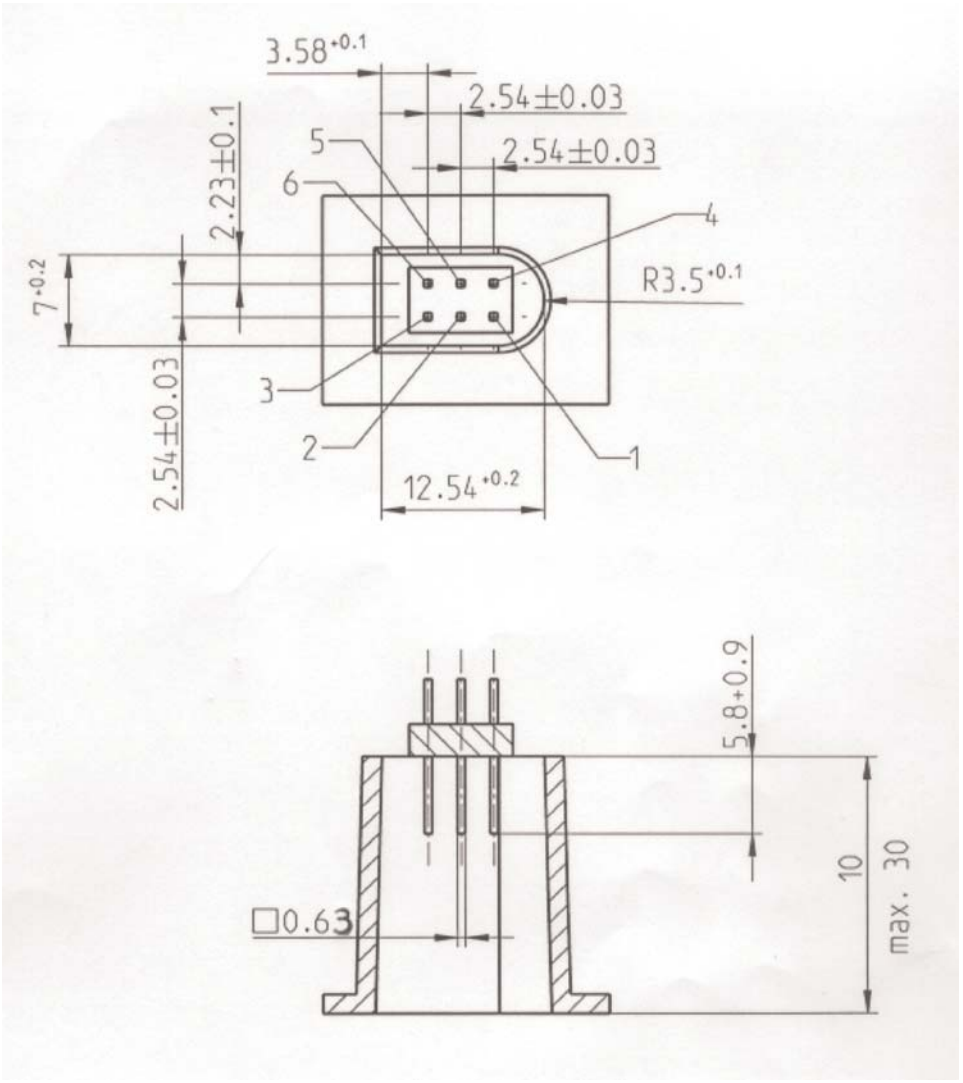
2 GRÄNSSNITT FÖR DATAÖVERFÖRING

3 GRÄNSSNITT FÖR KALIBRERING

1 MASKINVARA

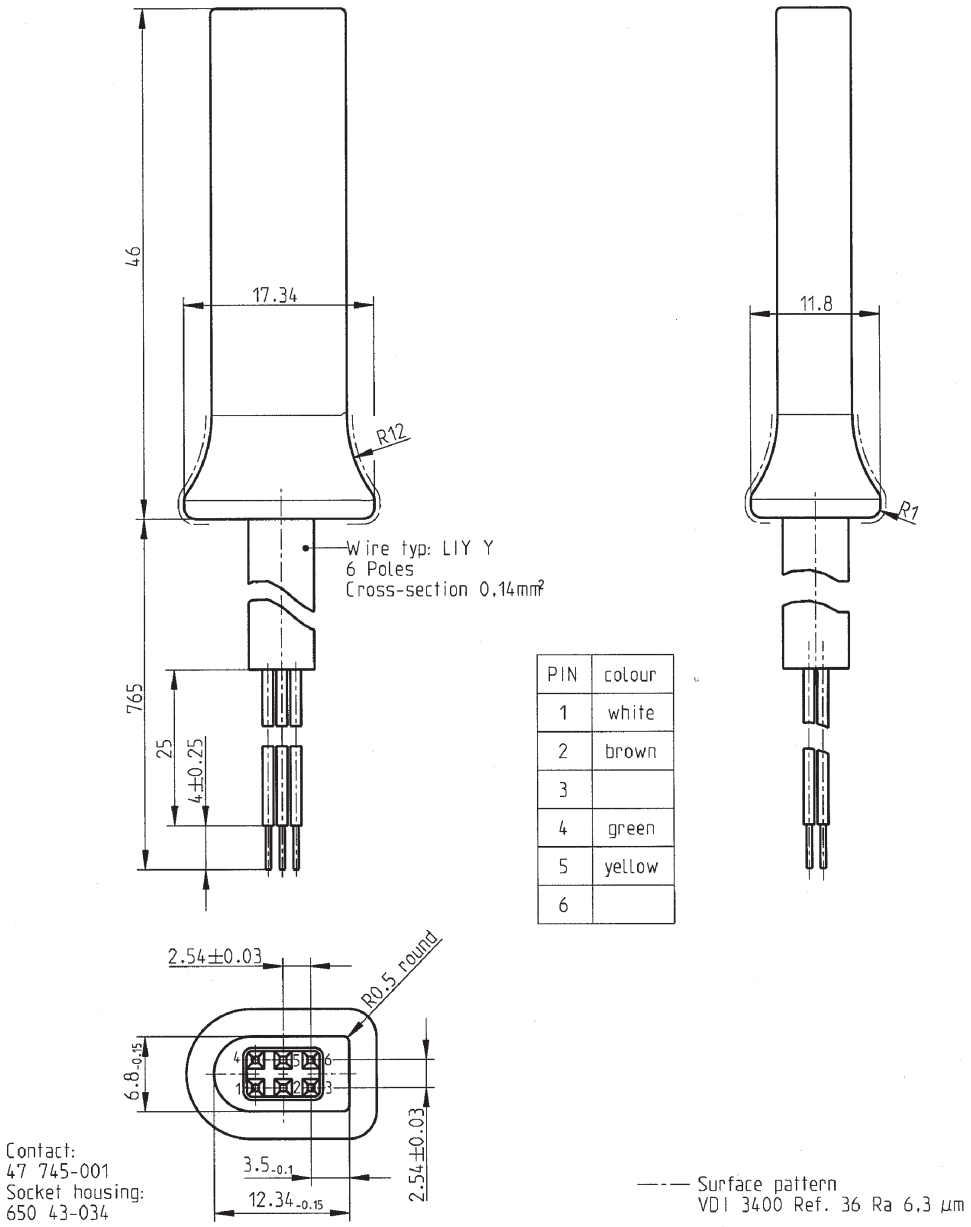
1.1 **Anslutning**

INT_001 Kalibrerings-/överföringsanslutningen ska vara en 6-stiftsanslutning, som är åtkomlig på frontpanelen utan att man behöver koppla ur någon del av färdskrivaren, och den ska överensstämma med följande ritning (alla mått i millimeter).



▼B

I följande ritning visas en typisk matchande kontakt med 6 stift:



1.2 **Tilldelning av kontakter**

INT_002 Kontakterna ska tilldelas enligt följande tabell:

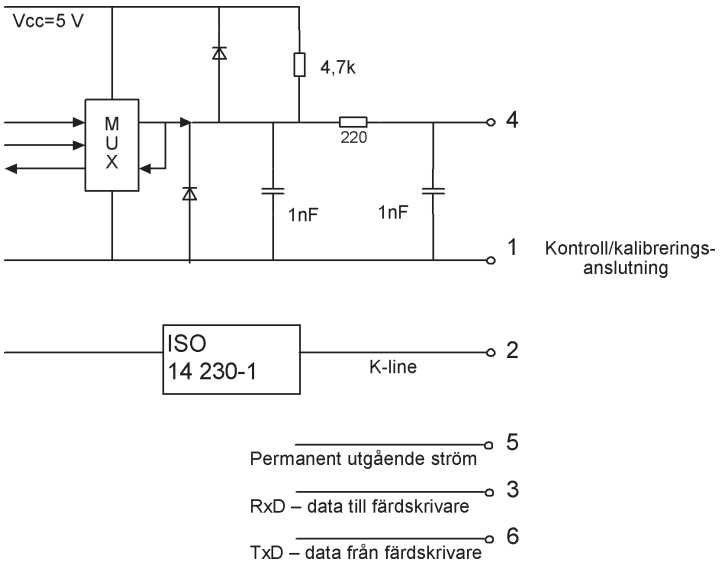
Stift	Beskrivning	Anmärkning
1	Batteriminus	Ansluten till fordonets batteriminus
2	Datakommunikation	K-line (ISO 14230-1)
3	RxD – dataöverföring	Indata till färdskrivaren
4	In-/utsignal	Kalibrering

▼B

Stift	Beskrivning	Anmärkning
5	Permanent utgående ström	Spänningsintervallet specificeras till fordonets spänning, minskad med 3 V för spänningsfallet över skyddskretsen. Utgående ström 40 mA.
6	TxD – dataöverföring	Utdata från färdskrivaren

1.3 **Blockdiagram**

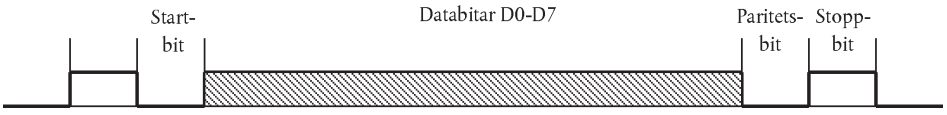
INT_003 Blockdiagrammet ska överensstämma med följande diagram:



2 GRÄNSSNITT FÖR DATAÖVERFÖRING

INT_004 Gränssnittet för dataöverföring ska överensstämma med RS232-specifikationerna.

INT_005 Gränssnittet för dataöverföring ska använda 1 startbit, 8 databitar med minst signifikanta bit (LSB) först, 1 jämn paritetsbit och 1 stoppbit.



Organisering av byte för data

Startbit: 1 bit med logisk nivå 0.

Databitar: överförs med LSB först.

Paritetsbit: jämn paritet.

Stoppbit: 1 bit med logisk nivå 1.

Vid överföring av numeriska data som är sammansatta av mer än en byte överförs mest signifikanta byte först och minst signifikanta byte sist.

INT_006 Överföringshastigheterna ska vara justerbara från 9 600 bps till 115 200 bps. Överföringen ska ske med största möjliga överföringshastighet, med den inledande hastigheten efter kommunikationsstart satt till 9 600 bps.

▼B

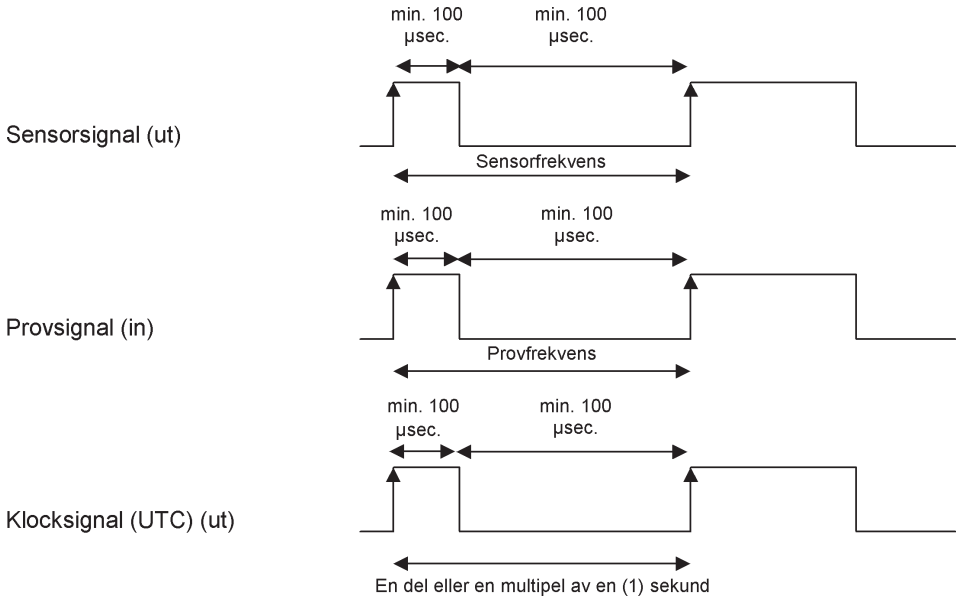
3 GRÄNSSNITT FÖR KALIBRERING

INT_007 Datakommunikationen ska överensstämma med ISO 14230-1 *Road vehicles – Diagnostic systems – Keyword protocol 2000 – Part 1: Physical layer, First edition: 1999*.

INT_008 In-/utsignalen ska överensstämma med följande elektriska specifikation:

Parameter	Min.	Typisk	Max.	Anmärkning
U_{low} (in)			1,0 V	I = 750 µA
U_{high} (in)	4 V			I = 200 µA
Frekvens			4 kHz	
U_{low} (ut)			1,0 V	I = 1 mA
U_{high} (ut)	4 V			I = 1 mA

INT_009 In-/utsignalen ska överensstämma med följande tidsdiagram:



▼B

Tillägg 7

PROTOKOLL FÖR DATAÖVERFÖRING

INNEHÅLLSFÖRTECKNING

1. INLEDNING

1.1. Tillämpningsområde

1.2. Förkortningar och beteckningar

2. ÖVERFÖRING AV DATA FRÅN FORDONSENHET

2.1. Överföringsförfarande

2.2. Protokoll för dataöverföring

2.2.1 Meddelandestruktur

2.2.2 Meddelandetyper

2.2.2.1 Start Communication Request (SID 81)

2.2.2.2 Positive Response Start Communication (SID C1)

2.2.2.3 Start Diagnostic Session Request (SID 10)

2.2.2.4 Positive Response Start Diagnostic (SID 50)

2.2.2.5 Link Control Service (SID 87)

2.2.2.6 Link Control Positive Response (SID C7)

2.2.2.7 Request Upload (SID 35)

2.2.2.8 Positive Response Request Upload (SID 75)

2.2.2.9 Transfer Data Request (SID 36)

2.2.2.10 Positive Response Transfer Data (SID 76)

2.2.2.11 Request Transfer Exit (SID 37)

2.2.2.12 Positive Response Request Transfer Exit (SID 77)

2.2.2.13 Stop Communication Request (SID 82)

2.2.2.14 Positive Response Stop Communication (SID C2)

2.2.2.15 Acknowledge Sub Message (SID 83)

2.2.2.16 Negative Response (SID 7F)

2.2.3 Meddelandeflöde

2.2.4 Tidsavpassning

▼B

2.2.5 Felhantering

2.2.5.1 Startfas för kommunikation

2.2.5.2 Kommunikationsfas

2.2.6 Innehåll i svarsmeddelande

2.2.6.1 Positive Response Transfer Data – Overview

2.2.6.2 Positive Response Transfer Data – Activities

2.2.6.3 Positive Response Transfer Data – Events and Faults

2.2.6.4 Positive Response Transfer Data – Detailed Speed

2.2.6.5 Positive Response Transfer Data – Technical Data

2.3. Fillagring på externt lagringsmedium

3. PROTOKOLL FÖR ÖVERFÖRING FRÅN FÄRDSKRIVARKORT

3.1. Tillämpningsområde

3.2. Definitioner

3.3. Överföring från kort

3.3.1 Initieringssekvens

3.3.2 Sekvens för osignerade datafiler

3.3.3 Sekvens för signerade datafiler

3.3.4 Sekvens för återställning av kalibreringsräknare

3.4. Format för lagring av data

3.4.1 Inledning

3.4.2 Filformat

4. ÖVERFÖRING FRÅN ETT FÄRDSKRIVARKORT VIA EN FORDONSENHET

1. INLEDNING

I detta tillägg specificeras de förfaranden som måste följas för att utföra de olika typerna av dataöverföring till ett externt lagringsmedium (ESM, *External Storage Medium*), och de protokoll som måste användas för att säkerställa korrekt dataöverföring och full kompatibilitet hos överfört dataformat, så att alla kontrollanter (kontrolltjänstemän) ska kunna besiktiga dessa data och kontrollera deras autenticitet och integritet innan de analyserar dem.

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*).

▼B

— 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.

DDP_001 Data som överförs under en överföringssession måste lagras på det externa lagringsmediet inom en enda fil.

1.2. **Förkortningar och beteckningar**

Följande förkortningar används i detta tillägg:

AID *Application Identifier* (tillämpningsidentifierare)

ATR *Answer To Reset* (återställningssignal)

CS *Checksum byte* (byte för kontrollsumma)

DF *Dedicated File* (dedikerad fil)

DS_ *Diagnostic Session* (diagnossession)

EF *Elementary File* (elementfil)

ESM *External Storage Medium* (externt lagringsmedium)

FID *File Identifier (File ID)* (filidentifierare)

FMT *Format Byte* (byte för format, första byte i ett meddelandes startdel (*header*))

ICC *Integrated Circuit Card* (smartkort, kort med integrerade kretsar)

IDE *Intelligent Dedicated Equipment* (utrustning för att överföra data till ett externt lagringsmedium, exempelvis en persondator)

IFD *Interface Device* (kortläsare)

KWP Keyword Protocol 2000

LEN *Length Byte* (byte för längd, sista byte i ett meddelandes startdel (*header*))

PPS *Protocol Parameter Selection* (val av protokollparameter)

PSO *Perform Security Operation* (kommando för säkerhetsoperation)

SID *Service Identifier* (tjänsteidentifierare)

SRC *Source byte* (byte för källadress)

TGT *Target Byte* (byte för måladress)

TLV *Tag Length Value* (tagglängd)

TREP *Transfer Response Parameter* (parameter för överföringssvar)

TRTP *Transfer Request Parameter* (parameter för begäran om överföring)

VU *Vehicle Unit* (fordonsenhet)

▼B

2. ÖVERFÖRING AV DATA FRÅN FORDONSENHET

2.1. **Överföringsförfarande**

För att överföra data från en fordonsenhet måste användaren göra följande:

— Sätta in sitt färdskrivarkort i en kortplats i fordonsenheten (*).

— Ansluta IDE-enhet till fordonsenhetens överföringsanslutning.

— Upprätta en anslutning mellan IDE-enhet och fordonsenhet.

— På IDE-enheten välja de data som ska överföras och sända begäran till fordonsenheten.

— Avsluta överföringssessionen.

2.2. **Protokoll för dataöverföring**

Protokollet är uppbyggt enligt modellen ”master-slave”, med IDE-enheten som ”master” och fordonsenheten som ”slave”.

Meddelandestruktur, meddelandetyper och meddelandeflöden bygger huvudsakligen på *Keyword Protocol 2000* (KWP) (ISO 14230-2 *Road vehicles – Diagnostic systems – Keyword protocol 2000 – Part2: Data link layer*).

Tillämpningsskiktet grundas i princip på det gällande utkastet till ISO 14229-1 (*Road vehicles – Diagnostic systems – Part 1: Diagnostic services*, version 6 av den 22 februari 2001).

2.2.1 *Meddelandestruktur*

DDP_002 Alla meddelanden som utbyts mellan IDE-enhet och fordonsenhet formateras med en struktur som består av följande tre delar:

— Startdel (*header*) bestående av en byte för format (FMT), en byte för mål (TGT), en byte för källa (SRC) och eventuellt en byte för längd (LEN).

— Datafält bestående av en byte för tjänsteidentifierare (SID) och ett varierande antal byte för data, som kan inbegripa en byte för diagnossession (DS_) eller en valfri byte för överföringsparameter (TRTP eller TREP).

— Kontrollsumma bestående av en byte för kontrollsumma (CS).

Startdel (*header*)				Datafält					Kontrollsumma
FMT	TGT	SRC	LEN	SID	DATA	…	…	…	CS
4 byte				Max. 255 byte					1 byte

Byte för TGT och SRC representerar den fysiska adressen till meddelandets mottagare och avsändare. Värdena är F0 Hex för IDE-enheten och EE Hex för fordonsenheten (VU).

Byte för LEN är längden på datafältsdelen.

Byte för CS innehåller 8 bits-summorna modulo 256 av alla byte i meddelandet, med undantag för CS själv.

Byte för FMT, SID, DS_, TRTP och TREP definieras nedan i detta dokument.

(*) Det kort som sätts in aktiverar lämpliga rättigheter till överföringsfunktionen och till data. Det ska dock vara möjligt att överföra data från ett förarkort som sätts in i en av fordonsenhetens kortplatser när inget annat kort finns i den andra kortplatsen.

▼B

DDP_003 I de fall där de data som ska överföras i meddelandet är längre än det utrymme som finns tillgängligt i datafältsdelen sänds meddelandet i själva verket i flera undermeddelanden. Varje undermeddelande har en startdel (*header*), samma SID, TREP och en undermeddelanderäknare på 2 byte som anger undermeddelandenummer inom hela meddelandet. IDE-enheten kvitterar varje undermeddelande för att ge en möjlighet att felkontrollera och avbryta. IDE-enheten kan godta undermeddelandet, be att det överförs igen, begära att fordonsenheten startar igen eller avbryta överföringen.

DDP_004 Om det sista undermeddelandet innehåller exakt 255 byte i datafältet måste ett slutgiltigt undermeddelande med ett tomt (förutom SID, TREP och undermeddelanderäknare) datafält tillfogas för att visa slutet på meddelandet.

Exempel:

Startdel (*header*)	SID	TREP	Meddelande	CS
4 byte	Längre än 255 byte			

Kommer att överföras som

Startdel (*header*)	SID	TREP	00	01	Undermeddelande 1	CS
4 byte	255 byte					

Startdel (*header*)	SID	TREP	00	02	Undermeddelande 2	CS
4 byte	255 byte					

…

Startdel (*header*)	SID	TREP	xx	yy	Undermeddelande n	CS
4 byte	Mindre än 255 byte					

eller som

Startdel (*header*)	SID	TREP	00	01	Undermeddelande 1	CS
4 byte	255 byte					

Startdel (*header*)	SID	TREP	00	02	Undermeddelande 2	CS
4 byte	255 byte					

…

Startdel (*header*)	SID	TREP	xx	yy	Undermeddelande n	CS
4 byte	255 byte					

Startdel (*header*)	SID	TREP	xx	yy + 1	CS
4 byte	4 byte				

▼B

2.2.2 *Meddelandetyper*

Kommunikationsprotokollet för dataöverföring mellan fordonsenhet och IDE-enhet förutsätter utbyte av åtta olika meddelandetyper.

Dessa meddelanden sammanfattas i följande tabell.

Meddelandestruktur	Max. 4 byte Startdel (*header*)				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	9 B
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
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	0 A	35		00,00,00,00, 00,FF,FF,FF, FF	99
Positive Response Request Upload	80	F0	EE	03	75		00,FF	D5
Transfer Data Request								
Overview	80	EE	F0	02	36	01		97
Activities	80	EE	F0	06	36	02	Date	CS
Events & Faults	80	EE	F0	02	36	03		99
Detailed Speed	80	EE	F0	02	36	04		9 A
Technical Data	80	EE	F0	02	36	05		9 B
Card download	80	EE	F0	02	36	06	Slot	CS
Positive Response Transfer Data	80	F0	EE	Len	76	TREP	Data	CS
Request Transfer Exit	80	EE	F0	01	37			96
Positive Response Request Transfer Exit	80	F0	EE	01	77			D6

▼B

Meddelandestruktur	Max. 4 byte Startdel (*header*)				Max. 255 byte Data			1 byte Kontrollsumma
IDE -> <- VU	FMT	TGT	SRC	LEN	SID	DS_/TRTP	DATA	CS
Stop Communication Request	80	EE	F0	01	82			E1
Positive Response Stop Communication	80	F0	EE	01	C2			21
Acknowledge sub message	80	EE	F0	Len	83		Data	CS
Negativa svar								
Allmänt avvisande (*General reject*)	80	F0	EE	03	7F	Sid Req	10	CS
Tjänsten stöds ej (*Service not supported*)	80	F0	EE	03	7F	Sid Req	11	CS
Underfunktion stöds ej (*Sub function not supported*)	80	F0	EE	03	7F	Sid Req	12	CS
Fel meddelandelängd (*Incorrect Message Length*)	80	F0	EE	03	7F	Sid Req	13	CS
Fel omständigheter eller sekvensfel för begäran (*Conditions not correct or Request sequence error*)	80	F0	EE	03	7F	Sid Req	22	CS
Begäran utanför tillåtet intervall (*Request out of range*)	80	F0	EE	03	7F	Sid Req	31	CS
Överföring ej accepterad (*Upload not accepted*)	80	F0	EE	03	7F	Sid Req	50	CS
Svar dröjer (*Response pending*)	80	F0	EE	03	7F	Sid Req	78	CS
Data ej tillgängliga (*Data not available*)	80	F0	EE	03	7F	Sid Req	FA	CS

Anmärkningar:

— Sid Req = SID för motsvarande begäran.

— TREP = TRTP för motsvarande begäran.

— Mörka fält betecknar att inget överförs.

— Termen ”överföring” motsvarar uppladdning (*upload*), sett från IDE-enheten, i ISO 14229. Den betyder även nedladdning (*download*), sett från fordonsenheten.

— Eventuella 2-bytes undermeddelanderäknare visas inte i tabellen.

— *Slot* står för kortplatsnummer, antingen ”1” (kort i förarens kortplats) eller ”2” (kort i medförarens kortplats).

— Om kortplatsen inte anges ska fordonsenheten välja kortplats 1 om ett kort finns i denna kortplats, och välja kortplats 2 endast om denna väljs specifikt av användaren.

2.2.2.1 Start Communication Request (SID 81)

DDP_005 IDE-enheten utfärdar detta meddelande för att upprätta kommunikationslänken med fordonsenheten. De första meddelandena utväxlas alltid med 9 600 baud (tills överföringshastigheten eventuellt ändras med hjälp av meddelandet *Link Control Services* och lämpligt värde).

▼B

2.2.2.2 Positive Response Start Communication (SID C1)

DDP_006 Fordonsenheten utfärdar detta meddelande för att svara positivt på en begäran om att starta kommunikationen. Det inbegriper de två byte för nyckel (‘EA’ ‘8F’) som anger att enheten stöder protokoll med startdel (*header*) som innehåller information om mål, källa och längd.

2.2.2.3 Start Diagnostic Session Request (SID 10)

DDP_007 IDE-enheten utfärdar meddelandet *Start Diagnostic Session Request* för att begära en ny diagnossession med fordonsenheten. Underfunktionen för standardsession (81 Hex) anger att en diagnossession av standardtyp ska öppnas.

2.2.2.4 Positive Response Start Diagnostic (SID 50)

DDP_008 Fordonsenheten sänder meddelandet *Positive Response Start Diagnostic* som positivt svar på *Start Diagnostic Session Request*.

2.2.2.5 Link Control Service (SID 87)

DDP_052 IDE-enheten använder *Link Control Service* för att inleda en ändring av överföringshastigheten. Detta sker i två steg: I steg 1 föreslår IDE-enheten ändringen av överföringshastigheten (*baud rate*) och anger den nya hastigheten. Vid mottagandet av ett positivt svar från fordonsenheten sänder IDE-enheten en bekräftelse av ändringen av överföringshastigheten till fordonsenheten (steg 2). Därefter ändrar IDE-enheten till den nya överföringshastigheten. Efter mottagandet av bekräftelsen ändrar fordonsenheten till den nya överföringshastigheten.

2.2.2.6 Link Control Positive Response (SID C7)

DDP_053 Fordonsenheten utfärdar meddelandet *Link Control Positive Response* för att svara positivt på en begäran via *Link Control Service* (steg 1). Notera att inget svar lämnas på begäran om bekräftelse (steg 2).

2.2.2.7 Request Upload (SID 35)

DDP_009 IDE-enheten utfärdar meddelandet *Request Upload* för att specificera för fordonsenheten att en överföring begärs. För att uppfylla kraven i ISO 14229 ingår data som omfattar adress, storlek och format för de data som begärs. Eftersom dessa inte är kända av IDE-enheten före en överföring är minnesadressen inställd på 0, formatet är okrypterat och okomprimerat och minnesstorleken är inställd på maximal storlek.

2.2.2.8 Positive Response Request Upload (SID 75)

DDP_010 Fordonsenheten sänder meddelandet *Positive Response Request Upload* för att ange för IDE-enheten att fordonsenheten är beredd att överföra data. För att uppfylla kraven i ISO 14229 ingår data i detta positiva svarsmeddelande som anger för IDE-enheten att ytterligare meddelanden av typen *Positive Response Transfer Data* kommer att omfatta högst 00FF byte (hex).

▼B

2.2.2.9 Transfer Data Request (SID 36)

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:

— *Overview* (TRTP 01) (översikt).

— *Activities of a specified date* (TRTP 02) (aktiviteter med avseende på ett särskilt datum).

— *Events and faults* (TRTP 03) (händelser och fel).

— *Detailed speed* (TRTP 04) (detaljerade hastighetsdata).

— *Technical data* (TRTP 05) (tekniska data).

— *Card download* (TRTP 06) (överföring från kort).

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

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

2.2.2.10 Positive Response Transfer Data (SID 76)

DDP_012 Fordonsenheten sänder meddelandet *Positive Response Transfer Data* som svar på *Transfer Data Request*. Meddelandet innehåller begärda data, med en parameter för överföringssvar (TREP) som motsvarar TRTP i begäran.

DDP_055 I det första fallet (TREP 01) 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.

▼B

2.2.2.11 Request Transfer Exit (SID 37)

DDP_013 IDE-enheten sänder meddelandet *Request Transfer Exit* för att informera fordonsenheten om att överföringssessionen avslutas.

2.2.2.12 Positive Response Request Transfer Exit (SID 77)

DDP_014 Fordonsenheten sänder meddelandet *Positive Response Request Transfer Exit* för att kvittera *Request Transfer Exit*.

2.2.2.13 Stop Communication Request (SID 82)

DDP_015 IDE-enheten sänder meddelandet *Stop Communication Request* för att koppla ned kommunikationslänken med fordonsenheten.

2.2.2.14 Positive Response Stop Communication (SID C2)

DDP_016 Fordonsenheten sänder meddelandet *Positive Response Stop Communication* för att kvittera *Stop Communication Request*.

2.2.2.15 Acknowledge Sub Message (SID 83)

DDP_017 IDE-enheten sänder meddelandet *Acknowledge Sub Message* för att bekräfta mottagandet av varje del av ett meddelande som överförs som flera undermeddelanden. Datafältet innehåller SID som mottagits från fordonsenheten och en kod på 2 byte enligt följande:

— ”MsgC + 1” kvitterar korrekt mottagande av undermeddelande nummer ”MsgC”.

Begäran från IDE-enheten till fordonsenheten att sända nästa undermeddelande.

— ”MsgC” anger att ett problem uppstått med mottagande av undermeddelande nummer ”MsgC”.

Begäran från IDE-enheten till fordonsenheten att sända undermeddelandet igen.

— ”FFFF” begär att meddelandet avslutas.

Detta kan användas av IDE-enheten för att avsluta överföringen av fordonsenhetens meddelande av vilken orsak som helst.

Det sista undermeddelandet i ett meddelande (byte för LEN < 255) får kvitteras med hjälp av någon av dessa koder eller inte kvitteras alls.

De svar från fordonsenheten som kommer att bestå av flera undermeddelanden är följande:

— Positive Response Transfer Data (SID 76)

▼B

2.2.2.16 Negative Response (SID 7F)

DDP_018 Fordonsenheten sänder meddelandet *Negative Response* som svar på ovan nämnda meddelande om begäran när fordonsenheten inte kan tillmötesgå begäran. Meddelandets datafält innehåller svarets SID (7F), SID för begäran och en kod som specificerar orsaken till det negativa svaret. Följande koder finns tillgängliga:

— 10 Allmänt avvisande

Åtgärden kan inte utföras, till följd av en anledning som inte omfattas nedan.

— 11 Tjänsten stöds ej

SID för begäran ej förstådd.

— 12 Underfunktion stöds ej

DS_ eller TRTP för begäran är inte förstådd, eller det finns inga ytterligare undermeddelanden som ska överföras.

— 13 Fel meddelandelängd

Längden på det mottagna meddelandet är felaktig.

— 22 Fel omständigheter eller sekvensfel för begäran

Den begärda tjänsten är inte aktiv eller sekvensen av meddelanden om begäran är felaktig.

— 31 Begäran utanför tillåtet intervall

Posten med parameter för begäran (datafält) är inte giltig.

— 50 Överföring ej accepterad

Begäran kan inte utföras (fordonsenheten i olämpligt funktionsläge eller internt fel i fordonsenheten).

— 78 Svar dröjer

Begärd åtgärd kan inte fullgöras i tid och fordonsenheten är inte beredd att godta en annan begäran.

— FA Data ej tillgängliga

Dataobjektet i en begäran om dataöverföring finns inte tillgängligt i fordonsenheten (t.ex.: inget kort har satts in, …).

2.2.3 *Meddelandeflöde*

Nedan visas ett typiskt meddelandeflöde under en normal dataöverföring:

IDE-enhet		Fordonsenhet (VU)
Start Communication Request	⇨	
	⇦	Positive Response
Start Diagnostic Service Request	⇨	
	⇦	Positive Response
Request Upload	⇨	
	⇦	Positive Response

▼B

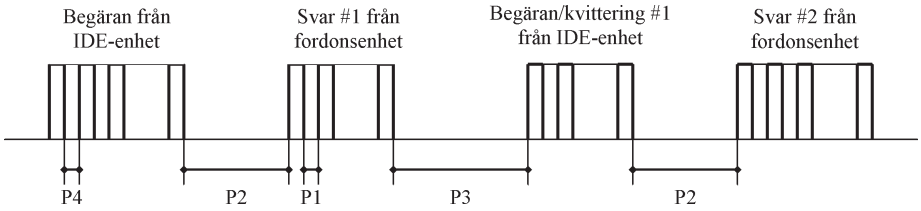
IDE-enhet		Fordonsenhet (VU)
Transfer Data Request – Overview	⇨ ⇦	Positive Response
Transfer Data Request #2	⇨	
	⇦	*Positive Response* #1
Acknowledge Sub Message #1	⇨	
	⇦	*Positive Response* #2
Acknowledge Sub Message #2	⇨	
	⇦	*Positive Response* #m
Acknowledge Sub Message #m	⇨	
	⇦	*Positive Response* (datafält < 255 byte)
Acknowledge Sub Message (frivilligt)	⇨	
…		
Transfer Data Request #n	⇨ ⇦	Positive Response
Request Transfer Exit	⇨ ⇦	Positive Response
Stop Communication Request	⇨ ⇦	Positive Response

2.2.4 *Tidsavpassning*

DDP_019 Vid normal drift är de tidsparametrar som visas i följande figur relevanta:

Figur 1

Meddelandeflöde, tidsavpassning



där

P1 = Tid mellan byte för fordonsenhetens svar.

P2 = Tid mellan slut på begäran från IDE-enheten och början på fordonsenhetens svar, eller mellan slut på kvittering från IDE-enheten och början på fordonsenhetens nästa svar.

P3 = Tid mellan slut på fordonsenhetens svar och början på ny begäran från IDE-enheten, eller mellan slut på fordonsenhetens svar och början på kvittering från IDE-enheten, eller mellan slut på begäran från IDE-enheten och början på ny begäran från IDE-enheten om fordonsenheten inte svarar.

P4 = Tid mellan byte för begäran från IDE-enheten.

P5 = Utökat värde för P3 för överföring från kort.

▼B

Tillåtna värden för tidsparametrar visas i följande tabell (utökade tidsparametrar enligt KWP, används vid fysisk adressering för snabbare kommunikation).

Tidsavpassning Parameter	Nedre gränsvärde (ms)	Övre gränsvärde (ms)
P1	0	20
P2	20	1 000 (*)
P3	10	5 000
P4	5	20
P5	10	20 minuter

(*) Om fordonsenheten svarar med *Negative Response* och en kod som innebär att begäran har tagits emot korrekt och att svaret dröjer utökas detta värde till det övre gränsvärdet för P3.

2.2.5 *Felhantering*

Om ett fel inträffar vid meddelandeutbytet ändras schemat för meddelandeflödet beroende på vilken utrustning som har upptäckt felet och på det meddelande som genererat felet.

I figur 2 och 3 visas procedurerna för felhantering med avseende på fordonsenhet respektive IDE-enhet.

2.2.5.1 Startfas för kommunikation

DDP_020 Om IDE-enheten upptäcker ett fel under kommunikationens startfas, antingen genom tidsavpassning eller genom bitflöde, kommer den att vänta under en period P3min innan den utfärdar begäran igen.

DDP_021 Om fordonsenheten upptäcker ett fel i sekvensen som kommer från IDE-enheten ska den inte sända något svar utan vänta på ytterligare ett meddelande av typen *Start Communication Request* inom en period P3max.

2.2.5.2 Kommunikationsfas

Följande två typer av felhantering kan definieras:

1. **Fordonsenheten upptäcker ett fel vid överföring från IDE-enheten**

DDP_022 För varje mottaget meddelande ska fordonsenheten upptäcka fel avseende tidsavpassning, byteformat (t.ex. fel som rör start- och stoppbitar) och ramar (fel antal mottagna byte, fel byte för kontrollsumma).

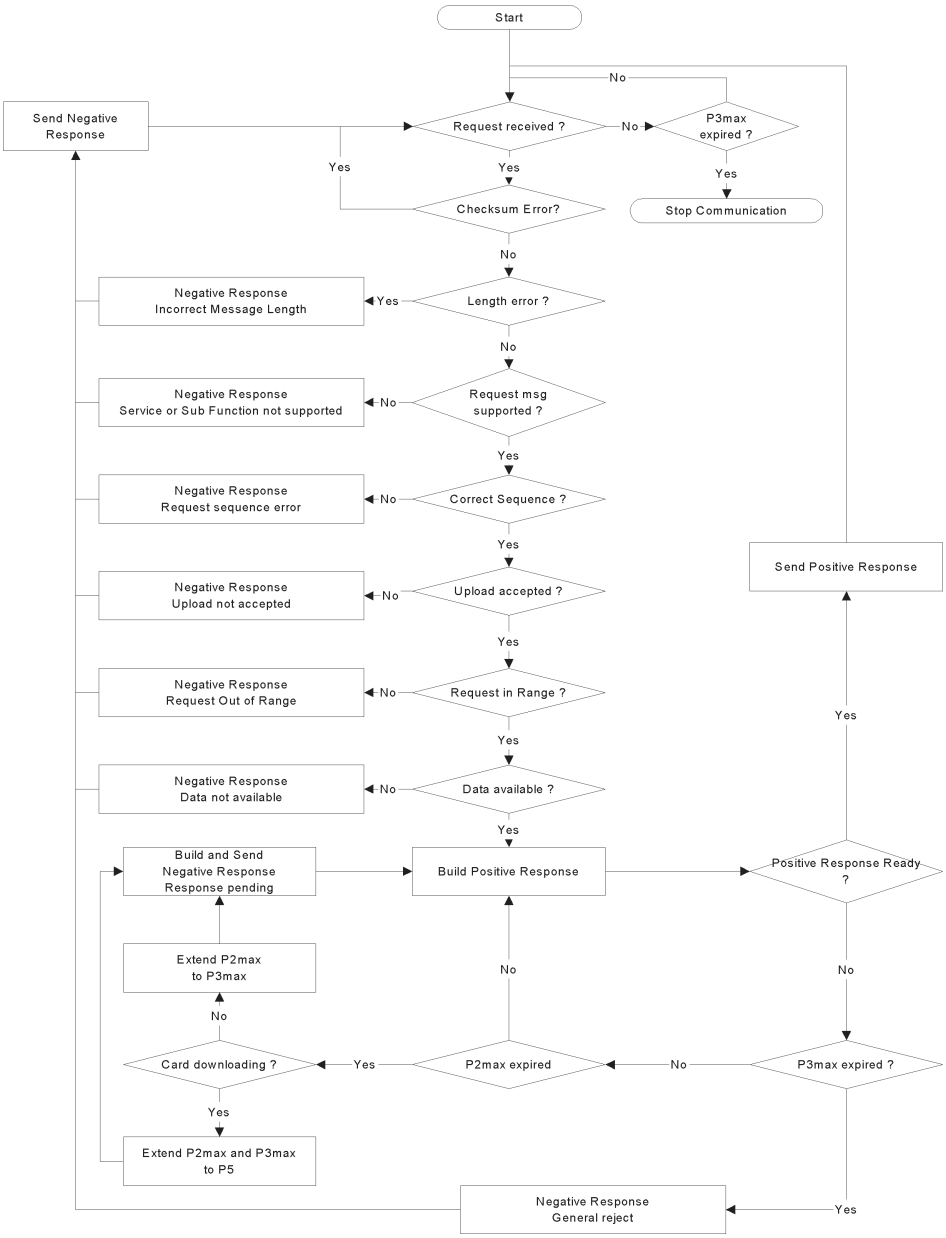
DDP_023 Om fordonsenheten upptäcker ett av ovanstående fel sänder den inget svar och ignorerar det mottagna meddelandet.

DDP_024 Fordonsenheten kan upptäcka andra fel i det mottagna meddelandets format eller innehåll (t.ex. att meddelandet ej stöds) även om meddelandet uppfyller kraven på längd och kontrollsumma. I så fall ska fordonsenheten svara IDE-enheten med meddelandet Negative Response och specificera typen av fel.

▼B

Figur 2

Felhantering i fordonsenhet



2. **IDE-enheten upptäcker ett fel vid överföring från fordonsenheten**

DDP_025 För varje mottaget meddelande ska IDE-enheten upptäcka eventuella fel avseende tidsavpassning, byteformat (t.ex. fel som rör start- och stoppbitar) och ramar (fel antal mottagna byte, fel byte för kontrollsumma).

DDP_026 IDE-enheten ska upptäcka eventuella sekvensfel, t.ex. felaktiga steg från räknaren av undermeddelanden i fråga om mottagna meddelanden som följer på varandra.

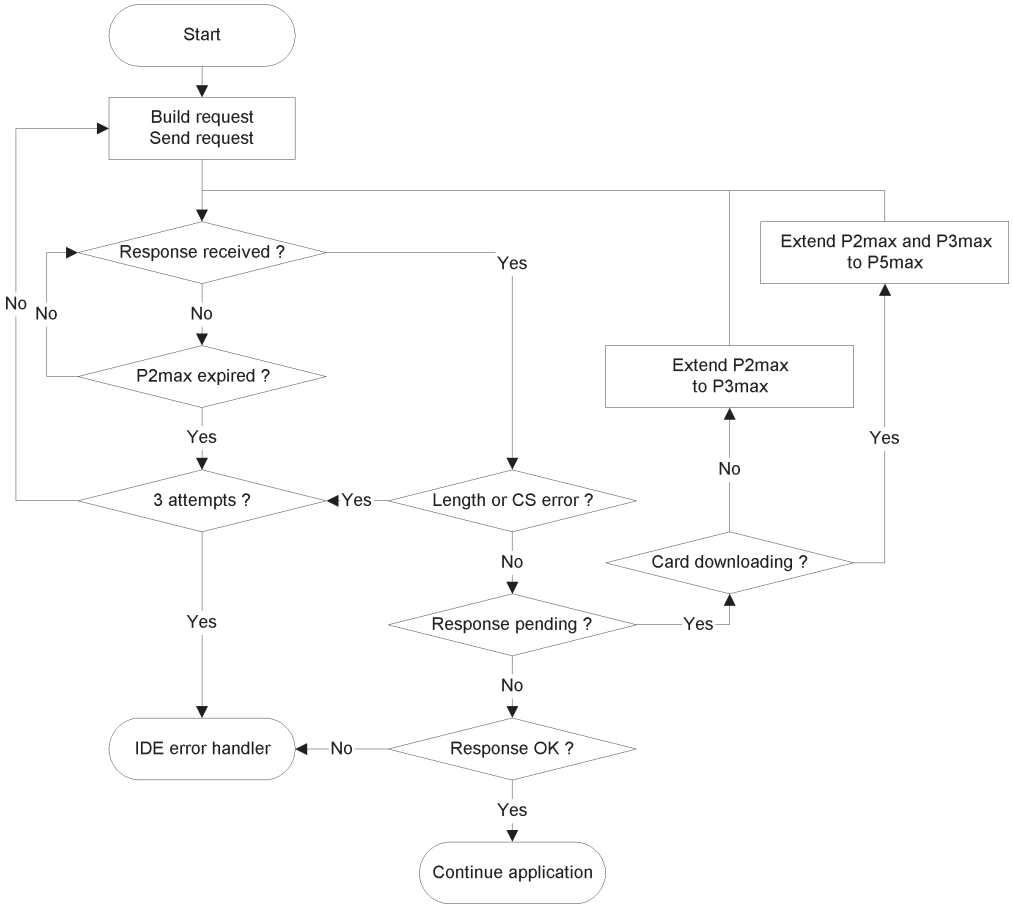
DDP_027 Om IDE-enheten upptäcker ett fel eller om det inte kom något svar från fordonsenheten inom perioden P2max ska meddelandet om begäran sändas igen så att det sammanlagt överförs högst tre gånger. För att bidra till att dessa fel upptäcks kommer en kvittering av undermeddelanden att betraktas som en begäran till fordonsenheten.

▼B

DDP_028 IDE-enheten ska vänta åtminstone under en period P3min innan den påbörjar varje överföring. Väntеperioden ska mätas från senast beräknade förekomst av en stoppbit efter det att felet upptäcktes.

Figur 3

Felhantering i IDE-enhet



2.2.6 *Innehåll i svarsmeddelande*

I denna punkt specificeras innehållet i datafälten i de olika positiva svarsmeddelandena.

Dataelement definieras i tillägg 1 om datakatalogen.

Anmärkning: För överföringar enligt generation 2 representeras varje dataelement på toppnivån av en uppställning av poster, även om det bara innehåller en enda post. En uppställning av poster börjar med en startdel (*header*) som innehåller posttypen, poststorleken och antalet poster. Uppställningarna av poster betecknas som …RecordArray (med startdel) i följande tabeller.

2.2.6.1 Positive Response Transfer Data – Overview

DDP_029 Datafältet i meddelandet *Positive Response Transfer Data – Overview* ska tillhandahålla följande data i följande ordning, med angivande av SID = 76 Hex, TREP = 01 Hex och med passande delning och räkning av undermeddelanden:

▼B

Datastruktur för generation 1

Dataelement	Kommentar
MemberStateCertificate VUCertificate	Säkerhetsintyg för fordonsenhet
VehicleIdentificationNumber VehicleRegistrationIdentification	Fordonsidentifiering
CurrentDateTime	Fordonsenhetens aktuella datum och tid
VuDownloadablePeriod	Överföringsbar period
CardSlotsStatus	Typ av kort som finns i fordonsenheten
VuDownloadActivityData	Tidigare överföring från fordonsenhet
VuCompanyLocksData	Alla lagrade företagslås. Om avsnittet är tomt sänds endast noOfLocks = 0.
VuControlActivityData	Alla kontrollposter som lagrats i fordonsenheten. Om avsnittet är tomt sänds endast noOfControls = 0.
Signature	RSA-signatur för alla data (utom certifikat), från VehicleIdentificationNumber till sista byte för sista VuControlActivityData.

Datastruktur för generation 2

Dataelement	Kommentar
MemberStateCertificateRecordArray	Intyg från medlemsstaten
VUCertificateRecordArray	Fordonsenhetens certifikat
VehicleIdentificationNumberRecordArray	Fordonsidentifiering
VehicleRegistrationNumberRecordArray	Fordonets registreringsnummer
CurrentDateTimeRecordArray	Fordonsenhetens aktuella datum och tid
VuDownloadablePeriodRecordArray	Överföringsbar period
CardSlotsStatusRecordArray	Typ av kort som finns i fordonsenheten
VuDownloadActivityDataRecordArray	Tidigare överföring från fordonsenhet
VuCompanyLocksRecordArray	Alla lagrade företagslås. Om detta avsnitt är tomt sänds en startpost för uppställningen med noOfRecords = 0.
VuControlActivityRecordArray	Alla kontrollposter som lagrats i fordonsenheten. Om detta avsnitt är tomt sänds en startpost för uppställningen med noOfRecords = 0.
SignatureRecordArray	ECC-signatur för alla föregående data, med undantag för certifikat.

2.2.6.2 Positive Response Transfer Data – Activities

DDP_030 Datafältet i meddelandet *Positive Response Transfer Data – Activities* ska tillhandahålla följande data i följande ordning med angivande av SID = 76 Hex, TREP = 02 Hex och med passande delning och räkning av undermeddelanden:

▼B

Datastruktur för generation 1

Dataelement	Kommentar
TimeReal	Datum för den dag som överförs.
OdometerValueMidnight	Vägmätarställning vid slutet av den dag som överförs.
VuCardIWData	Data om cykler med insättning/uttag av kort. — Om detta avsnitt inte innehåller några data sänds endast noOfVuCardIWRecords = 0. — När en VuCardIWRecord spänner över kl. 00.00 (kort insatt föregående dag) eller över kl. 24.00 (kort uttaget efterföljande dag) ska posten synas i sin helhet för båda två dagarna som berörs.
VuActivityDailyData	Kortplatsstatus kl. 00.00 och aktivitetsändringar som registrerats för den dag som överförs.
VuPlaceDailyWorkPeriodData	Platsrelaterade data som registrerats för den dag som överförs. Om avsnittet är tomt sänds endast noOfPlaceRecords = 0.
VuSpecificConditionData	Data om särskilda omständigheter som registrerats för den dag som överförs. Om avsnittet är tomt sänds endast noOfSpecificConditionRecords = 0.
Signature	RSA-signatur för alla data, från TimeReal till sista byte för sista post om särskilda omständigheter.

Datastruktur för generation 2

Dataelement	Kommentar
DateOfDayDownloadedRecordArray	Datum för den dag som överförs.
OdometerValueMidnightRecordArray	Vägmätarställning vid slutet av den dag som överförs.
VuCardIWRecordArray	Data om cykler med insättning/uttag av kort. — Om detta avsnitt inte innehåller några tillgängliga data sänds en startpost för uppställningen med noOfRecords = 0. — När en VuCardIWRecord spänner över kl. 00.00 (kort insatt föregående dag) eller över kl. 24.00 (kort uttaget efterföljande dag) ska posten synas i sin helhet för båda två dagarna som berörs.
VuActivityDailyRecordArray	Kortplatsstatus kl. 00.00 och aktivitetsändringar som registrerats för den dag som överförs.
VuPlaceDailyWorkPeriodRecordArray	Platsrelaterade data som registrerats för den dag som överförs. Om detta avsnitt är tomt sänds en startpost för uppställningen med noOfRecords = 0.
VuGNSSCDRecordArray	GNSS-positioner för fordonet om förarens sammanhängande körtid uppgår till en multipel av tre timmar. Om detta avsnitt är tomt sänds en startpost för uppställningen med noOfRecords = 0.
VuSpecificConditionRecordArray	Data om särskilda omständigheter som registrerats för den dag som överförs. Om detta avsnitt är tomt sänds en startpost för uppställningen med noOfRecords = 0.
SignatureRecordArray	ECC-signatur för alla föregående data.

▼B

2.2.6.3 Positive Response Transfer Data – Events and Faults

DDP_031 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 Hex och med passande delning och räkning av undermeddelanden:

Datastruktur för generation 1

Dataelement	Kommentar
VuFaultData	Alla fel som lagrats eller håller på att registreras i fordonsenheten. Om avsnittet är tomt sänds endast noOfVuFaults = 0.
VuEventData	Alla händelser (med undantag för hastighetsöverträdelse) som lagrats eller håller på att registreras i fordonsenheten. Om avsnittet är tomt sänds endast noOfVuEvents = 0.
VuOverSpeedingControlData	Data som rör den senaste kontrollen av hastighetsöverträdelse (standardvärde om data saknas).
VuOverSpeedingEventData	Alla händelser av typen hastighetsöverträdelse som lagrats i fordonsenheten. Om avsnittet är tomt sänds endast noOfVuOverSpeedingEvents = 0.
VuTimeAdjustmentData	Alla händelser av typen tidsinställning som lagrats i fordonsenheten (utanför ramen för en full kalibrering). Om avsnittet är tomt sänds endast noOfVuTimeAdjRecords = 0.
Signature	RSA-signatur för alla data, från noOfVuFaults till sista byte för sista post om tidsinställning.

Datastruktur för generation 2

Dataelement	Kommentar
VuFaultRecordArray	Alla fel som lagrats eller håller på att registreras i fordonsenheten. Om detta avsnitt är tomt sänds en startpost för uppställningen med noOfRecords = 0.
VuEventRecordArray	Alla händelser (med undantag för hastighetsöverträdelse) som lagrats eller håller på att registreras i fordonsenheten. Om detta avsnitt är tomt sänds en startpost för uppställningen med noOfRecords = 0.
VuOverSpeedingControlDataRecordArray	Data som rör den senaste kontrollen av hastighetsöverträdelse (standardvärde om data saknas).
VuOverSpeedingEventRecordArray	Alla händelser av typen hastighetsöverträdelse som lagrats i fordonsenheten. Om detta avsnitt är tomt sänds en startpost för uppställningen med noOfRecords = 0.
VuTimeAdjustmentRecordArray	Alla händelser av typen tidsinställning som lagrats i fordonsenheten (utanför ramen för en full kalibrering). Om detta avsnitt är tomt sänds en startpost för uppställningen med noOfRecords = 0.
VuTimeAdjustmentGNSSRecordArray	
SignatureRecordArray	ECC-signatur för alla föregående data.

▼B

2.2.6.4 Positive Response Transfer Data – Detailed Speed

DDP_032 Datafältet i meddelandet *Positive Response Transfer Data – Detailed Speed* ska tillhandahålla följande data i följande ordning med angivande av SID = 76 Hex, TREP = 04 Hex och med passande delning och räkning av undermeddelanden:

Datastruktur för generation 1

Dataelement	Kommentar
VuDetailedSpeedData	Alla detaljerade hastighetsdata som lagrats i fordonsenheten (ett hastighetsblock per minut medan fordonet har varit i rörelse). 60 hastighetsvärden per minut (ett per sekund).
Signature	RSA-signatur för alla data, från noOfSpeedBlocks till sista byte för sista hastighetsblock.

Datastruktur för generation 2

Dataelement	Kommentar
VuDetailedSpeedBlockRecordArray	Alla detaljerade hastighetsdata som lagrats i fordonsenheten (ett hastighetsblock per minut medan fordonet har varit i rörelse). 60 hastighetsvärden per minut (ett per sekund).
SignatureRecordArray	ECC-signatur för alla föregående data.

2.2.6.5 Positive Response Transfer Data – Technical Data

DDP_033 Datafältet i meddelandet *Positive Response Transfer – Technical Data* ska tillhandahålla följande data i följande ordning med angivande av SID = 76 Hex, TREP = 05 Hex och med passande delning och räkning av undermeddelanden:

Datastruktur för generation 1

Dataelement	Kommentar
VuIdentification	
SensorPaired	
VuCalibrationData	Alla kalibreringsposter som lagrats i fordonsenheten.
Signature	RSA-signatur för alla data, från vuManufacturerName till sista byte för sista VuCalibrationRecord.

▼B

Datastruktur för generation 2

Dataelement	Kommentar
VuIdentificationRecordArray	
VuSensorPairedRecordArray	Alla parningar med rörelsesensorer som lagrats i fordonsenheten.
VuSensorExternalGNSSCoupledRecordArray	Alla kopplingar med externa GNSS-anordningar som lagrats i fordonsenheten.
VuCalibrationRecordArray	Alla kalibreringsposter som lagrats i fordonsenheten.
VuCardRecordArray	Alla data om insättning av kort som lagrats i fordonsenheten.
VuITSConsentRecordArray	
VuPowerSupplyInterruptionRecordArray	
SignatureRecordArray	ECC-signatur för alla föregående data.

2.3. **Fillagring på externt lagringsmedium**

DDP_034 När en överföringssession har inbegripit överföring av data från fordonsenheten ska IDE-enheten lagra alla data som mottagits från fordonsenheten under överföringssessionen inom meddelanden av typen *Positive Response Transfer Data* i en enda fysisk fil. Lagrade data inbegriper ej meddelandens startdelar (*header*), räknare av undermeddelanden, tomma undermeddelanden och kontrollsummor men de inbegriper SID och TREP (endast i första undermeddelandet vid flera undermeddelanden).

3. PROTOKOLL FÖR ÖVERFÖRING FRÅN FÄRDSKRIVARKORT

3.1. **Tillämpningsområde**

I denna punkt beskrivs direkt överföring av kortdata från ett färdskrivarkort till en IDE-enhet. IDE-enheten är inte en del av den säkra miljön, och följaktligen utförs ingen autentisering mellan kortet och IDE-enheten.

3.2. **Definitioner**

Överföringssession: Varje utförd överföring av data från smartkort (ICC). Sessionen omfattar en fullständig procedur från återställning av smartkortet i en kortläsare (IFD) till avaktivering av smartkortet (urtagning av kort eller nästa återställning).

Signerad datafil: En fil från smartkortet. Filen överförs till kortläsaren i klartext. Filen hashas och signeras på smartkortet och signaturen överförs till kortläsaren.

3.3. **Överföring från kort**

DDP_035 Överföring från ett färdskrivarkort inbegriper följande steg:

— Överför kortets basinformation i EF ICCoch EF IC. Denna information är valfri att överföra och säkras inte med en digital signatur.

▼B

— Överför EF Card_Certificate (eller EF CardSignCertificate) och EF CA_Certificate. Denna information säkras inte med en digital signatur.

Överföring av dessa filer är obligatorisk vid varje överföringssession.

— Överför övriga EF för tillämpningsdata (under DF Tachograph Och DF Tachograph_G2 om detta är relevant), med undantag för EF Card_Download. Denna information säkras med en digital signatur.

— Överföring av åtminstone EF Application_Identification och EF ID är obligatorisk vid varje överföringssession.

— Vid överföring från ett förarkort är överföring av följande EF också obligatorisk:

- Events_Data,
- Faults_Data,
- Driver_Activity_Data,
- Vehicles_Used,
- Places,
- GNSS_Places (om detta är relevant),
- Control_Activity_Data,
- Specific_Conditions.

— Vid överföring från ett förarkort, uppdatera datumet för LastCardDownload i EF Card_Download.

— Vid överföring från ett verkstadskort, återställ kalibreringsräknaren i EF Card_Download.

— Vid överföring från ett verkstadskort ska EF Sensor_Installation_Data inte överföras.

3.3.1 *Initieringssekvens*

DDP_036 IDE-enheten ska initiera sekvensen enligt följande:

Kort	Riktning	IDE/IFD	Betydelse/anmärkningar
	⇦	Maskinvaruåterställning	
ATR	⇨		

Det är valfritt att använda PPS för att byta till en högre överföringshastighet så länge smartkortet stöder detta.

3.3.2 *Sekvens för osignerade datafiler*

DDP_037 Sekvensen för överföring av EF ICC, EF IC, EF Card_Certificate (eller EF CardSignCertificate) och EF CA_Certificate är följande:

Kort	Riktning	IDE/IFD	Betydelse/anmärkningar
	⇦	**Select File**	Välj med hjälp av filidentifierare.
OK	⇨		

▼B

Kort	Riktning	IDE/IFD	Betydelse/anmärkningar
	⇦	**Read Binary**	Om filen innehåller mer data än buffertstorleken hos läsaren eller kortet måste kommandot upprepas tills den fullständiga filen har lästs.
Fildata OK	⇨	Lagra data till externt lagringsmedium (ESM)	Enligt **3.4** Data storage format

Anmärkning 1: Innan EF Card_Certificate (eller EF Card-SignCertificate) väljs, måste färdskrivartillämpning väljas (med hjälp av tillämpningsidentifierare (AID)).

Anmärkning 2: Med hjälp av kommandot READ BINARY och en SFID (kort identifierare för elementfil) kan filen både väljas och avläsas i samma steg.

3.3.3 *Sekvens för signerade datafiler*

DDP_038 Följande sekvens ska användas för var och en av följande filer som måste överföras med sin signatur.

Kort	Riktning	IDE/IFD	Betydelse/anmärkningar
	⇦	**Select File**	
OK	⇨		
	⇦	**Perform Hash of File**	Beräknar hashvärdet för datainnehållet i vald fil med hjälp av föreskriven hashalgoritm enligt 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

▼B

Kort	Riktning	IDE/IFD	Betydelse/anmärkningar
	⇦	**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

Anmärkning: Med hjälp av kommandot READ BINARY och en SFID (kort identifierare för elementfil) kan filen både väljas och avläsas i samma steg. I detta fall kan elementfilen (EF) både väljas och läsas innan kommandot **Perform Hash of File** utförs.

3.3.4 *Sekvens för återställning av kalibreringsräknare*

DDP_039 Sekvensen för att återställa räknaren `NoOfCalibrationsSinceDownload` i `Card_Download` på ett verkstadskort är följande:

Kort	Riktning	IDE/IFD	Betydelse/anmärkningar
	⇦	**Select File** EF Card_Download	Välj med hjälp av filidentifierare.
OK	⇨		
	⇦	**Update Binary (uppdatera binär)** NoOfCalibrationsSinceDownload = ‘00 00’	
Återställer antal överföringar från kort			
OK	⇨		

Anmärkning: Med hjälp av kommandot UPDATE BINARY och SFID (kort identifierare för elementfil) kan filen både väljas och uppdateras i samma steg.

3.4. **Format för lagring av data**

3.4.1 *Inledning*

DDP_040 Överförda data måste lagras enligt följande villkor:

— Data ska lagras transparent. Detta innebär att ordningen av byte och ordningen av bitar inuti de byte som överförs från kortet måste bevaras vid lagring.

— Alla filer på ett kort som överförs vid en överföringssession lagras i en (1) fil i det externa lagringsmediet.

▼B

3.4.2 *Filformat*

DDP_041 Filformatet är en sammansättning av flera TLV-objekt.

DDP_042 Taggen för en EF ska vara FID plus tillägget ”00”.

DDP_043 Taggen för en signatur för en EF ska vara FID för filen plus tillägget ”01”.

DDP_044 Längden är ett värde på två byte. Värdet definierar antalet byte i värdefältet. Värdet ”FF FF” i längdfältet är reserverat för framtida användning.

DDP_045 Om en fil inte överförs ska inte något som förknippas med filen lagras (ingen tagg och ingen noll-längd).

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)	3 byte
FID (2 byte) || ”01”	Tagg för signatur för EF (FID)	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 EFVehicles_Used
05 05 01	00 80	Signatur för EFVehicles_Used

4. ÖVERFÖRING FRÅN ETT FÄRDSKRIVARKORT VIA EN FORDONSENHET

DDP_047 Fordonsenheten måste möjliggöra överföring av innehållet från ett insatt förarkort till en ansluten IDE-enhet.

DDP_048 IDE-enheten ska sända meddelandet *Transfer Data Request Card Download* till fordonsenheten för att initiera detta läge (se 2.2.2.9).

DDP_049 Fordonsenheten ska sedan överföra hela kortet, fil efter fil, enligt det protokoll för överföring från kort som definieras i punkt 3, och vidaresända alla data som mottagits från kortet till IDE-enheten i lämpligt TLV-filformat (se 3.4.2), inkapslade i meddelandet *Positive Response Transfer Data*.

▼B

DDP_050 IDE-enheten ska hämta kortdata från meddelandet *Positive Response Transfer Data* (och stryka alla startdelar (*header*), SID, TREP, undermeddelanderäknare och kontrollsummor) och lagra dem i en enda fysisk fil i enlighet med punkt 2.3.

DDP_051 Fordonsenheten ska därefter i förekommande fall uppdatera förarkortets EF `Control_Activity_Data` eller EF `Card_Download`.

▼B

Tillägg 8

KALIBRERINGSPROTOKOLL

INNEHÅLLSFÖRTECKNING

1. INLEDNING

2. TERMER, DEFINITIONER OCH REFERENSER

3. ÖVERSIKT ÖVER TJÄNSTER

3.1. Tillgängliga tjänster

3.2. Svarskoder

4. KOMMUNIKATIONSTJÄNSTER

4.1. Tjänsten StartCommunication

4.2. Tjänsten StopCommunication

4.2.1 Meddelandebeskrivning

4.2.2 Meddelandeformat

4.2.3 Parameterdefinition

4.3. Tjänsten TesterPresent

4.3.1 Meddelandebeskrivning

4.3.2 Meddelandeformat

5. FÖRVALTNINGSTJÄNSTER

5.1. Tjänsten StartDiagnosticSession

5.1.1 Meddelandebeskrivning

5.1.2 Meddelandeformat

5.1.3 Parameterdefinition

5.2. Tjänsten SecurityAccess

5.2.1 Meddelandebeskrivning

5.2.2 Meddelandeformat – SecurityAccess – requestSeed

5.2.3 Meddelandeformat – SecurityAccess – sendKey

6. DATAÖVERFÖRINGSTJÄNSTER

6.1. Tjänsten ReadDataByIdentifier

6.1.1 Meddelandebeskrivning

6.1.2 Meddelandeformat

6.1.3 Parameterdefinition

6.2. Tjänsten WriteDataByIdentifier

6.2.1 Meddelandebeskrivning

6.2.2 Meddelandeformat

6.2.3 Parameterdefinition

▼B

7. KONTROLL AV PROVPULSER – FUNKTIONSENHET FÖR KONTROLL AV IN-/UTDATA

7.1. Tjänsten InputOutputControlByIdentifier

7.1.1 Meddelandebeskrivning

7.1.2 Meddelandeformat

7.1.3 Parameterdefinition

8. FORMAT FÖR DATARECORDS

8.1. Intervall för överförda parametrar

8.2. Format för dataRecords

1. INLEDNING

I detta tillägg beskrivs hur data utbyts mellan en fordonsenhet och en provare (*tester*) via K-line, som utgör en del av det gränssnitt för kalibrering som beskrivs i tillägg 6. Dessutom beskrivs kontroll av linjen för in-/utsignal i kalibreringsanslutningen.

Upprättande av kommunikation via K-line beskrivs i avsnitt 4 ”Communication Services”.

I detta tillägg används begreppet ”diagnossessioner” för att avgöra tillämpningsområdet för K-line under olika omständigheter. Den förvalda sessionen är ”StandardDiagnosticSession”, där alla data kan avläsas från, men inga data kan skrivas till, en fordonsenhet.

Val av diagnossession beskrivs i avsnitt 5 ”Management Services”.

Detta tillägg ska betraktas som relevant för fordonsenheter och verkstadskort i båda generationerna, i enlighet med de krav på driftskompatibilitet som föreskrivs i denna förordning.

CPR_001 ”ECUProgrammingSession” möjliggör inmatning av data till fordonsenheten. När det gäller inmatning av kalibreringsdata ska fordonsenheten dessutom vara i funktionsläge CALIBRATION (kalibrering).

Dataöverföring via K-line beskrivs i avsnitt 6 ”Data Transmission Services”. Formaten för data som överförs beskrivs närmare i avsnitt 8 ”dataRecords formats”.

CPR_002 ”ECUAdjustmentSession” gör det möjligt att välja in-/utläget för den linje som via K-Line-gränssnittet används för in-/utsignaler vid kalibrering. Kontroll av linjen för in-/utsignaler vid kalibrering beskrivs i avsnitt 7 ”Control of Test Pulses – Input/Output Control functional unit”.

CPR_003 I hela detta dokument betecknas provarens adress med ”tt”. Även om fordonsenheten i första hand använder vissa adresser för provaren ska fordonsenheten svara korrekt oavsett vilken adress provaren har. Fordonsenhetens fysiska adress är 0xEE.

▼B

2. TERMER, DEFINITIONER OCH REFERENSER

Protokollen, meddelandena och felkoderna bygger huvudsakligen på den aktuella versionen av ISO 14229-1 (*Road vehicles – Diagnostic systems – Part 1: Diagnostic services*, version 6 av den 22 februari 2001).

Byte-kodning och hexadecimala värden används för identifierare av tjänster, för begäran och svar om tjänster samt för standardparametrarna.

Termen ”provare” (*tester*) avser den utrustning som används för att mata in programmerings-/kalibreringsdata till fordonsenheten.

Termerna ”klient” (*client*) och ”server” avser provaren respektive fordonsenheten.

Termen ECU betyder *Electronic Control Unit* (elektronisk styrenhet) och avser fordonsenheten.

Referenser

ISO 14230-2:

Road Vehicles -Diagnostic Systems – Keyword Protocol 2000- Part 2: Data Link Layer.

First edition: 1999.

3. ÖVERSIKT ÖVER TJÄNSTER

3.1. **Tillgängliga tjänster**

Nedanstående tabell ger en översikt över de tjänster som kommer att finnas tillgängliga i färdskrivaren och som definieras i detta dokument.

CPR_004 I tabellen visas de tjänster som finns tillgängliga i en aktiverad diagnossession.

— I den **första kolumnen** förtecknas de tjänster som finns tillgängliga.

— Den **andra kolumnen** i vilket avsnitt i detta tillägg som tjänsten definieras närmare.

— I den **tredje kolumnen** tilldelas tjänsteidentifierarnas värden för meddelanden med begäran.

— I den **fjärde kolumnen** specificeras de tjänster inom **StandardDiagnosticSession (SD)** som måste vara införda i varje fordonsenhet.

— I den **femte kolumnen** specificeras de tjänster inom **ECUAdjustmentSession (ECUAS)** som måste vara införda för att det ska vara möjligt att kontrollera linjen för in-/utsignaler i kalibreringsanslutningen på fordonsenhetens frontpanel.

— I den **sjätte kolumnen** specificeras de tjänster inom **ECUProgrammingSession (ECUPS)** som måste vara införda för att det ska vara möjligt att programmera parametrar i fordonsenheten.

▼B

Tabell 1

Sammanfattande tabell över värden på tjänsteidentifierare

			Diagnossessioner		
Namn på diagnostjänst	Avsnitt nr.	Tjänsteidentifierare (SId) (värde i begäran)	SD	ECUAS	ECUPS
StartCommunication (starta kommunikation)	4.1	81	■	■	■
StopCommunication (avsluta kommunikation)	4.2	82	■		
TesterPresent (provare inkopplad)	4.3	3E	■	■	■
StartDiagnosticSession (starta diagnossession)	5.1	10	■	■	■
SecurityAccess (säkerhetstillträde)	5.2	27	■	■	■
ReadDataByIdentifier (läs data med hjälp av identifierare)	6.1	22	■	■	■
WriteDataByIdentifier (skriv data med hjälp av identifierare)	6.2	2E			■
InputOutputControlByIdentifier (kontroll av in-/utdata med hjälp av identifierare)	7.1	2F		■	

■ Denna symbol visar att tjänsten är obligatorisk i denna diagnossession.
Om symbol saknas visar det att tjänsten inte är tillåten i denna diagnossession.

3.2. **Svarskoder**

Svarskoder (*response code*) är definierade för varje tjänst.

4. KOMMUNIKATIONSTJÄNSTER

Vissa tjänster behövs för att kommunikation ska kunna upprättas och upprätthållas. De finns inte i tillämpningsskiktet. Tillgängliga tjänster specificeras i nedanstående tabell:

Tabell 2

Kommunikationstjänster

Namn på tjänsten	Beskrivning
StartCommunication (starta kommunikation)	Klienten begär att få starta en kommunikationssession med en eller flera servrar.
StopCommunication (avsluta kommunikation)	Klienten begär att få avsluta pågående kommunikationssession.
TesterPresent (provare inkopplad)	Klienten meddelar servern att den fortfarande är inkopplad.

CPR_005 Tjänsten StartCommunication används för att starta en kommunikationssession. För att en tjänst ska kunna utföras måste kommunikationen initieras och lämpliga kommunikationsparametrar finnas för önskat läge (*mode*).

4.1. **Tjänsten StartCommunication**

CPR_006 Vid mottagande av ett indikeringsprimitiv för StartCommunication ska fordonsenheten kontrollera om den begärda kommunikationslänken kan initieras under innevarande omständigheter. Giltiga omständigheter för initiering av en kommunikationslänk beskrivs i dokument ISO 14230-2.

▼B

CPR_007 Fordonsenheten ska därefter utföra alla de operationer som krävs för att initiera kommunikationslänken och sända ett svarsprimitiv för StartCommunication med de parametrar för positivt svar (*Positive Response*) som valts.

CPR_008 Om en fordonsenhet som redan har initierats (och som är i en diagnossession) tar emot en ny StartCommunication Request (begäran om att starta kommunikation) (exempelvis på grund av felåterställning i provaren) ska begäran godtas och fordonsenheten ska återinitieras.

CPR_009 Om kommunikationslänken av någon anledning inte kan initieras ska fordonsenheten fortsätta att fungera på samma sätt som omedelbart före försöket att initiera kommunikationslänken.

CPR_010 Meddelandet med StartCommunication Request måste vara fysiskt adresserat.

CPR_011 Initiering av fordonsenheten för tjänster sker via ”snabb initiering”:

— Det finns en bussvilotid (*bus idle time*) före varje aktivitet.

— Provaren sänder därefter ett initieringsmönster.

— All den information som behövs för att upprätta kommunikation finns i fordonsenhetens svar.

CPR_012 Efter avslutad initiering gäller följande:

— Alla kommunikationsparametrar sätts till de värden som anges i Table 4 i enlighet med byte för nyckel (*key bytes*).

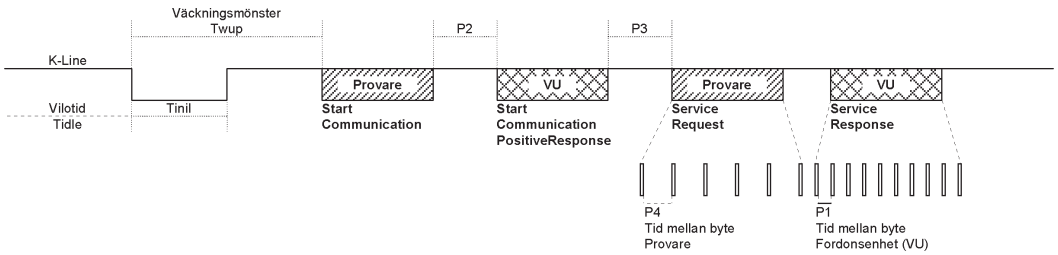
— Fordonsenheten väntar på provarens första begäran.

— Fordonsenheten är i förvalt diagnosläge, dvs. StandardDiagnosticSession.

— Linjen för in-/utsignaler vid kalibrering är i förvalt läge, dvs. avaktiverat läge.

CPR_014 Dataöverföringshastigheten för K-line ska vara 10 400 baud.

CPR_016 Den snabba initieringen påbörjas av provaren, som överför ett väckningsmönster (Wup, *Wake-up pattern*) via K-line. Mönstret börjar efter vilotid för K-line, med låg signal under tiden T_{inil}. Provaren överför första bit i tjänsten StartCommunication efter en tid T_{wup} som följer på första fallande kant.



▼B

CPR_017 Tidsvärdena för snabb initiering och kommunikation i allmänhet anges i detalj i tabellerna nedan. Det finns olika möjligheter när det gäller vilotid:

— Första överföring efter det att strömmen slagits på, T_{idle} = 300 ms.

— Efter slutförd StopCommunication-tjänst, T_{idle} = P3 min.

— Efter det att kommunikationen avslutats genom time-out P3 max, T_{idle} = 0.

Tabell 3

Tidsvärden för snabb initiering

Parameter		Min. värde	Max. värde
T_{inil}	25 ±1 ms	24 ms	26 ms
T_{wup}	50 ±1 ms	49 ms	51 ms

Tabell 4

Tidsvärden för kommunikation

Tidsavpassning Parameter	Parameterbeskrivning	Nedre gränsvärden (ms)	Övre gränsvärden (ms)
		Min.	Max.
P1	Tid mellan byte för fordonsenhetens svar.	0	20
P2	Tid mellan provarens begäran och fordonsenhetens svar eller mellan två svar från fordonsenheten.	25	250
P3	Tid mellan slut på fordonsenhetens svar och start på ny begäran från provaren.	55	5 000
P4	Tid mellan byte för begäran från provaren.	5	20

CPR_018 Meddelandeformatet för snabb initiering anges i detalj i nedanstående tabeller. (ANMÄRKNING: ”Hex” betyder hexadecimal.)

Tabell 5

Meddelande med begäran om StartCommunication

Byte #	Parameternamn	Hexvärde	Memosymbol (*mnemonic*)
#1	Byte för format – fysisk adressering	81	FMT
#2	Byte för måladress	EE	TGT
#3	Byte för källadress	tt	SRC

▼B

Byte #	Parameternamn	Hexvärde	Memosymbol (*mnemonic*)
#4	**StartCommunication Request Service Id**	**81**	**SCR**
#5	Kontrollsumma	00-FF	CS

Tabell 6

Positivt svarsmeddelande om StartCommunication

Byte #	Parameternamn	Hexvärde	Memosymbol (*mnemonic*)
#1	Byte för format – fysisk adressering	80	FMT
#2	Byte för måladress	tt	TGT
#3	Byte för källadress	EE	SRC
#4	Byte för extra längd	03	LEN
#5	**StartCommunication Positive Response Service Id**	**C1**	**SCRPR**
#6	Byte 1 för nyckel (*key byte 1*)	EA	KB1
#7	Byte 2 för nyckel (*key byte 2*)	8F	KB2
#8	Kontrollsumma	00-FF	CS

CPR_019 Det finns inget negativt svar på meddelandet med begäran om StartCommunication. Om det inte finns något positivt svarsmeddelande att överföra är fordonsenheten inte initierad, inget överförs och den kvarstår i normal drift.

4.2. Tjänsten StopCommunication

4.2.1 *Meddelandebeskrivning*

Syftet med denna tjänst i kommunikationsskiktet är att avsluta en kommunikationssession.

CPR_020 När fordonsenheten tar emot ett indikeringsprimitiv för StopCommunication ska den kontrollera om aktuella omständigheter tillåter att denna kommunikation avslutas. I så fall ska fordonsenheten utföra alla de operationer som krävs för att avsluta denna kommunikation.

CPR_021 Om det är möjligt att avsluta kommunikationen ska fordonsenheten utfärda ett svarsprimitiv för StopCommunication med parametrarna för positivt svar valda innan kommunikationen avslutas.

CPR_022 Om kommunikationen av någon anledning inte kan avslutas ska fordonsenheten utfärda ett svarsprimitiv för StopCommunication med parametrarna för negativt svar valda.

CPR_023 Om time-out av P3max upptäcks av fordonsenheten ska kommunikationen avslutas utan att något svarsprimitiv utfärdas.

▼B

4.2.2 *Meddelandeformat*

CPR_024 Meddelandeformat för primitiv för *StopCommunication* anges i detalj i nedanstående tabeller.

Tabell 7

Meddelande med begäran om StopCommunication

Byte #	Parameternamn	Hexvärde	Memosymbol (*mnemonic*)
#1	Byte för format – fysisk adressering	80	FMT
#2	Byte för måladress	EE	TGT
#3	Byte för källadress	tt	SRC
#4	Byte för extra längd	01	LEN
#5	**StopCommunication Request Service Id**	**82**	**SPR**
#6	Kontrollsumma	00-FF	CS

Tabell 8

Positivt svarsmeddelande om StopCommunication

Byte #	Parameternamn	Hexvärde	Memosymbol (*mnemonic*)
#1	Byte för format – fysisk adressering	80	FMT
#2	Byte för måladress	tt	TGT
#3	Byte för källadress	EE	SRC
#4	Byte för extra längd	01	LEN
#5	**StopCommunication Positive Response Service Id**	**C2**	**SPRPR**
#6	Kontrollsumma	00-FF	CS

Tabell 9

Negativt svarsmeddelande om StopCommunication

Byte #	Parameternamn	Hexvärde	Memosymbol (*mnemonic*)
#1	Byte för format – fysisk adressering	80	FMT
#2	Byte för måladress	tt	TGT
#3	Byte för källadress	EE	SRC
#4	Byte för extra längd	03	LEN

▼B

Byte #	Parameternamn	Hexvärde	Memosymbol (*mnemonic*)
#5	**Negative Response Service Id**	**7F**	**NR**
#6	StopCommunication Request Service Identification	82	SPR
#7	Svarskod (*responseCode*) = allmänt avvisande (*generalReject*)	10	RC_GR
#8	Kontrollsumma	00-FF	CS

4.2.3 *Parameterdefinition*

Denna tjänst förutsätter inte någon definition av parametrar.

4.3. **Tjänsten TesterPresent**

4.3.1 *Meddelandebeskrivning*

Tjänsten TesterPresent används av provaren för att meddela servern att den fortfarande är inkopplad. Syftet är att hindra servern från att automatiskt återgå till normal drift och eventuellt avsluta kommunikationen. Denna tjänst, som skickas ut regelbundet, håller diagnossessionen/kommunikationen aktiv genom att återställa P3-timern varje gång en begäran om denna tjänst tas emot.

4.3.2 *Meddelandeformat*

CPR_079 Meddelandeformat för primitiv för *TesterPresent* anges i detalj i nedanstående tabeller.

Tabell 10

Meddelande med begäran om TesterPresent

Byte #	Parameternamn	Hexvärde	Memosymbol (*mnemonic*)
#1	Byte för format – fysisk adressering	80	FMT
#2	Byte för måladress	EE	TGT
#3	Byte för källadress	tt	SRC
#4	Byte för extra längd	02	LEN
#5	**TesterPresent Request Service Id**	**3E**	**TP**
#6	Underfunktion = *responseRequired* = [yes	01	RESPREQ_Y
	no]	02	RESPREQ_NO
#7	Kontrollsumma	00-FF	CS

CPR_080 Om parametern *responseRequired* sätts till *yes* ska servern svara med följande positiva svarsmeddelande. Om parametern sätts till *no* ska inget svar skickas av servern.

▼B

Tabell 11

Positivt svarsmeddelande om TesterPresent

Byte #	Parameternamn	Hexvärde	Memosymbol (*mnemonic*)
#1	Byte för format – fysisk adressering	80	FMT
#2	Byte för måladress	tt	TGT
#3	Byte för källadress	EE	SRC
#4	Byte för extra längd	01	LEN
#5	**TesterPresent Positive Response Service Id**	**7E**	**TPPR**
#6	Kontrollsumma	00-FF	CS

CPR_081 Tjänsten ska stödja följande negativa svarskoder:

Tabell 12

Negativt svarsmeddelande om TesterPresent

Byte #	Parameternamn		Hexvärde	Memosymbol (*mnemonic*)
#1	Byte för format – fysisk adressering		80	FMT
#2	Byte för måladress		tt	TGT
#3	Byte för källadress		EE	SRC
#4	Byte för extra längd		03	LEN
#5	**Negative Response Service Id**		**7F**	**NR**
#6	TesterPresent Request Service Identification		3E	TP
#7	Svarskod (*responseCode* =	[SubFunctionNotSupported-InvalidFormat	12	RC_SFNS_IF
		incorrectMessageLength]	13	RC_IML
#8	Kontrollsumma		00-FF	CS

▼B

5. FÖRVALTNINGSTJÄNSTER

Tillgängliga tjänster specificeras i nedanstående tabell:

Tabell 13

Förvaltningstjänster

Namn på tjänsten	Beskrivning
StartDiagnosticSession (starta diagnossession)	Klienten begär att få starta en diagnossession med en fordonsenhet.
SecurityAccess (säkerhetstillträde)	Klienten begär tillträde till funktioner som är begränsade till auktoriserade användare.

5.1. **Tjänsten StartDiagnosticSession**

5.1.1 *Meddelandebeskrivning*

CPR_025 Tjänsten StartDiagnosticSession används för att aktivera olika diagnossessioner i servern. En diagnossession aktiverar en specifik mängd tjänster enligt Table 17. En session kan aktivera tjänster som är specifika för vissa fordonstillverkare och som inte beskrivs i detta dokument. Användningsreglerna ska uppfylla följande krav:

— Det ska alltid vara exakt en diagnossession aktiv i fordonsenheten.

— När fordonsenheten kopplas in ska den alltid starta StandardDiagnosticSession. Om ingen annan diagnossession startas ska StandardDiagnosticSession vara aktiv så länge fordonsenheten får ström.

— Om en diagnossession som redan är aktiv har begärts av provaren ska fordonsenheten skicka ett positivt svarsmeddelande.

— Varje gång provaren begär en ny diagnossession ska fordonsenheten först skicka ett positivt svarsmeddelande om StartDiagnosticSession innan den nya sessionen blir aktiv i fordonsenheten. Om fordonsenheten inte kan starta den begärda nya diagnossessionen ska den svara med ett negativt svarsmeddelande om StartDiagnosticSession, och den innevarande sessionen ska fortsätta.

CPR_026 En diagnossession ska startas endast om kommunikation har upprättats mellan klienten och fordonsenheten.

CPR_027 De tidsparametrar som definieras i Table 4 ska vara aktiva efter en lyckad StartDiagnosticSession med parametern *diagnosticSession* satt till ”StandardDiagnosticSession” i meddelandet med begäran, om en annan diagnossession tidigare var aktiv.

5.1.2 *Meddelandeformat*

CPR_028 Meddelandeformat för primitiv för *StartDiagnosticSession* anges i detalj i nedanstående tabeller.

▼B

Tabell 14

Meddelande med begäran om StartDiagnosticSession

Byte #	Parameternamn	Hexvärde	Memosymbol (*mnemonic*)
#1	Byte för format – fysisk adressering	80	FMT
#2	Byte för måladress	EE	TGT
#3	Byte för källadress	tt	SRC
#4	Byte för extra längd	02	LEN
#5	**StartDiagnosticSession Request Service Id**	**10**	**STDS**
#6	diagnosticSession = [ett värde från Table 17]	xx	DS_…
#7	Kontrollsumma	00-FF	CS

Tabell 15

Positivt svarsmeddelande om StartDiagnosticSession

Byte #	Parameternamn	Hexvärde	Memosymbol (*mnemonic*)
#1	Byte för format – fysisk adressering	80	FMT
#2	Byte för måladress	tt	TGT
#3	Byte för källadress	EE	SRC
#4	Byte för extra längd	02	LEN
#5	**StartDiagnosticSession Positive Response Service Id**	**50**	**STDSPR**
#6	diagnosticSession = [samma värde som i byte #6 i Table 14]	xx	DS_…
#7	Kontrollsumma	00-FF	CS

Tabell 16

Negativt svarsmeddelande om StartDiagnosticSession

Byte #	Parameternamn	Hexvärde	Memosymbol (*mnemonic*)
#1	Byte för format – fysisk adressering	80	FMT
#2	Byte för måladress	tt	TGT
#3	Byte för källadress	EE	SRC

▼B

Byte #	Parameternamn		Hexvärde	Memosymbol (*mnemonic*)
#4	Byte för extra längd		03	LEN
#5	**Negative Response Service Id**		**7F**	**NR**
#6	StartDiagnosticSession Request Service Id		10	STDS
#7	Svarskod (*responseCode* =	[subFunctionNotSupported ([α])	12	RC_SFNS
		incorrectMessageLength ([β])	13	RC_IML
		conditionsNotCorrect ([γ])	22	RC_CNC
#8	Kontrollsumma		00-FF	CS

([α]) Värdet för byte #6 i svarsmeddelandet stöds inte, dvs. det finns inte i Table 17.
([β]) Längden på meddelandet är felaktig.
([γ]) Kriterierna för att begära StartDiagnosticSession är inte uppfyllda.

5.1.3 *Parameterdefinition*

CPR_029 Parametern *diagnosticSession (DS_)* används av tjänsten StartDiagnosticSession för att välja serverns/servrarnas specifika funktion. Följande diagnossessioner specificeras i detta dokument:

Tabell 17

Definition av värden för diagnosticSession

Hex	Beskrivning	Memosymbol (*mnemonic*)
81	**StandardDiagnosticSession** Denna diagnossession aktiverar alla tjänster som anges i kolumn SD i **Table 1**. Dessa tjänster möjliggör avläsning av data från en server (fordonsenhet). Denna diagnossession är aktiv efter det att initieringen har slutförts med positivt resultat mellan klient (provare) och server (fordonsenhet). Denna diagnossession får skrivas över av andra diagnossessioner som specificeras i detta avsnitt.	**SD**
85	**ECUProgrammingSession** Denna diagnossession aktiverar alla tjänster som anges i kolumn ECUPS i **Table 1**. Dessa tjänster stöder minnesprogrammering i en server (fordonsenhet). Denna diagnossession får skrivas över av andra diagnossessioner som specificeras i detta avsnitt.	**ECUPS**

▼B

Hex	Beskrivning	Memosymbol (*mnemonic*)
87	**ECUAdjustmentSession** Denna diagnossession aktiverar alla tjänster som anges i kolumn ECUAS i **Table 1**. Dessa tjänster stöder kontroll av in-/utdata till/från en server (fordonsenhet). Denna diagnossession får skrivas över av andra diagnossessioner som specificeras i detta avsnitt.	**ECUAS**

5.2. **Tjänsten SecurityAccess**

Skrivning av kalibreringsdata är bara möjlig om fordonsenheten är i kalibreringsläge (CALIBRATION). Utöver att sätta in ett giltigt verkstadskort i fordonsenheten måste fordonsenhetens korrekta PIN-kod anges innan tillträde till kalibreringsläget (CALIBRATION) beviljas.

När fordonsenheten är i kalibrerings- (CALIBRATION) eller kontrolläge (CONTROL) är det också möjligt att få tillträde till in-/utdatalinjen för kalibrering.

Tjänsten SecurityAccess ger möjlighet att ange PIN-koden och att ange för provaren huruvida fordonsenheten är i kalibreringsläge (CALIBRATION).

Det är godtagbart att PIN-koden anges med alternativa metoder.

5.2.1 *Meddelandebeskrivning*

Tjänsten SecurityAccess omfattar två meddelanden: *requestSeed*, eventuellt följt av *sendKey*. Tjänsten SecurityAccess måste utföras efter tjänsten StartDiagnosticSession.

CPR_033 Provaren ska använda meddelandet *requestSeed* för att kontrollera om fordonsenheten är beredd att godta en PIN-kod.

CPR_034 Om fordonsenheten redan är i kalibreringsläge (CALIBRATION) ska den svara på begäran genom att sända ett startvärde (*seed*) som är 0x0000 med hjälp av tjänsten SecurityAccess Positive Response.

CPR_035 Om fordonsenheten är beredd att godta en PIN-kod för verifiering med ett verkstadskort ska den svara på begäran genom att sända ett startvärde (*seed*) som är större än 0x0000 med hjälp av tjänsten SecurityAccess Positive Response.

CPR_036 Om fordonsenheten inte är beredd att godta en PIN-kod från provaren, antingen på grund av att det insatta verkstadskortet inte är giltigt, att inget verkstadskort har satts in eller att fordonsenheten förväntar sig PIN-koden via en annan metod, ska den svara på begäran med ett Negative Response (negativt svar) med en svarskod satt till *conditionsNotCorrectOrRequestSequenceError*.

CPR_037 Provaren ska då eventuellt använda meddelandet *sendKey* för att sända en PIN-kod vidare till fordonsenheten. För att ge kortautentiseringen den tid som krävs ska fordonsenheten använda den negativa svarskoden *requestCorrectlyReceived-ResponsePending* för att utöka svarstiden. Maximal svarstid får dock inte överstiga fem minuter. Så snart den begärda tjänsten har slutförts ska fordonsenheten sända

▼B

ett positivt eller negativt svarsmeddelande med en annan svarskod. Den negativa svarskoden *requestCorrectlyReceived-ResponsePending* får upprepas av fordonsenheten till dess att den begärda tjänsten har slutförts och det slutliga svarsmeddelandet har sänts.

CPR_038 Fordonsenheten ska svara på denna begäran genom att använda tjänsten *SecurityAccess Positive Response* endast när den är i kalibreringsläge (CALIBRATION).

CPR_039 I nedanstående fall ska fordonsenheten svara på denna begäran med Negative Response (negativt svar) med en svarskod som är satt till följande:

— *subFunctionNot supported*: Ogiltigt format för underfunktionens parameter (*accessType*).

— *conditionsNotCorrectOrRequestSequenceError*: Fordonsenheten ej klar att godta en angiven PIN-kod.

— *invalidKey*: PIN-koden inte giltig, max. antal försök att ange PIN-kod har inte uppnåtts.

— *exceededNumberOfAttempts*: PIN-koden inte giltig, max. antal försök att ange PIN-kod har uppnåtts.

— *generalReject*: Rätt PIN-kod men den ömsesidiga autentiseringen med verkstadskortet misslyckades.

5.2.2 *Meddelandeformat – SecurityAccess – requestSeed*

CPR_040 Meddelandeformat för primitiv för *requestSeed* anges i detalj i nedanstående tabeller.

Tabell 18

Meddelande med begäran om SecurityAccess – requestSeed

Byte #	Parameternamn	Hexvärde	Memosymbol (*mnemonic*)
#1	Byte för format – fysisk adressering	80	FMT
#2	Byte för måladress	EE	TGT
#3	Byte för källadress	tt	SRC
#4	Byte för extra längd	02	LEN
#5	**SecurityAccess Request Service Id**	**27**	**SA**
#6	accessType – requestSeed	7D	AT_RSD
#7	Kontrollsumma	00-FF	CS

▼B

Tabell 19

Positivt svarsmeddelande om SecurityAccess – requestSeed

Byte #	Parameternamn	Hexvärde	Memosymbol (*mnemonic*)
#1	Byte för format – fysisk adressering	80	FMT
#2	Byte för måladress	tt	TGT
#3	Byte för källadress	EE	SRC
#4	Byte för extra längd	04	LEN
#5	**SecurityAccess Positive Response Service Id**	**67**	**SAPR**
#6	accessType – requestSeed	7D	AT_RSD
#7	Seed High (högt startvärde)	00-FF	SEEDH
#8	Seed Low (lågt startvärde)	00-FF	SEEDL
#9	Kontrollsumma	00-FF	CS

Tabell 20

Negativt svarsmeddelande om SecurityAccess

Byte #	Parameternamn	Hexvärde	Memosymbol (*mnemonic*)
#1	Byte för format – fysisk adressering	80	FMT
#2	Byte för måladress	tt	TGT
#3	Byte för källadress	EE	SRC
#4	Byte för extra längd	03	LEN
#5	**NegativeResponse Service Id**	**7F**	**NR**
#6	SecurityAccess Request Service Id	27	SA
#7	Svarskod (*responseCode* = [conditionsNotCorrectOrRequestSequenceError	22	RC_CNC
	incorrectMessageLength]	13	RC_IML
#8	Kontrollsumma	00-FF	CS

▼B

5.2.3 *Meddelandeformat – SecurityAccess – sendKey*

CPR_041 Meddelandeformat för primitiv för *sendKey* anges i detalj i nedanstående tabeller.

Tabell 21

Meddelande med begäran om SecurityAccess – sendKey

Byte #	Parameternamn	Hexvärde	Memosymbol (*mnemonic*)
#1	Byte för format – fysisk adressering	80	FMT
#2	Byte för måladress	EE	TGT
#3	Byte för källadress	tt	SRC
#4	Byte för extra längd	m+2	LEN
#5	**SecurityAccess Request Service Id**	**27**	**SA**
#6	accessType – sendKey	7E	AT_SK
#7 till #m+6	Key #1 (hög) … Key #m (låg, m måste vara minst 4 och högst 8)	xx … xx	KEY
#m+7	Kontrollsumma	00-FF	CS

Tabell 22

Positivt svarsmeddelande om SecurityAccess – sendKey

Byte #	Parameternamn	Hexvärde	Memosymbol (*mnemonic*)
#1	Byte för format – fysisk adressering	80	FMT
#2	Byte för måladress	tt	TGT
#3	Byte för källadress	EE	SRC
#4	Byte för extra längd	02	LEN
#5	**SecurityAccess Positive Response Service Id**	**67**	**SAPR**
#6	accessType – sendKey	7E	AT_SK
#7	Kontrollsumma	00-FF	CS

▼B

Tabell 23

Negativt svarsmeddelande om SecurityAccess

Byte #	Parameternamn		Hexvärde	Memosymbol (*mnemonic*)
#1	Byte för format – fysisk adressering		80	FMT
#2	Byte för måladress		tt	TGT
#3	Byte för källadress		EE	SRC
#4	Byte för extra längd		03	LEN
#5	**NegativeResponse Service Id**		**7F**	**NR**
#6	SecurityAccess Request Service Id		27	SA
#7	Svarskod (*responseCode* =	[generalReject	10	RC_GR
		subFunctionNotSupported	12	RC_SFNS
		incorrectMessageLength	13	RC_IML
		conditionsNotCorrectOrRequestSequenceError	22	RC_CNC
		invalidKey	35	RC_IK
		exceededNumberOfAttempts	36	RC_ENA
		requestCorrectlyReceived-ResponsePending]	78	RC_RCR_RP
#8	Kontrollsumma		00-FF	CS

6. DATAÖVERFÖRINGSTJÄNSTER

Tillgängliga tjänster specificeras i nedanstående tabell:

Tabell 24

Dataöverföringstjänster

Namn på tjänsten	Beskrivning
ReadDataByIdentifier (läs data med hjälp av identifierare)	Klienten begär överföring av befintligt värde av en post som nås via *recordDataIdentifier*.
WriteDataByIdentifier (skriv data med hjälp av identifierare)	Klienten begär att få skriva en post som nås via *recordDataIdentifier*.

▼B

6.1. **Tjänsten ReadDataByIdentifier**

6.1.1 *Meddelandebeskrivning*

CPR_050 Tjänsten *ReadDataByIdentifier* används av klienten för att begära datapostvärden från en server. Dessa data identifieras genom *recordDataIdentifier*. Tillverkaren ansvarar för att fordonsenheten uppfyller servervillkoren när denna tjänst utförs.

6.1.2 *Meddelandeformat*

CPR_051 Meddelandeformat för primitiv för *ReadDataByIdentifier* anges i detalj i nedanstående tabeller.

Tabell 25

Meddelande med begäran om ReadDataByIdentifier

Byte #	Parameternamn	Hexvärde	Memosymbol (*mnemonic*)
#1	Byte för format – fysisk adressering	80	FMT
#2	Byte för måladress	EE	TGT
#3	Byte för källadress	tt	SRC
#4	Byte för extra längd	03	LEN
#5	**ReadDataByIdentifier Request Service Id**	**22**	**RDBI**
#6 till #7	recordDataIdentifier = [ett värde från Table 28]	xxxx	RDI_…
#8	Kontrollsumma	00-FF	CS

Tabell 26

Positivt svarsmeddelande om ReadDataByIdentifier

Byte #	Parameternamn	Hexvärde	Memosymbol (*mnemonic*)
#1	Byte för format – fysisk adressering	80	FMT
#2	Byte för måladress	tt	TGT
#3	Byte för källadress	EE	SRC
#4	Byte för extra längd	m+3	LEN
#5	**ReadDataByIdentifier Positive Response Service Id**	**62**	**RDBIPR**
#6 och #7	recordDataIdentifier = [samma värde som byte #6 och #7 i Table 25]	xxxx	RDI_…

▼B

Byte #	Parameternamn		Hexvärde	Memosymbol (*mnemonic*)
#8 till #m+7	dataRecord[] =	[data#1	xx	DREC_DATA1
		:	:	:
		data#m]	xx	DREC_DATAm
#m+8	Kontrollsumma		00-FF	CS

Tabell 27

Negativt svarsmeddelande om ReadDataByIdentifier

Byte #	Parameternamn		Hexvärde	Memosymbol (*mnemonic*)
#1	Byte för format – fysisk adressering		80	FMT
#2	Byte för måladress		tt	TGT
#3	Byte för källadress		EE	SRC
#4	Byte för extra längd		03	LEN
#5	**NegativeResponse Service Id**		**7F**	**NR**
#6	ReadDataByIdentifier Request Service Id		22	RDBI
#7	Svarskod (*responseCode* =	[requestOutOfRange	31	RC_ROOR
		incorrectMessageLength	13	RC_IML
		conditionsNotCorrect]	22	RC_CNC
#8	Kontrollsumma		00-FF	CS

6.1.3 *Parameterdefinition*

CPR_052 Parametern *recordDataIdentifier (RDI_)* i ett meddelande med begäran om *ReadDataByIdentifier* identifierar en datapost.

CPR_053 Värden för *recordDataIdentifier* som definieras i detta dokument visas i tabellen nedan.

Tabellen för *recordDataIdentifier* består av fyra kolumner och flera rader.

— Den **första kolumnen** innehåller det hexadecimala värde som tilldelas den *recordDataIdentifier* som anges i den tredje kolumnen.

— I den **andra kolumnen** anges de dataelement i tillägg 1 som ligger till grund för *recordDataIdentifier* (ibland är omkodning nödvändig).

▼B

— I den **tredje kolumnen** anges motsvarande namn på *recordDataIdentifier*.

— I den **fjärde kolumnen** anges memosymbol för denna *recordDataIdentifier*.

Tabell 28

Definition av värden för recordDataIdentifier

Hex	Dataelement	Namn på *recordDataIdentifier* (se format i avsnitt 8.2)	Memosymbol (*mnemonic*)
F90B	CurrentDateTime	TimeDate	RDI_TD
F912	HighResOdometer	HighResolutionTotalVehicle-Distance	RDI_HRTVD
F918	K-ConstantOfRecordingEquipment	Kfactor	RDI_KF
F91C	L-TyreCircumference	LfactorTyreCircumference	RDI_LF
F91D	W-VehicleCharacteristicConstant	WvehicleCharacteristicFactor	RDI_WVCF
F921	TyreSize	TyreSize	RDI_TS
F922	nextCalibrationDate	NextCalibrationDate	RDI_NCD
F92C	SpeedAuthorised	SpeedAuthorised	RDI_SA
F97D	vehicleRegistrationNation	RegisteringMemberState	RDI_RMS
F97E	VehicleRegistrationNumber	VehicleRegistrationNumber	RDI_ VRN
F190	VehicleIdentificationNumber	VIN	RDI_ VIN

CPR_054 Parametern *dataRecord (DREC_)* används av det positiva svarsmeddelandet för *ReadDataByIdentifier* för att tillhandahålla det datapostvärde som identifieras av *recordDataIdentifier* till klienten (provaren). Dataformaten specificeras i avsnitt 8. Ytterligare valfria användardata (*dataRecords*), inklusive in- och utdata samt interna data som är specifika för fordonsenheten, kan införas, men de definieras inte i detta dokument.

6.2. Tjänsten WriteDataByIdentifier

6.2.1 *Meddelandebeskrivning*

CPR_056 Tjänsten *WriteDataByIdentifier* används av klienten för att skriva datapostvärden till en server. Dessa data identifieras genom *recordDataIdentifier*. Tillverkaren ansvarar för att fordonsenheten uppfyller servervillkoren när denna tjänst utförs. Vid uppdatering av de parametrar som förtecknas i Table 28 måste fordonsenheten vara i kalibreringsläge (CALIBRATION).

6.2.2 *Meddelandeformat*

CPR_057 Meddelandeformat för primitiv för *WriteDataByIdentifier* anges i detalj i nedanstående tabeller.

▼B

Tabell 29

Meddelande med begäran om WriteDataByIdentifier

Byte #	Parameternamn	Hexvärde	Memosymbol (*mnemonic*)
#1	Byte för format – fysisk adressering	80	FMT
#2	Byte för måladress	EE	TGT
#3	Byte för källadress	tt	SRC
#4	Byte för extra längd	m + 3	LEN
#5	**WriteDataByIdentifier Request Service Id**	**2E**	**WDBI**
#6 till #7	*recordDataIdentifier* = [ett värde från Table 28]	xxxx	RDI_…
#8 till #m+7	dataRecord[] = [data#1 : data#m]	xx : xx	DREC_DATA1 : DREC_DATAm
#m+8	Kontrollsumma	00-FF	CS

Tabell 30

Positivt svarsmeddelande om WriteDataByIdentifier

Byte #	Parameternamn	Hexvärde	Memosymbol (*mnemonic*)
#1	Byte för format – fysisk adressering	80	FMT
#2	Byte för måladress	tt	TGT
#3	Byte för källadress	EE	SRC
#4	Byte för extra längd	03	LEN
#5	**WriteDataByIdentifier Positive Response Service Id**	**6E**	**WDBIPR**
#6 till #7	recordDataIdentifier = [samma värde som byte #6 och #7 i Table 29]	xxxx	RDI_…
#8	Kontrollsumma	00-FF	CS

▼B

Tabell 31

Negativt svarsmeddelande om WriteDataByIdentifier

Byte #	Parameternamn		Hexvärde	Memosymbol (*mnemonic*)
#1	Byte för format – fysisk adressering		80	FMT
#2	Byte för måladress		tt	TGT
#3	Byte för källadress		EE	SRC
#4	Byte för extra längd		03	LEN
#5	**NegativeResponse Service Id**		**7F**	**NR**
#6	WriteDataByIdentifier Request Service Id		2E	WDBI
#7	Svarskod (*responseCode* =	[requestOutOfRange	31	RC_ROOR
		incorrectMessageLength	13	RC_IML
		conditionsNotCorrect]	22	RC_CNC
#8	Kontrollsumma		00-FF	CS

6.2.3 *Parameterdefinition*

Parametern *recordDataIdentifier (RDI_)* definieras i Table 28.

Parametern *dataRecord (DREC_)* används av meddelandet med begäran om *WriteDataByIdentifier* för att tillhandahålla servern (fordonsenheten) de datapostvärden som identifieras genom *recordDataIdentifier*. Dataformaten specificeras i avsnitt 8.

7. KONTROLL AV PROVPULSER – FUNKTIONSENHET FÖR KONTROLL AV IN-/UTDATA

Tillgängliga tjänster specificeras i nedanstående tabell:

Tabell 32

Funktionsenhet för kontroll av in-/utdata

Namn på tjänsten	Beskrivning
InputOutputControlByIdentifier (kontroll av in-/utdata med hjälp av identifierare)	Klienten begär kontroll av in-/utdata som är specifika för servern.

7.1. **Tjänsten InputOutputControlByIdentifier**

7.1.1 *Meddelandebeskrivning*

Det finns en koppling via frontanslutningen som gör det möjligt att kontrollera eller övervaka provpulser med hjälp av en lämplig provare.

▼B

CPR_058 Denna linje för in-/utsignaler vid kalibrering kan konfigureras med K-line-kommandon med hjälp av tjänsten *InputOutputControlByIdentifier* för att välja den in-/utfunktion som krävs för linjen. Linjen har följande tillstånd:

— *disabled* (avaktiverat).

— *speedSignalInput*, där linjen för in-/utsignaler vid kalibrering används för inmatning av en hastighetssignal (provsignal) som ersätter hastighetssignalen från rörelsesensorn. Denna funktion är inte tillgänglig i kontrolläge (CONTROL).

— *realTimeSpeedSignalOutputSensor*, där linjen för in-/utsignaler vid kalibrering används för utdata i form av hastighetssignalen från rörelsesensorn.

— *RTCOutput*, där linjen för in-/utsignaler vid kalibrering används för utdata i form av klocksignalen (UTC). Denna funktion är inte tillgänglig i kontrolläge (CONTROL).

CPR_059 Fordonsenheten måste ha påbörjat en inställningssession och den måste vara i kalibrerings- (CALIBRATION) eller kontrolläge (CONTROL) för att konfigurera linjens tillstånd. När fordonsenheten är i kalibreringsläge (CALIBRATION) kan de fyra linjetillstånden väljas (*disabled*, *speedSignalInput*, *realTimeSpeedSignalOutputSensor*, *RTCOutput*). När fordonsenheten är i kontrolläge (CONTROL) kan endast två av de fyra linjetillstånden väljas (*disabled*, *realTimeSpeedSignalOutputSensor*). Vid avslutande av inställningssession eller av kalibrerings- (CALIBRATION) eller kontrolläge (CONTROL) ska fordonsenheten se till att linjen för in-/utsignaler vid kalibrering återställs till ”avaktiverat” (förvalt) tillstånd.

CPR_060 Om hastighetspulser tas emot i fordonsenhetens ingående linje för hastighetssignal i realtid medan linjen för in-/utsignaler vid kalibrering är inställd för indata ska linjen för in-/utsignaler vid kalibrering ställas om för utdata eller återställas till det avaktiverade tillståndet.

CPR_061 Sekvensen ska vara följande:

— Upprätta kommunikation genom tjänsten StartCommunication.

— Påbörja en inställningssession genom tjänsten StartDiagnosticSession och stå i kalibrerings- (CALIBRATION) eller kontrolläge (CONTROL) (ordningen på dessa två operationer saknar betydelse).

— Ändra tillstånd för utdata med hjälp av InputOutputControlByIdentifier.

7.1.2 *Meddelandeformat*

CPR_062 Meddelandeformat för primitiv för *InputOutputControlByIdentifier* anges i detalj i nedanstående tabeller.

▼B

Tabell 33

Meddelande med begäran om InputOutputControlByIdentifier

Byte #	Parameternamn	Hexvärde	Memosymbol (*mnemonic*)
#1	Byte för format – fysisk adressering	80	FMT
#2	Byte för måladress	EE	TGT
#3	Byte för källadress	tt	SRC
#4	Byte för extra längd	xx	LEN
#5	**InputOutputControlByIdentifier Request Sid**	**2F**	**IOCBI**
#6 och #7	InputOutputIdentifier = [CalibrationInputOutput]	F960	IOI_CIO
#8 eller #8 till #9	ControlOptionRecord = [		COR_…
	inputOutputControlParameter – ett värde från Table 36	xx	IOCP_…
	controlState – ett värde från Table 37 (se anmärkning nedan)]	xx	CS_…
#9 eller #10	Kontrollsumma	00-FF	CS

Anmärkning: Parametern controlState ingår endast i vissa fall (se avsnitt 7.1.3).

Tabell 34

Positivt svarsmeddelande om InputOutputControlByIdentifier

Byte #	Parameternamn	Hexvärde	Memosymbol (*mnemonic*)
#1	Byte för format – fysisk adressering	80	FMT
#2	Byte för måladress	tt	TGT
#3	Byte för källadress	EE	SRC
#4	Byte för extra längd	xx	LEN
#5	**inputOutputControlByIdentifier Positive Response SId**	**6F**	**IOCBIPR**
#6 och #7	inputOutputIdentifier = [CalibrationInputOutput]	F960	IOI_CIO
#8 eller #8 till #9	controlStatusRecord = [		CSR_
	inputOutputControlParameter (samma värde som byte #8 i Table 33)	xx	IOCP_…
	controlState (samma värde som byte #9 i Table 33)] (i förekommande fall)	xx	CS_…
#9 eller #10	Kontrollsumma	00-FF	CS

▼B

Tabell 35

Negativt svarsmeddelande om InputOutputControlByIdentifier

Byte #	Parameternamn	Hexvärde	Memosymbol (*mnemonic*)
#1	Byte för format – fysisk adressering	80	FMT
#2	Byte för måladress	tt	TGT
#3	Byte för källadress	EE	SRC
#4	Byte för extra längd	03	LEN
#5	**NegativeResponse Service Id**	**7F**	**NR**
#6	inputOutputControlByIdentifier Request SId	2F	IOCBI
#7	Svarskod (*responseCode = [*		
	incorrectMessageLength	13	RC_IML
	conditionsNotCorrect	22	RC_CNC
	requestOutOfRange	31	RC_ROOR
	deviceControlLimitsExceeded]	7 A	RC_DCLE
#8	Kontrollsumma	00-FF	CS

7.1.3 *Parameterdefinition*

CPR_064 Parametern *inputOutputControlParameter (IOCP_)* definieras i nedanstående tabell.

Tabell 36

Definition av värden för InputOutputControlByIdentifier

Hex	Beskrivning	Memosymbol (*mnemonic*)
00	**ReturnControlToECU** Detta värde ska ange för servern (fordonsenheten) att provaren inte längre har kontroll över linjen för in-/utsignaler vid kalibrering.	RCTECU
01	**ResetToDefault** Med detta värde får servern (fordonsenheten) en begäran om att återställa linjen för in-/utsignaler vid kalibrering till dess förvalda tillstånd.	RTD

▼B

Hex	Beskrivning	Memosymbol (*mnemonic*)
03	**ShortTermAdjustment** Med detta värde får servern (fordonsenheten) en begäran om att ställa in linjen för in-/utsignaler vid kalibrering på det värde som ingår i parametern *controlState*.	STA

CPR_065 Parametern *controlState* ingår endast när *inputOutputControlParameter* har satts till *ShortTermAdjustment*, och den definieras i nedanstående tabell.

Tabell 37

Definition av värden för controlState

Läge	Hexvärde	Beskrivning
Avaktivera	00	Linjen för in-/utsignaler är avaktiverad (förvalt tillstånd).
Aktivera	01	Aktivera linjen för in-/utsignaler vid kalibrering som *speedSignalInput*.
Aktivera	02	Aktivera linjen för in-/utsignaler vid kalibrering som *realTimeSpeedSignalOutputSensor*.
Aktivera	03	Aktivera linjen för in-/utsignaler vid kalibrering som *RTCOutput*.

8. FORMAT FÖR DATARECORDS

I detta avsnitt beskrivs följande:

— Allmänna regler som ska tillämpas på de olika parametrar som överförs av fordonsenheten till provaren.

— Format som ska användas för data som överförs via de dataöverföringstjänster som beskrivs i avsnitt 6.

CPR_067 Det ska finnas stöd i fordonsenheten för alla parametrar som beskrivs här.

CPR_068 Data som överförs av fordonsenheten till provaren som svar på en begäran ska vara uppmätta (dvs. aktuellt värde på den begärda parametern enligt fordonsenhetens mätning eller observation).

8.1. **Intervall för överförda parametrar**

CPR_069 Table 38 visar de intervall som används för att avgöra huruvida en överförd parameter har ett giltigt värde.

CPR_070 Med hjälp av värdena i det intervall som betecknas ”felindikator” kan fordonsenheten omedelbart meddela att det för närvarande inte finns några tillgängliga giltiga parameterdata på grund av någon typ av fel i färdskrivaren.

CPR_071 Med hjälp av värdena i intervallet ”ej tillgängligt” kan fordonsenheten skicka ett meddelande som innehåller en parameter som inte är tillgänglig eller som inte är giltig i den aktuella modulen. Med hjälp av värdena i intervallet ”ej begärt” kan en enhet skicka ett kommandomeddelande och identifiera de parametrar för vilka inget svar förväntas från den mottagande enheten.

▼B

CPR_072 Om ett komponentfel förhindrar överföringen av giltiga data för en parameter, bör den felindikator som beskrivs i Table 38 användas i stället för parameterns data. Om uppmätta eller beräknade data har ett värde som är giltigt men som inte ligger inom det fastställda parameterintervallet, bör felindikatorn emellertid inte användas. I sådana fall bör data överföras i form av motsvarande minsta eller största parametervärde.

Tabell 38

Intervall för dataRecords

Intervallbeteckning	1 byte (Hexvärde)	2 byte (Hexvärde)	4 byte (Hexvärde)	ASCII
Giltig signal	00 till FA	0000 till FAFF	00000000 till FAFFFFFF	1–254
Parameterspecifik indikator	FB	FB00 till FBFF	FB000000 till FBFFFFFF	Saknas
Intervall reserverat för framtida indikatorbitar	FC till FD	FC00 till FDFF	FC000000 till FDFFFFFF	Saknas
Felindikator	FE	FE00 till FEFF	FE000000 till FEFFFFFF	0
Ej tillgängligt eller ej begärt	FF	FF00 till FFFF	FF000000 till FFFFFFFF	FF

CPR_073 För ASCII-kodade parametrar är tecknet ”*” reserverat som avgränsare.

8.2. **Format för dataRecords**

I tabellerna Table 39–Table 42 nedan beskrivs de format som ska användas via tjänsterna *ReadDataByIdentifier* och *WriteDataByIdentifier*.

CPR_074 Table 39 innehåller uppgifter om längd, upplösning och driftsintervall för varje parameter som identifieras med hjälp av sin *recordDataIdentifier*:

Tabell 39

Format för dataRecords

Parameternamn	Datalängd (byte)	Upplösning	Driftsintervall
TimeDate	8	Se vidare detaljer i Table 40.	
HighResolutionTotalVehicle-Distance	4	5 m ökning per bit, 0 m offset	0 till +21 055 406 km
Kfactor	2	0,001 pulser/m ökning per bit, 0 offset	0 till 64,255 pulser/m
LfactorTyreCircumference	2	0,125 10^{-3} m ökning per bit, 0 offset	0 till +8,031 m
WvehicleCharacteristicFactor	2	0,001 pulser/m ökning per bit, 0 offset	0 till 64,255 pulser/m
TyreSize	15	ASCII	ASCII
NextCalibrationDate	3	Se vidare detaljer i Table 41.	
SpeedAuthorised	2	1/256 km/h ökning per bit, 0 offset	0 till 250,996 km/h

▼B

Parameternamn	Datalängd (byte)	Upplösning	Driftsintervall
RegisteringMemberState	3	ASCII	ASCII
VehicleRegistrationNumber	14	Se vidare detaljer i Table 42.	
VIN	17	ASCII	ASCII

CPR_075 Table 40 innehåller uppgifter om formaten för de olika byte som ingår i parametern *TimeDate*:

Tabell 40

Detaljformat för TimeDate (värde # F90B för recordDataIdentifier)

Byte	Parameterdefinition	Upplösning	Driftsintervall
1	Sekunder	0,25 s ökning per bit, 0 s offset	0 till 59,75 s
2	Minuter	1 min ökning per bit, 0 min offset	0 till 59 min
3	Timmar	1 h ökning per bit, 0 h offset	0 till 23 h
4	Månad	1 månad ökning per bit, 0 månader offset	1 till 12 månader
5	Dag	0,25 dagar ökning per bit, 0 dagar offset (se anmärkning under Table 41)	0,25 till 31,75 dagar
6	År	1 år ökning per bit, +1985 år offset (se anmärkning under Table 41)	1985 till 2235 år
7	Lokal offset – minuter	1 min ökning per bit, – 125 min offset	– 59 till +59 min
8	Lokal offset – timmar	1 h ökning per bit, – 125 h offset	– 23 till +23 h

CPR_076 Table 41 innehåller uppgifter om formaten för de olika byte som ingår i parametern *NextCalibrationDate*:

Tabell 41

Detaljformat för NextCalibrationDate (värde # F922 för recordDataIdentifier)

Byte	Parameterdefinition	Upplösning	Driftsintervall
1	Månad	1 månad ökning per bit, 0 månader offset	1 till 12 månader
2	Dag	0,25 dagar ökning per bit, 0 dagar offset (se anmärkning nedan)	0,25 till 31,75 dagar
3	År	1 år ökning per bit, +1985 år offset (se anmärkning nedan)	1985 till 2235 år

▼B

Anmärkning beträffande användningen av parametern för ”dag”:

1) 0 är ett ogiltigt värde för datum. Värdena 1, 2, 3 och 4 betecknar den första dagen i månaden; 5, 6, 7 och 8 betecknar den andra dagen i månaden osv.

2) Denna parameter ändrar eller påverkar inte parametern för ”timmar” ovan.

Anmärkning beträffande användningen av parametern för ”år”:

Värdet 0 för år betecknar år 1985; värdet 1 betecknar 1986 osv.

CPR_078 Table 42 innehåller uppgifter om formaten för de olika byte som ingår i parametern *VehicleRegistrationNumber*:

Tabell 42

Detaljformat för VehicleRegistrationNumber (värde # F97E för recordDataIdentifier)

Byte	Parameterdefinition	Upplösning	Driftsintervall
1	Teckentabell (enligt definitionen i tillägg 1)	ASCII	01 till 0 A
2 – 14	Fordonets registreringsnummer (enligt definitionen i tillägg 1)	ASCII	ASCII

▼B

Tillägg 9

TYPGODKÄNNANDE FÖRTECKNING ÖVER MINSTA NÖDVÄNDIGA UPPSÄTTNING PROV

INNEHÅLLSFÖRTECKNING

1. INLEDNING

2. FUNKTIONSPROVNING AV FORDONSENHET

3. FUNKTIONSPROVNING AV RÖRELSESENSOR

4. FUNKTIONSPROVNING AV FÄRDSKRIVARKORT

5. PROVNING AV EXTERN GNSS-ANORDNING

6. PROVNING AV KOMMUNIKATIONSANORDNING FÖR FJÄRRAVLÄSNING

7. FUNKTIONSPROVNING AV PAPPER

8. PROVNING AV DRIFTSKOMPATIBILITET

1. INLEDNING

1.1. **Typgodkännande**

EG-typgodkännande för en färdskrivare (eller komponent) eller ett färdskrivarkort bygger på följande:

— En **säkerhetscertifiering**, baserad på specifikationer enligt CC (*Common Criteria*), i förhållande till ett säkerhetsmål som till fullo överensstämmer med tillägg 10 till denna bilaga.

— En **funktionscertifiering**, utförd av en myndighet i en medlemsstat, som intygar att det provade föremålet uppfyller kraven i denna bilaga med avseende på funktioner, mätnoggrannhet och miljöegenskaper.

— En **certifiering av driftskompatibiliteten**, utförd av ett behörigt organ, som intygar att färdskrivaren (eller färdskrivarkortet) är fullständigt driftskompatibel(t) med de modeller av färdskrivarkort (eller färdskrivare) som krävs (se kapitel 8 i denna bilaga).

I detta tillägg anges de prov som minst ska utföras av en myndighet i en medlemsstat vid funktionsprovningarna, och de prov som minst ska utföras av ett behörigt organ vid provningarna av driftskompatibiliteten. Förfaranden för att utföra proven eller typen av prov specificeras inte ytterligare.

Säkerhetscertifieringen omfattas inte av detta tillägg. Om vissa prov som krävs för typgodkännande utförs vid säkerhetsutvärderingen och säkerhetscertifieringen behöver dessa prov inte utföras igen. I detta fall behöver bara resultaten från dessa säkerhetsprov undersökas. De krav som förväntas bli provade (eller som är nära förknippade med prov som förväntas bli utförda) vid säkerhetscertifieringen är markerade med ”*” i detta tillägg.

De numrerade kraven hänvisar till huvudtexten i bilagan, medan övriga krav hänvisar till de andra tilläggen (t.ex. hänvisar ”PIC_001” till krav PIC_001 i tillägg 3 om piktogram).

I detta tillägg åtskiljs typgodkännandet av rörelsesensorn, fordonsenheten och den externa GNSS-anordningen, som alla betraktas som komponenter

▼B

i färdskrivaren. Varje komponent kommer att få sitt eget typgodkännandeintyg, där övriga driftskompatibla komponenter kommer att anges. Funktionsprovet av rörelsesensorn (eller den externa GNSS-anordningen) utförs tillsammans med fordonsenheten och omvänt.

Driftskompatibilitet mellan varje modell av rörelsesensor (respektive extern GNSS-anordning) och varje modell av fordonsenhet är inte nödvändig. I detta fall kan ett typgodkännande för en rörelsesensor (respektive extern GNSS-anordning) beviljas endast i kombination med typgodkännandet för den relevanta fordonsenheten och omvänt.

1.2. **Referenser**

Följande referenser används i detta tillägg:

IEC 60068-2-1: Environmental testing – Part 2-1: Tests – Test A: Cold

IEC 60068-2-2: Basic environmental testing procedures; part 2: tests; tests B: dry heat

(sinusoidal). IEC 60068-2-6:

Environmental testing – Part 2: Tests – Test Fc: Vibration IEC 60068-2-14:

Environmental testing; Part 2-14: Tests; Test N: Change of temperature IEC 60068-2-27:

Environmental testing. Part 2: Tests. Test Ea and guidance: Shock IEC 60068-2-30:

Environmental testing – Part 2-30: Tests – Test Db: Damp heat, cyclic (12 h + 12 h cycle) IEC 60068-2-64:

Environmental testing – Part 2-64: Tests – Test Fh: Vibration, broadband random and guidance IEC 60068-2-78

Environmental testing – Part 2-78: Tests – Test Cab: Damp heat, steady state ISO 16750-3 –

Mechanical loads (2012-12) ISO 16750-4 –

Climatic loads (2010-04). ISO 20653: Road vehicles – Degree of protection (IP code) – Protection of electrical equipment against foreign objects, water and access

ISO 10605:2008 + Technical Corrigendum:2010 + AMD1:2014 Road vehicles – Test methods for electrical disturbances from electrostatic discharge

ISO 7637-1:2002 + AMD1: 2008 Road vehicles – Electrical disturbances from conduction and coupling – Part 1: Definitions and general considerations.

ISO 7637-2 Road vehicles – Electrical disturbances from conduction and coupling – Part 2: Electrical transient conduction along supply lines only.

ISO 7637-3 Road vehicles – Electrical disturbances from conduction and coupling – Part 3: Electrical transient transmission by capacitive and inductive coupling via lines other than supply lines.

ISO/IEC 7816-1 Identification cards – Integrated circuit(s) cards with contacts – Part 1: Physical characteristics..

▼B

ISO/IEC 7816-2 Information technology – Identification cards – Integrated circuit(s) cards with contacts – Part 2: Dimensions and location of the contacts.

ISO/IEC 7816-3 Information technology – Identification cards – Integrated circuit(s) cards with contacts – Part 3: Electronic signals and transmission protocol.

ISO/IEC 10373-1:2006 + AMD1:2012 Identification cards – Test methods – Part 1: General characteristics

ISO/IEC 10373-3:2010 + Technical Corrigendum:2013 Identification cards – Test methods – Part 3: Integrated circuit cards with contacts and related interface devices

ISO 16844-3:2004, Cor 1:2006 Road vehicles – Tachograph systems – Part 3: Motion sensor interface (with vehicle units).

ISO 16844-4 Road vehicles – Tachograph systems – Part 4: CAN interface

ISO 16844-6 Road vehicles – Tachograph systems – Part 6: Diagnostics

ISO 16844-7 Road vehicles – Tachograph systems – Part 7: Parameters

ISO 534 Paper and board – Determination of thickness, density and specific volume

UN ECE R10 Uniform provisions concerning the approval of vehicles with regard to electromagnetic compatibility (United Nation Economic Commission for Europe)

2. FUNKTIONSPROVNING AV FORDONSENHET

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		03, 04, 05, 07, 382,
3.2	Driftlägen		09–11*, 132, 133
3.3	Rättigheter till tillgång 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*, 132
3.5	Mätning av hastighet och sträcka		21–31

▼B

Nr	Prov	Beskrivning	Tillämpliga krav
3.6	Tidsmätning (prov utförs vid 20 °C)		38–43
3.7	Övervakning av föraraktiviteter		44–53, 132
3.8	Övervakning av förarstatus		54, 55, 132
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, 132
3.13	Utrustningens identifieringsdata		93*, 94*, 97, 100
3.14	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		134, 135,, 136*, 137*, 139*, 140, 141 142, 143, 144*, 145*, 146*, 147, 148
3.28	Visning		90, 132, 149–166, PIC_001, DIS_001
3.29	Utskrift		90, 132, 167–179, PIC_001, PRT_001–PRT_014
3.30	Varning		132, 180–189, PIC_001
3.31	Överföring av data till externa media		90, 132, 190–194
3.32	Fjärravläsning vid riktade vägkontroller		195–197
3.33	Utdata till ytterligare externa anordningar		198, 199

▼B

Nr	Prov	Beskrivning	Tillämpliga krav
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
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 (*dwell time*) 2 timmar vid varje temperatur) En minskad uppsättning av 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

▼B

Nr	Prov	Beskrivning	Tillämpliga krav
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 x 12 timmar (12 timmar per axel). I ISO 16750-3 krävs inget prov med sinusformade vibrationer för anordningar som är placerade i en fjädrad *(decoupled)* fordonshytt. 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 m/s^2, effektivvärde i längdled 11,8 m/s^2, effektivvärde i sidled 13,1 m/s^2, 3 axlar, 32 timmar per axel, inklusive temperaturcykel mellan – 20 °C och + 70 °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.	219
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 °C, 1 timme 12 V-versioner: 17 V vid + 40 °C, 1 timme (ISO 16750-2)	216

▼B

Nr	Prov	Beskrivning	Tillämpliga krav
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: +/– 4 kV för kontakt och +/– 8 kV för urladdning till luft	218
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: Vs = – 450 V, Ri = 50 Ohm puls 2a: Vs = +37 V, Ri = 2 Ohm puls 2b: Vs = +20 V, Ri = 0,05 Ohm puls 3a: Vs = – 150 V, Ri = 50 Ohm puls 3b: Vs = +150 V, Ri = 50 Ohm puls 4: Vs = – 16 V, Va = – 12 V, t6 = 100 ms puls 5: Vs = +120 V, Ri = 2,2 Ohm, td = 250 ms För 12 V-versioner: överensstämmelse med ISO 7637-1 + ECE förordning nr 10 Rev. 3: puls 1: Vs = – 75 V, Ri = 10 Ohm puls 2a: Vs = +37 V, Ri = 2 Ohm puls 2b: Vs = +10 V, Ri = 0,05 Ohm puls 3a: Vs = – 112 V, Ri = 50 Ohm puls 3b: Vs = +75 V, Ri = 50 Ohm puls 4: Vs = – 6 V, Va = – 5 V, t6 = 15 ms puls 5: Vs = +65 V, Ri = 3 Ohm, td = 100 ms Puls 5 ska endast provas för de fordonsenheter som är avsedda att installeras i fordon för vilka inget externt gemensamt skydd mot laddningsdump (*load dump*) används. För förslag till laddningsdump, se ISO 16750-2, 4:e utgåvan, kapitel 4.6.4.	218

▼B

3. FUNKTIONSPROVNING AV RÖRELSESENSOR

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
2.4	Plombering		398, 401–405
3	**Funktionsprov**		
3.1	Sensorns identifieringsdata		95–97*
3.2	Parning av rörelsesensor och fordonsenhet		122*, 204
3.3	Rörelseavkänning Rörelsemätningens noggrannhet		30–35
3.4	Gränssnitt med fordonsenhet		02
3.5	Kontrollera att rörelsesensorn är immun mot magnetfält, eller kontrollera att rörelsesensorn reagerar på konstanta magnetfält som stör fordonets rörelseavkänning, så att en ansluten fordonsenhet kan upptäcka, registrera och lagra sensorfel.		217
4	**Miljöprovningar**		
4.1	Drifttemperatur	Kontrollera funktionalitet (enligt definition i prov nr. 3.3) i temperaturintervallet från – 40 °C till + 135 °C genom följande: IEC 60068-2-1, test Ad, med en provtid av 96 timmar vid en lägsta temperatur av To_{min}. IEC 60068-2-2, test Bd, med en provtid av 96 timmar vid en högsta temperatur av To_{max}. Prov enligt ISO 16750-4, kapitel 5.1.1.2: Low temperature operation test (24 h vid – 40 °C). Detta prov hänvisar till IEC 60068-2-1: Environmental testing – Part 2-1: Tests – Test A: Cold IEC 68-2-2, test Bd, med en provningsvaraktighet av 96 timmar vid en lägsta temperatur av – 40 °C. Prov enligt ISO 16750-4, kapitel 5.1.2.2: High temperature operation test (96 h vid 135 °C). Detta prov hänvisar till IEC 60068-2-2: Basic environmental testing procedures; part 2: tests; tests B: dry heat	213

▼B

Nr	Prov	Beskrivning	Tillämpliga krav
4.2	Temperaturcykler	Prov enligt ISO 16750-4, kapitel 5.3.2: Rapid change of temperature with specified transition duration (– 40 °C/+ 135 °C, 20 cykler, uppehållstid (*dwell time*) 2 timmar vid varje temperatur) IEC 60068-2-14: Environmental testing – Part 2-14: Tests; Test N: Change of temperature.	213
4.3	Luftfuktighetscykler	Kontrollera funktionalitet (enligt definition i prov nr 3.3) 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
4.4	Vibrationer	ISO 16750-3, kapitel 4.1.2.6: Test VI: Commercial vehicle, engine, gearbox Blandat vibrationsprov, inklusive följande: a) Prov med sinusformade vibrationer, 20–520 Hz, 11,4– 120 m/s^2, <= 0,5 okt/min. b) Prov med slumpartade vibrationer, 10–2 000 Hz, effektivvärde 177 m/s^2. 94 timmar per axel, inklusive temperaturcykel från – 20 °C till + 70 °C Detta prov hänvisar till IEC 60068-2-80: Environmental testing – Part 2-80: Tests – Test Fi: Vibration – Mixed mode	219
4.5	Mekaniska stötar	ISO 16750-3, kapitel 4.2.3: Test VI: Test for devices in or on the gearbox Halvsinusformad stöt, acceleration (ännu ej överenskommen) i intervallet 3 000–15 000 m/s^2, pulsvaraktighet ännu ej överenskommen men < 1 ms, antal stötar ännu ej överenskommet). Detta prov hänvisar till IEC 60068-2-27: Environmental testing. Part 2: Tests. Test Ea and guidance: Shock.	219
4.6	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 IP 64)	220, 221
4.7	Skydd mot omkastade poler	Kontrollera att rörelsesensorn tål en omkastning av strömtillförseln.	216
4.8	Skydd mot kortslutning	Kontrollera att in- och utsignaler är skyddade mot kortslutning i strömtillförsel och jord.	216

▼B

Nr	Prov	Beskrivning	Tillämpliga krav
5	**EMC**		
5.1	Utstrålning och känslighet	Kontrollera 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
5.3	Känslighet för överförda transienter i datakablar	För 24 V-versioner: överensstämmelse med ISO 7637-2 + ECE förordning nr 10 Rev. 3: puls 1a: Vs = – 450 V, Ri = 50 Ohm puls 2a: Vs = +37 V, Ri = 2 Ohm puls 2b: Vs = +20 V, Ri = 0,05 Ohm puls 3a: Vs = – 150 V, Ri = 50 Ohm puls 3b: Vs = +150 V, Ri = 50 Ohm puls 4: Vs = – 16 V, Va = – 12 V, t6 = 100 ms puls 5: Vs = +120 V, Ri = 2,2 Ohm, td = 250 ms För 12 V-versioner: överensstämmelse med ISO 7637-1 + ECE förordning nr 10 Rev. 3: puls 1: Vs = – 75 V, Ri = 10 Ohm puls 2a: Vs = +37 V, Ri = 2 Ohm puls 2b: Vs = +10 V, Ri = 0,05 Ohm puls 3a: Vs = – 112 V, Ri = 50 Ohm puls 3b: Vs = +75 V, Ri = 50 Ohm puls 4: Vs = – 6 V, Va = – 5 V, t6 = 15 ms puls 5: Vs = +65 V, Ri = 3 Ohm, td = 100 ms Puls 5 ska endast provas för de fordonsenheter som är avsedda att installeras i fordon för vilka inget externt gemensamt skydd mot laddningsdump (*load dump*) används. För förslag till laddningsdump, se ISO 16750-2, 4:e utgåvan, kapitel 4.6.4.	218

4. FUNKTIONSPROVNING AV FÄRDSKRIVARKORT

I detta avsnitt ingår prov

nr. 5 ”Protokollprov”,

nr. 6 ”Kortets struktur” och

nr. 7 ”Funktionsprov”

som kan utföras av utvärderaren eller certifieraren under säkerhetscertifieringen enligt CC (*Common Criteria*) av chipmodulen.

Prov nr. 2.3 är samma som prov nr. 4.2. Dessa utgör de mekaniska proven av det egentliga kortet tillsammans med chipmodulen. Om någon av dessa komponenter (det egentliga kortet eller chipmodulen) ändras är dessa prov nödvändiga.

▼B

Nr	Prov	Beskrivning	Tillämpliga krav
1	**Administrativ provning**		
1.1	Dokumentation	Dokumentationens korrekthet	
2	**Kort**		
2.1	Utformning av tryckta uppgifter	Kontrollera att alla skyddsfunktioner och synliga uppgifter är korrekt tryckta på kortet och att de uppfyller bestämmelserna. [Beteckning] Bilaga 1C, kapitel 4.1 Synliga uppgifter, 227) Framsidan ska innehålla följande: Ordet ”förarkort”, ”kontrollkort”, ”verkstadskort” eller ”företagskort”, beroende på korttyp, tryckt med versaler på det eller de officiella språken i den medlemsstat som utfärdar kortet. [Medlemsstatens namn] Bilaga 1C, kapitel 4.1 Synliga uppgifter, 228) Framsidan ska innehålla följande: Namnet på den medlemsstat som utfärdar kortet (frivilligt). [Nationalitetsbeteckning] Bilaga 1C, kapitel 4.1 Synliga uppgifter, 229) Framsidan ska innehålla följande: Nationalitetsbeteckningen för den medlemsstat som utfärdar kortet, inlagd i vitt i en blå rektangel och omgiven av tolv gula stjärnor. [Numrering] Bilaga 1C, kapitel 4.1 Synliga uppgifter, 232) Baksidan ska innehålla följande: En förklaring av de numrerade punkterna på kortets framsida. [Färg] Bilaga 1C, kapitel 4.1 Synliga uppgifter, 234) Färdskrivarkorten ska tryckas i följande dominerande bakgrundsfärger: — Förarkort: vitt. — Verkstadskort: rött. — Kontrollkort: blått. — Företagskort: gult.	227–229, 232, 234–236

▼B

Nr	Prov	Beskrivning	Tillämpliga krav
		[Säkerhet] Bilaga 1C, kapitel 4.1 Synliga uppgifter, 235) Färdskrivarkorten ska åtminstone ha följande skyddsfunktioner mot förfalskning och manipulering: — En säkerhetsmönstrad bakgrund med fint guilloche-mönster och iristryck. — Minst en tvåfärgad mikrotextrad.	
		[Märkningar] Bilaga 1C, kapitel 4.1 Synliga uppgifter, 236) Medlemsstaterna får lägga till färger eller märkningar, såsom nationella symboler eller säkerhetsfunktioner.	
		[Typgodkännandemärke] Färdskrivarkort ska innehålla ett typgodkännandemärke. Typgodkännandemärket ska bestå av — en rektangel, inom vilken bokstaven ”e” ska vara inskriven, följd av en siffer- eller bokstavskombination som identifierar det land som har utfärdat typgodkännandet, — ett typgodkännandenummer som motsvarar numret på det typgodkännandeintyg som utfärdats för färdskrivarkortet, placerat i rektangelns omedelbara närhet.	
2.2	Mekaniska prov	[Kortets storlek] Färdskrivarkort ska uppfylla standard ISO/IEC 7810, Identification cards – Physical characteristics, [5] Dimension of card, [5.1] Card size, [5.1.1] Card dimensions and tolererances, card type ID-1 Unused card	240, 243 ISO/IEC 7810
		[Kortets kanter] Färdskrivarkort ska uppfylla standard ISO/IEC 7810, Identification cards – Physical characteristics, [5] Dimension of card, [5.1] Card size, [5.1.2] Card edges	

▼B

Nr	Prov	Beskrivning	Tillämpliga krav
		[Kortets konstruktion] Färdskrivarkort ska uppfylla standard ISO/IEC 7810, Identification cards – Physical characteristics, [6] Card construction	
		[Kortets material] Färdskrivarkort ska uppfylla standard ISO/IEC 7810, Identification cards – Physical characteristics, [7] Card materials	
		[Böjstyvhet] Färdskrivarkort ska uppfylla standard ISO/IEC 7810, Identification cards – Physical characteristics, [8] Card characteristics, [8.1] Bending stiffness	
		[Toxicitet] Färdskrivarkort ska uppfylla standard ISO/IEC 7810, Identification cards – Physical characteristics, [8] Card characteristics, [8.3] Toxicity	
		[Kemisk resistans] Färdskrivarkort ska uppfylla standard ISO/IEC 7810, Identification cards – Physical characteristics, [8] Card characteristics, [8.4] Resistance to chemicals	
		[Kortets stabilitet] Färdskrivarkort ska uppfylla standard ISO/IEC 7810, Identification cards – Physical characteristics, [8] Card characteristics, [8.5] Card dimensional stability and warpage with temperature and humidity	

▼B

Nr	Prov	Beskrivning	Tillämpliga krav
		[Ljus] Färdskrivarkort ska uppfylla standard ISO/IEC 7810, Identification cards – Physical characteristics, [8] Card characteristics, [8.6] Light	
		[Hållbarhet] Bilaga 1C, kapitel 4.4 Miljö- och elspecifikationer, 241) Färdskrivarkorten ska fungera korrekt under en femårsperiod om de används i enlighet med miljö- och elspecifikationerna.	
		Avrivningshållfasthet Färdskrivarkort ska uppfylla standard ISO/IEC 7810, Identification cards – Physical characteristics, [8] Card characteristics, [8.8] Peel strength	
		[Vidhäftning eller blockering] Färdskrivarkort ska uppfylla standard ISO/IEC 7810, Identification cards – Physical characteristics, [8] Card characteristics, [8.9] Adhesion or blocking	
		[Buktighet] Färdskrivarkort ska uppfylla standard ISO/IEC 7810, Identification cards – Physical characteristics, [8] Card characteristics, [8.11] Overall card warpage	
		[Värmebeständighet] Färdskrivarkort ska uppfylla standard ISO/IEC 7810, Identification cards – Physical characteristics, [8] Card characteristics, [8.12] Resistance to heat	

▼B

Nr	Prov	Beskrivning	Tillämpliga krav
		[Ytskevhet] Färdskrivarkort ska uppfylla standard ISO/IEC 7810, Identification cards – Physical characteristics, [8] Card characteristics, [8.13] Surface distortions	
		[Förorening] Färdskrivarkort ska uppfylla standard ISO/IEC 7810, Identification cards – Physical characteristics, [8] Card characteristics, [8.14] Contamination and interaction of card components	
2.3	Mekaniska prov med chipmodul inbyggd	[Böjning] Färdskrivarkort ska uppfylla standard ISO/IEC 7810:2003/Amd. 1:2009, Identification cards – Physical characteristics, Amendment 1: Criteria for cards containing integrated circuits [9.2] Dynamic bending stress Totalt antal böjcykler: 4 000.	ISO/IEC 7810
		[Vridning] Färdskrivarkort ska uppfylla standard ISO/IEC 7810:2003/Amd. 1:2009, Identification cards – Physical characteristics, Amendment 1: Criteria for cards containing integrated circuits [9.3] Dynamic torsional stress Totalt antal vridcykler: 4 000.	
3	**Modul**		
3.1	Modul	Modulen omfattar chippets inkapsling och kontaktplattan. [Ytprofil] Färdskrivarkort ska uppfylla standard ISO/IEC 7816-1:2011, Identification cards – Integrated circuit cards – Part 1: Cards with contacts – Physical characteristics [4.2] Surface profile of contacts	ISO/IEC 7816

▼B

Nr	Prov	Beskrivning	Tillämpliga krav
		[Mekanisk hållfasthet] Färdskrivarkort ska uppfylla standard ISO/IEC 7816-1:2011, Identification cards – Integrated circuit cards – Part 1: Cards with contacts – Physical characteristics [4.3] Mechanical strength (of a card and contacts)	
		[Elektrisk resistans] Färdskrivarkort ska uppfylla standard ISO/IEC 7816-1:2011, Identification cards – Integrated circuit cards – Part 1: Cards with contacts – Physical characteristics [4.4] Electrical resistance (of contacts)	
		[Dimensioner] Färdskrivarkort ska uppfylla standard ISO/IEC 7816-2:2007, Identification cards – Integrated circuit cards – Part 2: Cards with contacts – Dimension and location of the contacts [3] Dimension of the contacts	
		[Placering] Färdskrivarkort ska uppfylla standard ISO/IEC 7816-2:2007, Identification cards – Integrated circuit cards – Part 2: Cards with contacts – Dimension and location of the contacts [4] Number and location of the contacts För moduler med sex kontakter krävs inte detta prov för kontakterna C4 och C8.	
4	**Chip**		
4.1	Chip	[Drifttemperatur] Färdskrivarkortets chip ska fungera i omgivningstemperaturer mellan – 25 °C och + 85 °C.	241–244 ECE R10 ISO/IEC 7810 ISO/IEC 10373

▼B

Nr	Prov	Beskrivning	Tillämpliga krav
		[Temperatur och luftfuktighet] Bilaga 1C, kapitel 4.4 Miljö- och elspecifikationer, 241) Färdskrivarkorten ska fungera korrekt under alla klimatförhållanden som vanligtvis förekommer inom gemenskapens territorium och vid temperaturer mellan – 25 °C och + 70 °C, med tillfälliga toppar på upp till + 85 °C, varvid ”tillfälliga” innebär högst fyra timmar per gång och högst 100 gånger under kortets livstid. Färdskrivarkorten exponeras för följande temperaturer och luftfuktigheter under följande tidsperioder, steg för steg. Efter varje steg provas färdskrivarkortens elektriska funktionalitet. 1. Temperatur + 20 °C, 2 timmar. 2. Temperatur +/– 0 °C, 2 timmar. 3. Temperatur + 20 °C, 50 % RH, 2 timmar. 4. Temperatur + 50 °C, 50 % RH, 2 timmar. 5. Temperatur + 70 °C, 50 % RH, 2 timmar. Temperaturen höjs periodvis till + 85 °C, 50 % RH, under 60 minuter. 6. Temperatur + 70 °C, 85 % RH, 2 timmar. Temperaturen höjs periodvis till + 85 °C, 85 % RH, under 30 minuter.	
		[Luftfuktighet] Bilaga 1C, kapitel 4.4 Miljö- och elspecifikationer, 242) Färdskrivarkort ska fungera korrekt vid en luftfuktighet mellan 10 % och 90 %.	
		[Elektromagnetisk kompatibilitet – EMC] Bilaga 1C, kapitel 4.4 Miljö- och elspecifikationer, 244) Färdskrivarkort ska i drift uppfylla ECE R10 i fråga om elektromagnetisk kompatibilitet.	

▼B

Nr	Prov	Beskrivning	Tillämpliga krav
		[Statisk elektricitet] Bilaga 1C, kapitel 4.4 Miljö- och elspecifikationer, 244) Färdskrivarkort ska i drift vara skyddade mot elektrostatiska urladdningar. Färdskrivarkort ska uppfylla standard ISO/IEC 7810:2003/Amd. 1:2009, Identification cards – Physical characteristics, Amendment 1: Criteria for cards containing integrated circuits [9.4] Static electricity [9.4.1] Contact IC cards Provspänning: 4 000 V.	
		[Röntgenstrålning] Färdskrivarkort ska uppfylla standard ISO/IEC 7810:2003/Amd. 1:2009, Identification cards – Physical characteristics, Amendment 1: Criteria for cards containing integrated circuits [9.1] X-rays	
		[Ultraviolett ljus] ISO/IEC 10373-1:2006, Identification cards – Integrated circuit cards – Part 1: General characteristics [5.11] Ultraviolet light	
		[Trehjulsprov] Färdskrivarkort ska uppfylla standard ISO/IEC 10373-1:2006/Amd. 1:2012, Identification cards – Test methods – Part 1: General characteristics, Amendment 1 [5.22] ICC – Mechanical strength: 3 wheel test for ICCs with contacts	
		[Hölje] Färdskrivarkort ska uppfylla standard MasterCard CQM V2.03:2013 [11.1.3] R-L3-14-8: Wrapping Test Robustness [13.2.1.32] TM-422: Mechanical Reliability: Wrapping Test	

▼B

Nr	Prov	Beskrivning	Tillämpliga krav
4.2	Mekaniska prov av chipmodul inbyggd i det egentliga kortet-> samma som 2.3	[Böjning] Färdskrivarkort ska uppfylla standard ISO/IEC 7810:2003/Amd. 1:2009, Identification cards – Physical characteristics, Amendment 1: Criteria for cards containing integrated circuits [9.2] Dynamic bending stress Totalt antal böjcykler: 4 000. [Vridning] Färdskrivarkort ska uppfylla standard ISO/IEC 7810:2003/Amd. 1:2009, Identification cards – Physical characteristics, Amendment 1: Criteria for cards containing integrated circuits [9.3] Dynamic torsional stress Totalt antal vridcykler: 4 000.	ISO/IEC 7810
5	**Protokollprov**		
5.1	ATR	Kontrollera att ATR uppfyller bestämmelserna.	ISO/IEC 7816-3 TCS_14, TCS_17, TCS_18
5.2	T=0	Kontrollera att protokollet T=0 uppfyller bestämmelserna.	ISO/IEC 7816-3 TCS_11, TCS_12, TCS_13, TCS_15
5.3	PTS	Kontrollera att PTS-kommandot uppfyller bestämmelserna genom att ändra till T=1 från T=0.	ISO/IEC 7816-3 TCS_12, TCS_19, TCS_20, TCS_21
5.4	T=1	Kontrollera att protokollet T=1 uppfyller bestämmelserna.	ISO/IEC 7816-3 TCS_11, TCS_13, TCS_16
6	**Kortets struktur**		
6.1		Prova att filstrukturen på kortet uppfyller bestämmelserna genom att kontrollera förekomsten av obligatoriska filer på kortet och deras tillträdesvillkor.	TCS_22–TCS_28 TCS_140–TCS_179
7	**Funktionsprov**		
7.1	Normal behandling	Prova varje tillåten användning av varje kommando åtminstone en gång (prova t.ex. kommandot UPDATE BINARY med CLA = ‘00’, CLA = ‘0C’ och med olika P1-, P2- och Lc-parametrar). Kontrollera att operationerna verkligen har utförts på kortet (exempelvis genom att avläsa den fil som kommandot har utförts på).	TCS_29–TCS_139

▼B

Nr	Prov	Beskrivning	Tillämpliga krav
7.2	Felmeddelanden	Prova varje felmeddelande åtminstone en gång (såsom anges i tillägg 2) för varje kommando. Prova varje generiskt fel (utom integritetsfel ‘**6400**’ som kontrollerats vid säkerhetscertifiering) åtminstone en gång.	
7.3	Chiffersvit och standardiserade domänparametrar		CSM_48, CSM_50
8	**Användaranpassning**		
8.1	Optisk användar-anpassning	Bilaga 1C, kapitel 4.1 Synliga uppgifter, 230) Framsidan ska innehålla följande: De uppgifter som är särskiljande för det utfärdade kortet. Bilaga 1C, kapitel 4.1 Synliga uppgifter, 231) Framsidan ska innehålla följande: Datum i formatet ”dd/mm/yyyy” eller ”dd.mm.yyyy” (dag, månad, år). Bilaga 1C, kapitel 4.1 Synliga uppgifter, 235) Färdskrivarkorten ska åtminstone ha följande skyddsfunktioner mot förfalskning och manipulering: — I fältet där fotografiet sitter ska den säkerhetsmönstrade bakgrunden och fotografiet överlappa varandra.	230, 231, 235

5. PROVNING AV EXTERN GNSS-ANORDNING

Nr	Prov	Beskrivning	Tillämpliga krav
1	**Administrativ provning**		
1.1	Dokumentation	Dokumentationens korrekthet	
2	**Okulär besiktning av extern GNSS-anordning**		
2.1	Överensstämmelse med dokumentation		
2.2	Identifiering/märkningar		224–226
2.3	Material		219–223
3	**Funktionsprov**		
3.1	Sensorns identifieringsdata		98,99
3.2	Koppling mellan extern GNSS-anordning och fordonsenhet		123, 205

▼B

Nr	Prov	Beskrivning	Tillämpliga krav
3.3	GNSS-position		36, 37
3.4	Gränssnitt med fordonsenheten när GNSS-mottagaren finns utanför fordonsenheten		03
3.5	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 (*dwell time*) 1 timme vid varje temperatur) En minskad uppsättning av 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 x 12 timmar (12 timmar per axel). I ISO 16750-3 krävs inget prov med sinusformade vibrationer för anordningar som är placerade i en fjädrad *(decoupled)* fordonshytt.	219

▼B

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 m/s^2, effektivvärde i längdled 11,8 m/s^2, effektivvärde i sidled 13,1 m/s^2, 3 axlar, 32 timmar per axel, inklusive temperaturcykel mellan – 20 °C och + 70 °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)	220, 221
4.5	Skydd mot överspänning	Kontrollera att fordonsenheten tål strömtillförsel enligt följande: 24 V-versioner: 34 V vid +40 °C, 1 timme 12 V-versioner: 17 V vid +40 °C, 1 timme (ISO 16750-2, kapitel 4.3)	216
4.6	Skydd mot omkastade poler	Kontrollera att fordonsenheten tål en omkastning av strömtillförseln. (ISO 16750-2, kapitel 4.7)	216
4.7	Skydd mot kortslutning	Kontrollera att in- och utsignaler är skyddade mot kortslutning i strömtillförsel och jord. (ISO 16750-2, kapitel 4.10)	216
5	**EMC-prov**		
5.1	Utstrålning och känslighet	Överensstämmelse med förordning ECE R10	218

▼B

Nr	Prov	Beskrivning	Tillämpliga krav
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
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: Vs = – 450 V, Ri = 50 Ohm puls 2a: Vs = +37 V, Ri = 2 Ohm puls 2b: Vs = +20 V, Ri = 0,05 Ohm puls 3a: Vs = – 150 V, Ri = 50 Ohm puls 3b: Vs = +150 V, Ri = 50 Ohm puls 4: Vs = – 16 V, Va = – 12 V, t6 = 100 ms puls 5: Vs = +120 V, Ri = 2,2 Ohm, td = 250 ms För 12 V-versioner: överensstämmelse med ISO 7637-1 + ECE förordning nr 10 Rev. 3: puls 1: Vs = – 75 V, Ri = 10 Ohm puls 2a: Vs = +37 V, Ri = 2 Ohm puls 2b: Vs = +10 V, Ri = 0,05 Ohm puls 3a: Vs = – 112 V, Ri = 50 Ohm puls 3b: Vs = +75 V, Ri = 50 Ohm puls 4: Vs = – 6 V, Va = – 5 V, t6 = 15 ms puls 5: Vs = +65 V, Ri = 3 Ohm, td = 100 ms Puls 5 ska endast provas för de fordonsenheter som är avsedda att installeras i fordon för vilka inget externt gemensamt skydd mot laddningsdump (*load dump*) används. För förslag till laddningsdump, se ISO 16750-2, 4:e utgåvan, kapitel 4.6.4.	218

6. PROVNING AV KOMMUNIKATIONSANORDNING FÖR FJÄRRAVLÄSNING

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
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	213

▼B

Nr	Prov	Beskrivning	Tillämpliga krav
		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 (*dwell time*) 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.	
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 (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
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: Vs = – 450 V, Ri = 50 Ohm puls 2a: Vs = + 37 V, Ri = 2 Ohm puls 2b: Vs = + 20 V, Ri = 0,05 Ohm puls 3a: Vs = – 150 V, Ri = 50 Ohm puls 3b: Vs = + 150 V, Ri = 50 Ohm puls 4: Vs = – 16 V, Va = – 12 V, t6 = 100 ms puls 5: Vs = + 120 V, Ri = 2,2 Ohm, td = 250 ms För 12 V-versioner: överensstämmelse med ISO 7637-1 + ECE förordning nr 10 Rev. 3: puls 1: Vs = – 75 V, Ri = 10 Ohm puls 2a: Vs = + 37 V, Ri = 2 Ohm puls 2b: Vs = + 10 V, Ri = 0,05 Ohm puls 3a: Vs = – 112 V, Ri = 50 Ohm puls 3b: Vs = + 75 V, Ri = 50 Ohm puls 4: Vs = – 6 V, Va = – 5 V, t6 = 15 ms puls 5: Vs = +65 V, Ri = 3 Ohm, td = 100 ms Puls 5 ska endast provas för de fordonsenheter som är avsedda att installeras i fordon för vilka inget externt gemensamt skydd mot laddningsdump (*load dump*) används. För förslag till laddningsdump, se ISO 16750-2, 4:e utgåvan, kapitel 4.6.4.	218

▼B

7. FUNKTIONSPROVNING AV PAPPER

Nr	Prov	Beskrivning	Tillämpliga krav
1	**Administrativ provning**		
1.1	Dokumentation	Dokumentationens korrekthet	
2	**Allmänna prov**		
2.1	Antal tecken per rad	Okulär besiktning av utskrifter.	172
2.2	Minsta teckenstorlek	Okulär besiktning av utskrifter och besiktning av tecken.	173
2.3	Stöd för teckenmängd	Skrivaren ska stödja de tecken som anges i kapitel 4 ”Teckenmängder” i tillägg 1.	174
2.4	Utskrifternas skärpa	Kontroll av färdskrivarens typgodkännande och okulär besiktning av utskrifter.	174
2.5	Läsbarhet och identifiering av utskrifter	Besiktning av utskrifter. Bevisning genom tillverkarens provrapporter och provprotokoll. Typgodkännandenummer är tryckta på papperet för alla färdskrivare i vilka papperet får användas.	175, 177, 178
2.6	Tillägg av handskrivna anmärkningar	Okulär besiktning: Tillgång till fält för förarens namnteckning. Tillgång till andra fält för ytterligare handskriven text.	180
2.7	Ytterligare uppgifter på papperets sidor	Papperets fram- och baksida får innehålla ytterligare uppgifter och information. Ytterligare uppgifter och information får inte störa utskrifternas läsbarhet. Okulär besiktning.	177, 178
3	**Förvaringsprov**		
3.1	Torr värme	Förkonditionering: 16 timmar vid +23 °C ± 2 °C/55 % ± 3 % relativ luftfuktighet Provmiljö: 72 timmar vid +70 °C ± 2°C Återställning: 16 timmar vid +23 °C ± 2 °C/55 % ± 3 % relativ luftfuktighet	176, 178 IEC 60068-2-2-Bb
2.2	Fuktig värme	Förkonditionering: 16 timmar vid +23 °C ±2 °C/55 % ±3 % relativ luftfuktighet Provmiljö: 144 timmar vid +55 °C ±2 °C/93 % ±3 % relativ luftfuktighet Återställning: 16 timmar vid + 23 °C ± 2 °C/55 % ± 3 % relativ luftfuktighet	176, 178 IEC 60068-2-78-Cab

▼B

Nr	Prov	Beskrivning	Tillämpliga krav
4	**Driftprov av papper**		
4.1	Beständighet mot bakgrundsfuktighet (papper före utskrift)	Förkonditionering: 16 timmar vid + 23 °C ± 2 °C/55 % ± 3 % relativ luftfuktighet Provmiljö: 144 timmar vid +55 °C ± 2 °C/93 % ± 3 % relativ luftfuktighet Återställning: 16 timmar vid +23 °C ± 2 °C/55 % ± 3 % relativ luftfuktighet	176, 178 IEC 60068-2-78-Cab
4.2	Skrivbarhetsegenskaper	Förkonditionering: 24 timmar vid + 40 °C ± 2 °C/93 % ± 3 % relativ luftfuktighet Provmiljö: utskrift gjord vid + 23 °C ± 2 °C Återställning: 16 timmar vid + 23 °C ± 2 °C/55 % ±3 % relativ luftfuktighet	176, 178
4.3	Värmebeständighet	Förkonditionering: 16 timmar vid + 23 °C ± 2 °C/55 % ± 3 % relativ luftfuktighet Provmiljö: 2 timmar vid + 70 °C ± 2 °C, torr värme Återställning: 16 timmar vid +23 °C ± 2 °C/55 % ± 3 % relativ luftfuktighet	176, 178 IEC 60068-2-2-Bb
4.4	Lågtemperaturbeständighet	Förkonditionering: 16 timmar vid + 23 °C ± 2 °C/55 % ± 3 % relativ luftfuktighet Provmiljö: 24 timmar vid – 20 °C ± 3 °C, torr kyla Återställning: 16 timmar vid +23 °C ± 2 °C/55 % ± 3 % relativ luftfuktighet	176, 178 ISO 60068-2-1-Ab
4.5	Ljusbeständighet	Förkonditionering: 16 timmar vid + 23 °C ± 2 °C/55 % ± 3 % relativ luftfuktighet; provmiljö: 100 timmar med 5 000 Lux belysning vid + 23 °C ± 2 °C/55 % ± 3 % relativ luftfuktighet Återställning: 16 timmar vid +23 °C ± 2 °C/55 % ±3 % relativ luftfuktighet	176, 178

Läsbarhetskriterier för prov 3.x och 4.x:

Utskriftens läsbarhet är godkänd om den optiska densiteten överensstämmer med följande gränsvärden:

Utskrivna tecken: min. 1,0

Bakgrund (papper före utskrift): max. 0,2

Optisk densitet av de faktiska utskrifterna ska mätas i enlighet med DIN EN ISO 534.

Utskrifterna ska inte förevisa några ändringar i dimension och ska kvarstå som tydligt läsbara.

8. PROVNING AV DRIFTSKOMPATIBILITET

Nr	Prov	Beskrivning
9.1 Prov av driftskompatibilitet mellan fordonsenheter och färdskrivarkort		
1	Ömsesidig autentisering	Kontrollera att den ömsesidiga autentiseringen mellan fordonsenheten och färdskrivarkortet fungerar normalt.

▼B

Nr	Prov	Beskrivning
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.
9.2 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.
9.3 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.

▼B

Tillägg 10

SÄKERHETSKRAV

I detta tillägg specificeras kraven i fråga om IT-säkerhet för komponenterna i smarta färdskrivarsystem (andra generationens färdskrivare).

SEC_001 Följande komponenter i smarta färdskrivarsystem ska vara säkerhetscertifierade i enlighet med CC-systemet (*Common Criteria*):

— Fordonsenhet.

— Färdskrivarkort.

— Rörelsesensor.

— Extern GNSS-anordning.

SEC_002 De minimikrav i fråga om IT-säkerhet som ska uppfyllas av varje komponent som behöver säkerhetscertifiering ska definieras i en skyddsprofil för respektive komponent i enlighet med CC-systemet.

SEC_003 Europeiska kommissionen ska säkerställa att följande fyra skyddsprofiler som överensstämmer med denna bilaga finansieras, utarbetas och godkänns av den gemensamma arbetsgruppen (JIWG, *Joint Interpretation Working Group*) som arbetar för ömsesidigt erkännande av certifikat inom den europeiska gruppen av höga tjänstemän på informationssäkerhetsområdet (SOGIS-MRA, *Agreement on Mutual Recognition of Information Technology Security Evaluation Certificates*), och att dessa registreras:

— En skyddsprofil för fordonsenheter.

— En skyddsprofil för färdskrivarkort.

— En skyddsprofil för rörelsesensorer.

— En skyddsprofil för externa GNSS-anordningar.

Fordonsenhetens skyddsprofil ska omfatta båda de fall där fordonsenheten är utformad för användning med respektive utan en extern GNSS-anordning. I det förra fallet ska säkerhetskraven för den externa GNSS-anordningen finnas i dess egen skyddsprofil.

SEC_004 Komponenttillverkare ska efter behov förfina och slutföra en lämplig skyddsprofil för komponenten, utan att ändra eller ta bort befintliga hot, mål, förfaranden eller specifikationer av säkerhetsfunktioner, för att utforma ett säkerhetsmål gentemot vilket de ska ansöka om säkerhetscertifiering för komponenten.

SEC_005 Under utvärderingsprocessen måste man uppge att motsvarande skyddsprofil strikt uppfyller ett sådant specifikt säkerhetsmål.

SEC_006 Assuransnivån för varje skyddsprofil ska vara EAL4, förbättrad med assuranskomponenterna ATE_DPT.2 och AVA_VAN.5.

▼B

Tillägg 11

GEMENSAMMA SÄKERHETSMEKANISMER

INNEHÅLLSFÖRTECKNING

INLEDNING

DEL A FÖRSTA GENERATIONENS FÄRDSKRIVARSYSTEM

1. INLEDNING

1.1. Referenser

1.2. Beteckningar och förkortningar

2. KRYPTOSYSTEM OCH ALGORITMER

2.1. Kryptosystem

2.2. Kryptografiska algoritmer

2.2.1 RSA-algoritm

2.2.2 Hashalgoritm

2.2.3 Datakrypteringsalgoritm

3. NYCKLAR OCH CERTIFIKAT

3.1. Generering och distribuering av nycklar

3.1.1 Generering och distribuering av RSA-nycklar

3.1.2 RSA-nycklar för provning

3.1.3 Nycklar för rörelsesensorer

3.1.4 Generering och distribuering av sessionsnycklar för T-DES

3.2. Nycklar

3.3. Certifikat

3.3.1 Certifikatens innehåll

3.3.2 Utfärdade certifikat

3.3.3 Verifiering och uppackning av certifikat

4. ÖMSESIDIG AUTENTISERINGSMEKANISM

5. MEKANISMER FÖR SEKRETESS, INTEGRITET OCH AUTENTISERING VID ÖVERFÖRING AV DATA MELLAN FORDONSENHET OCH KORT

5.1. Säker meddelandehantering

5.2. Felhantering avseende säker meddelandehantering

5.3. Algoritm för beräkning av kryptografiska kontrollsummor

5.4. Algoritm för att beräkna kryptogram för sekretessdataobjekt

6. MEKANISMER FÖR DIGITAL SIGNATUR VID DATAÖVERFÖRING

6.1. Generering av signatur

▼B

6.2.	Verifiering av signatur
DEL B	ANDRA GENERATIONENS FÄRDSKRIVARSYSTEM
7.	INLEDNING
7.1.	Referenser
7.2.	Beteckningar och förkortningar
7.3.	Definitioner
8.	KRYPTOSYSTEM OCH ALGORITMER
8.1.	Kryptosystem
8.2.	Kryptografiska algoritmer
8.2.1	Symmetriska algoritmer
8.2.2	Asymmetriska algoritmer och standardiserade domänparametrar
8.2.3	Hashalgoritmer
8.2.4	Chifferföljder
9.	NYCKLAR OCH CERTIFIKAT
9.1.	Asymmetriska nyckelpar och certifikat för öppna nycklar
9.1.1	Allmänt
9.1.2	Europeisk nivå
9.1.3	Medlemsstatsnivå
9.1.4	Utrustningsnivå: Fordonsenheter
9.1.5	Utrustningsnivå: färdskrivarkort
9.1.6	Utrustningsnivå: externa GNSS-anordningar
9.1.7	Översikt: Ersättning av certifikat
9.2.	Symmetriska nycklar
9.2.1	Nycklar för att säkra kommunikation mellan fordonsenhet och rörelsesensor
9.2.2	Nycklar för att säkra DSRC-kommunikation
9.3.	Certifikat
9.3.1	Allmänt
9.3.2	Certifikatens innehåll
9.3.3	Förfrågan om certifikat
10.	ÖMSESIDIG AUTENTISERING OCH SÄKER MEDDELANDEHANTERING MELLAN FORDONSENHET OCH KORT
10.1.	Allmänt
10.2.	Ömsesidig verifiering av certifikatskedja
10.2.1	Fordonsenhetens verifiering av kortets certifikatskedja

▼B

10.2.2 Kortets verifiering av fordonsenhetens certifikatskedja

10.3. Autentisering av fordonsenhet

10.4. Autentisering av chip och överenskommelse om sessionsnyckel

10.5. Säker meddelandehantering

10.5.1 Allmänt

10.5.2 Säker meddelandestruktur

10.5.3 Avbryta en session med säker meddelandehantering

11. KOPPLING, ÖMSESIDIG AUTENTISERING OCH SÄKER MEDDELANDEHANTERING MELLAN FORDONSENHETER OCH EXTERNA GNSS-ANORDNINGAR

11.1. Allmänt

11.2. Koppling mellan fordonsenhet och extern GNSS-anordning

11.3. Ömsesidig verifiering av certifikatskedja

11.3.1 Allmänt

11.3.2 Vid koppling av fordonsenhet och extern GNSS-anordning

11.3.3 Under normal drift

11.4. Autentisering av fordonsenhet, autentisering av chip och överenskommelse om sessionsnyckel

11.5. Säker meddelandehantering

12. PARNING AV OCH KOMMUNIKATION MELLAN FORDONSENHET OCH RÖRELSESENSOR

12.1. Allmänt

12.2. Parning av fordonsenhet och rörelsesensor med användning av olika nyckelgenerationer

12.3. Parning av och kommunikation mellan fordonsenhet och rörelsesensor med användning av AES

12.4. Parning av fordonsenhet och rörelsesensor för olika utrustningsgenerationer

13. SÄKERHET FÖR FJÄRRKOMMUNIKATION VIA DSRC

13.1. Allmänt

13.2. Kryptering av nyttolast från färdskrivaren och MAC-generering

13.3. Verifiering och dekryptering av nyttolast från färdskrivaren

14. SIGNERING AV DATAÖVERFÖRINGAR OCH VERIFIERING AV SIGNATURER

14.1. Allmänt

14.2. Generering av signatur

14.3. Verifiering av signatur

▼B

INLEDNING

I detta tillägg specificeras de säkerhetsmekanismer som ska säkerställa följande:

— Ömsesidig autentisering mellan olika komponenter i färdskrivarsystemet.

— Sekretess, integritet, autenticitet och/eller oavvislighet avseende data som överförs mellan olika komponenter i färdskrivarsystemet eller till externa lagringsmedier.

Detta tillägg består av två delar. I del A definieras säkerhetsmekanismerna för första generationens färdskrivarsystem (digital färdskrivare). I del B definieras säkerhetsmekanismerna för andra generationens färdskrivarsystem (smart färdskrivare).

De mekanismer som specificeras i del A i detta tillägg ska tillämpas om minst en av de komponenter i färdskrivarsystemet som deltar i en ömsesidig autentisering och/eller en dataöverföring tillhör första generationen.

De mekanismer som specificeras i del B ska tillämpas om båda de komponenter i färdskrivarsystemet som deltar i den ömsesidiga autentiseringen och/eller dataöverföringen tillhör andra generationen.

I tillägg 15 finns mer information om användning av första generationens komponenter tillsammans med andra generationens komponenter.

DEL A

FÖRSTA GENERATIONENS FÄRDSKRIVARSYSTEM

1. INLEDNING

1.1. **Referenser**

Följande referenser används i detta tillägg:

SHA-1	National Institute of Standards and Technology (NIST). *FIPS Publication 180-1: Secure Hash Standard*. April 1995.
PKCS1	RSA Laboratories. PKCS # 1: *RSA Encryption Standard*. Version 2.0. October 1998.
TDES	National Institute of Standards and Technology (NIST). *FIPS Publication 46-3: Data Encryption Standard*. Draft 1999.
TDES-OP	ANSI X9.52, Triple Data Encryption Algorithm Modes of Operation. 1998.
ISO/IEC 7816-4	Information Technology – Identification cards – Integrated circuit(s) cards with contacts – Part 4: Interindustry commands for interexchange. First edition: 1995 + Amendment 1: 1997.
ISO/IEC 7816-6	Information Technology – Identification cards – Integrated circuit(s) cards with contacts – Part 6: Interindustry data elements. First edition: 1996 + Cor 1: 1998.
ISO/IEC 7816-8	Information Technology – Identification cards – Integrated circuit(s) cards with contacts – Part 8: Security related interindustry commands. First edition 1999.
ISO/IEC 9796-2	Information Technology – Security techniques – Digital signature schemes giving message recovery – Part 2: Mechanisms using a hash function. First edition: 1997.

▼B

ISO/IEC 9798-3	Information Technology – Security techniques – Entity authentication mechanisms – Part 3: Entity authentication using a public key algorithm. Second edition 1998.
ISO 16844-3	Road vehicles – Tachograph systems – Part 3: Motion sensor interface.

1.2. **Beteckningar och förkortningar**

Följande beteckningar och förkortningar används i detta tillägg:

(K_a, K_b, K_c)	en kombination av nycklar som används i krypteringsalgoritmen TDEA.
CA	*Certification Authority* (certifieringsinstans).
CAR	*Certification Authority Reference* (certifieringsinstansens referens).
CC	*Cryptographic Checksum* (kryptografisk kontrollsumma).
CG	*Cryptogram* (kryptogram).
CH	*Command Header* (startdel för kommando).
CHA	*Certificate Holder Authorisation* (certifikatinnehavarens auktorisering).
CHR	*Certificate Holder Reference* (certifikatinnehavarens referens).
D()	Dekryptering med DES.
DE	*Data Element* (dataelement).
DO	*Data Object* (dataobjekt).
d	Privat RSA-nyckel, privat exponent.
e	Öppen RSA-nyckel, öppen exponent.
E()	*Encryption with DES* (kryptering med DES).
EQT	*Equipment* (utrustning).
Hash()	Hashvärde, utdata från hashning.
Hash	Hashning, hashfunktion.
KID	*Key Identifier* (nyckelidentifierare).
Km	TDES-nyckel. Huvudnyckel enligt definitionen i ISO 16844-3.
Km_{VU}	TDES-nyckel i fordonsenheter.
Km_{WC}	TDES-nyckel i verkstadskort.
m	Löpnummer för meddelande, heltal mellan 0 och $n - 1$.
n	Modulus för RSA-nycklar.
PB	*Padding Bytes* (byte för utfyllnad).
PI	*Padding Indicator* (byte för indikering av utfyllnad, för användning i kryptogram för sekretessdataobjekt).
PV	*Plain Value* (klarvärde, värde i klartext).
s	Löpnummer för signatur, heltal mellan 0 och $n - 1$.
SSC	*Send Sequence Counter* (räknare för sekvenssändning).
SM	*Secure Messaging* (säker meddelandehantering).
TCBC	*TDEA Cipher Block Chaining* (användningssätt för TDEA).

▼B

TDEA	*Triple Data Encryption Algorithm* (krypteringsalgoritm).
TLV	*Tag Length Value* (tagglängd).
VU	*Vehicle Unit* (fordonsenhet).
X.C	Certifikat för användare X, utfärdat av en certifieringsinstans.
X.CA	Certifieringsinstans för användare X.
X.CA.PK $_{o}$ X.C	Uppackning av ett certifikat för att extrahera en öppen nyckel. Det är en infixoperator, vars vänstra operand är en certifieringsinstans öppna nyckel och vars högra operand är det certifikat som utfärdats av denna certifieringsinstans. Resultatet är den öppna nyckeln hos användare X, vars certifikat är den högra operanden.
X.PK	Öppen RSA-nyckel för användare X.
X.PK[I]	RSA-kryptering av viss information I, med användning av användare X öppna nyckel.
X.SK	Privat RSA-nyckel för användare X.
X.SK[I]	RSA-kryptering av viss information I, med användning av användare X privata nyckel.
‘xx’	Hexadecimalt värde.
||	Konkateneringsoperator.

2. KRYPTOSYSTEM OCH ALGORITMER

2.1. **Kryptosystem**

CSM_001 Fordonsenheter och färdskrivarkort ska använda ett klassiskt RSA-kryptosystem med öppna nycklar för att tillhandahålla följande säkerhetsmekanismer:

— Autentisering mellan fordonsenheter och kort.

— Transport av Triple DES-sessionsnycklar mellan fordonsenheter och färdskrivarkort.

— Digital signatur för data som överförs från fordonsenheter eller färdskrivarkort till externa media.

CSM_002 Fordonsenheter och färdskrivarkort ska använda ett symmetriskt Triple DES-kryptosystem för att tillhandahålla en mekanism för dataintegritet vid datautbyte mellan fordonsenheter och färdskrivarkort, och för att i förekommande fall tillhandahålla sekretessbelagt datautbyte mellan fordonsenheter och färdskrivarkort.

2.2. **Kryptografiska algoritmer**

2.2.1 *RSA-algoritm*

CSM_003 RSA-algoritmen definieras fullständigt genom följande förhållanden:

▼B

$$X.SK[m] = s = m^d \bmod n$$

$$X.PK[s] = m = s^e \bmod n$$

En utförligare beskrivning av RSA-funktionen finns i referens [PKCS1]. Den öppna exponenten, e, för RSA-beräkningar är ett heltal mellan 3 och n-1 som uppfyller gcd(e, lcm(p-1, q-1))=1.

2.2.2 *Hashalgoritm*

CSM_004 Mekanismerna för digital signatur ska använda hashalgoritmen SHA-1, som definieras i referens [SHA-1].

2.2.3 *Datakrypteringsalgoritm*

CSM_005 DES-baserade algoritmer ska användas i CBC-läge (*Cipher Block Chaining*).

3. Nycklar och certifikat

3.1. **Generering och distribuering av nycklar**

3.1.1 *Generering och distribuering av RSA-nycklar*

CSM_006 RSA-nycklar ska genereras med hjälp av följande tre hierarkiska funktionsnivåer:

— Europeisk nivå.

— Medlemsstatsnivå.

— Utrustningsnivå.

CSM_007 På europeisk nivå ska ett enda europeiskt nyckelpar (EUR.SK och EUR.PK) genereras. Den europeiska privata nyckeln ska användas för att certifiera medlemsstaternas öppna nycklar. Ett register ska föras över alla certifierade nycklar. Dessa arbetsuppgifter ska utföras av en europeisk certifieringsinstans, under Europeiska kommissionens överinseende och ansvar.

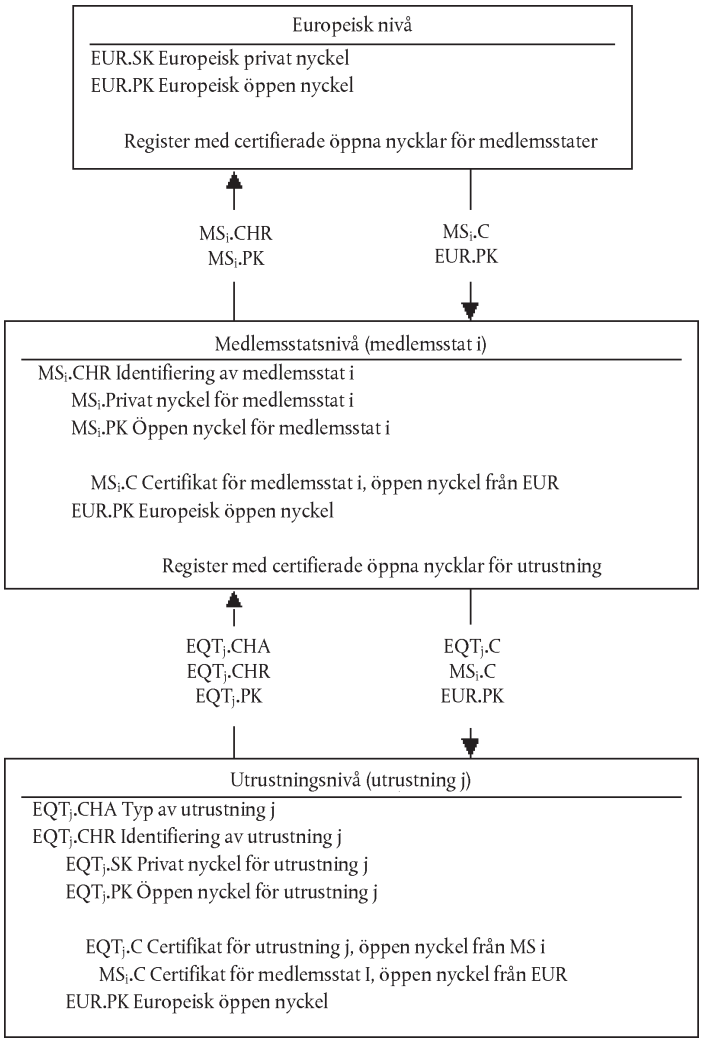
CSM_008 På medlemsstatsnivå ska ett nyckelpar för medlemsstaten (MS.SK och MS.PK) genereras. Medlemsstaternas öppna nycklar ska certifieras av den europeiska certifieringsinstansen. En medlemsstats privata nyckel ska användas för att certifiera de öppna nycklar som ska installeras i utrustningen (fordonsenhet eller färdskrivarkort). Alla certifierade öppna nycklar ska registreras med identifiering av den utrustning som de är avsedda för. Dessa arbetsuppgifter ska utföras av en certifieringsinstans i medlemsstaten. En medlemsstat får regelbundet byta sitt nyckelpar.

CSM_009 På utrustningsnivå ska ett enda nyckelpar (EQT.SK och EQT.PK) genereras och installeras i respektive utrustning. Öppna utrustningsnycklar ska certifieras av en medlemsstats certifieringsinstans. Dessa arbetsuppgifter får utföras av tillverkare av utrustning, användaranpassare (*personalisers*) av utrustning eller medlemsstaternas myndigheter. Detta nyckelpar används för autentisering, digital signering och kryptering.

CSM_010 Sekretessen för privata nycklar ska bibehållas vid generering, eventuell transport och lagring.

▼B

I följande figur sammanfattas dataflödet i denna process:



3.1.2 *RSA-nycklar för provning*

CSM_011 För att prova utrustning (även med avseende på driftskompatibilitet) ska den europeiska certifieringsinstansen generera ett annat särskilt europeiskt nyckelpar för provning och minst två medlemsstatsnyckelpar för provning, vars öppna nycklar ska certifieras med den europeiska privata provningsnyckeln. I utrustning som provas för typgodkännande ska tillverkarna installera provningsnycklar som certifierats av en av dessa medlemsstatsnycklar för provning.

3.1.3 *Nycklar för rörelsesensorer*

Sekretessen för de tre nedannämnda Triple DES-nycklarna ska bibehållas på lämpligt sätt vid generering, eventuell transport och lagring.

Som stöd för färdskrivarkomponenter som uppfyller bestämmelserna i ISO 16844 ska den europeiska certifieringsinstansen och medlemsstatens certifieringsinstanser dessutom säkerställa följande:

CSM_036 Den europeiska certifieringsinstansen ska generera KmVU och KmWC, två oberoende och unika nycklar för Triple DES, och generera Km som $Km = Km_{VU} XOR Km_{WC}$.

Den europeiska certifieringsinstansen ska överlämna dessa nycklar på ett säkert sätt till medlemsstaternas certifieringsinstanser på de senares begäran.

▼B

CSM_037 Medlemsstaternas certifieringsinstanser ska

— använda Km för att kryptera de rörelsesensordata som efterfrågas av rörelsesensortillverkarna (de data som ska krypteras med Km definieras i ISO 16844-3),

— överlämna Km_{VU} till fordonsenhetstillverkarna på ett säkert sätt för installation i fordonsenheterna, och

— säkerställa att Km_{WC} installeras i alla verkstadskort (`SensorInstallationSecData` i EF `Sensor_Installation_Data`) då kortet användaranpassas.

3.1.4 *Generering och distribuering av sessionsnycklar för T-DES*

CSM_012 Fordonsenheter och färdskrivarkort ska som en del av den ömsesidiga autentiseringen generera och utväxla nödvändiga data för att utforma en gemensam sessionsnyckel för Triple DES. Detta utbyte av data ska sekretesskyddas genom en mekanism för RSA-kryptering.

CSM_013 Denna nyckel ska användas för all efterföljande kryptografisk verksamhet där säker meddelandehantering (*secure messaging*) används. Dess giltighet ska gå ut när sessionen avslutas (uttag eller nollställning av kortet) och/eller efter 240 användningar (en användning av nyckeln = ett kommando som med säker meddelandehantering sänds till kortet och åtföljande svar).

3.2. **Nycklar**

CSM_014 RSA-nycklar ska (oavsett nivå) ha följande längder: modulus *n* 1 024 bitar, öppen exponent *e* maximalt 64 bitar, privat exponent *d* 1 024 bitar.

CSM_015 Triple DES-nycklar ska ha formen (K_a, K_b, K_a), där K_a och K_b är oberoende nycklar vars längd är 64 bitar. Inga bitar ska sättas för påvisande av paritetsfel.

3.3. **Certifikat**

CSM_016 Certifikat för öppna RSA-nycklar ska vara icke-självbeskrivande (*non self-descriptive*) och kortverifierbara (*card-verifiable*) certifikat (ref. ISO/IEC 7816-8).

3.3.1 *Certifikatens innehåll*

CSM_017 Certifikat för öppna RSA-nycklar byggs med följande data i följande ordning:

Data	Format	Byte	Anmärkningar
CPI	HELTAL	1	Identifierare för certifikatprofil (*Certificate Profile Identifier*) (‘01’ för denna version).
CAR	OKTETTSTRÄNG	8	Certifieringsinstansens referens (*Certification Authority Reference*).
CHA	OKTETTSTRÄNG	7	Certifikatinnehavarens auktorisering (*Certificate Holder Authorisation*).

▼B

Data	Format	Byte	Anmärkningar
EOV	TimeReal	4	Sista giltighetsdag för certifikatet. Frivillig, utfylls med ′FF′ om dessa data ej används.
CHR	OKTETT-STRÄNG	8	Certifikatinnehavarens referens (*Certificate Holder Reference*).
n	OKTETT-STRÄNG	128	Öppen nyckel (modulus).
e	OKTETT-STRÄNG	8	Öppen nyckel (öppen exponent).
		164	

Anmärkningar:

1. Identifieraren för certifikatprofil (CPI) beskriver autentiseringscertifikatets exakta struktur. Den kan användas av utrustningen som en intern identifierare för en relevant startlista (*headerlist*) som beskriver konkateneringen av dataelement inom certifikatet.

   Startlistan för detta certifikatinnehåll ser ut på följande sätt:

‘4D’	‘16’	‘5F 29’	‘01’	‘42’	‘08’	‘5F 4B’	‘07’	‘5F 24’	‘04’	‘5F 20’	‘08’	‘7F 49’	‘05’	‘81’	‘81 80’	‘82’	‘08’
Tagg för utökad startlista	Startlistans längd	CPI-tagg	CPI-längd	CAR-tagg	CAR-längd	CHA-tagg	CHA-längd	EOV-tagg	EOV-längd	CHR-tagg	CHR-längd	Tagg för öppen nyckel (konstruerad)	Längd för efterföljande dataobjekt	Modulus-tagg	Modulus-längd	Tagg för öppen exponent	Längd för öppen exponent

2. Certifieringsinstansens referens (CAR) har som syfte att identifiera den certifieringsinstans (CA) som utfärdar certifikat på så sätt att dataelementet kan användas samtidigt som en identifierare för instansens nyckel (*Authority Key Identifier*), som referens till certifieringsinstansens öppna nyckel (för kodning, se nyckelidentifierare (*Key Identifier*) nedan).

3. Certifikatinnehavarens auktorisering (CHA) används för att identifiera certifikatinnehavarens rättigheter. Den består av färdskrivarens tillämpningsidentifierare (*Application ID*) och av den typ av utrustning för vilken certifikatet är avsett (enligt dataelementet `EquipmentType`; ‘00’ för en medlemsstat).

▼B

4. Certifieringsinnehavarens referens (CHR) har som syfte att unikt identifiera certifikatinnehavaren (CH) på så sätt att dataelementet kan användas samtidigt som en identifierare för subjektnyckel (*Subject Key Identifier*), som referens till certifikatinnehavarens öppna nyckel.

5. Med nyckelidentifierare identifieras certifikatinnehavare eller certifieringsinstanser unikt. De är kodade på nedanstående sätt.

5.1 Utrustning (fordonsenhet eller kort):

Data	Utrustningens serienummer	Datum	Typ	Tillverkare
Längd	4 byte	2 byte	1 byte	1 byte
Värde	Heltal	mm yy, BCD-kodning	Tillverkarspecifikt	Tillverkarkod

När en tillverkare efterfrågar certifikat för en fordonsenhet är identifieringen av den utrustning i vilken nycklarna kommer att installeras antingen känd eller inte känd.

I det förra fallet kommer tillverkaren att sända utrustningens identifiering med den öppna nyckeln till sin medlemsstats certifieringsinstans. Certifikatet kommer då att innehålla utrustningens identifiering, och tillverkaren måste se till att nycklar och certifikat installeras i avsedd utrustning. Nyckelidentifieraren har den form som visas ovan.

I det senare fallet måste tillverkaren unikt identifiera varje certifikatförfrågan och sända denna identifiering med den öppna nyckeln till sin medlemsstats certifieringsinstans. Certifikatet kommer att innehålla identifiering av förfrågan. Tillverkaren måste meddela sin medlemsstats instans om hur nyckeln tillskrivs en viss utrustning (dvs. identifiering av certifikatförfrågan och identifiering av utrustningen) efter det att nyckeln installerats i utrustningen. Nyckelidentifieraren har följande form:

Data	Serienummer för förfrågan om certifikat	Datum	Typ	Tillverkare
Längd	4 byte	2 byte	1 byte	1 byte
Värde	Heltal	mm yy, BCD-kodning	‘FF’	Tillverkarkod

▼B

5.2 Certifieringsinstans:

Data	Instansens identifiering	Nyckelns serienummer	Övrig information	Identifierare
Längd	4 byte	1 byte	2 byte	1 byte
Värde	Numerisk landskod (1 byte) Alfanumerisk landskod (3 byte)	Heltal	Ytterligare kodning (specifik för certifieringsinstans), ‘FF FF’ om den inte används	‘01’

Nyckelns serienummer används för att särskilja en medlemsstats olika nycklar om nyckeln ändras.

6. Certifikatverifierare ska indirekt känna till att den certifierade öppna nyckeln är en RSA-nyckel som är relevant för autentisering, verifiering av digital signatur och kryptering för sekretesstjänster (certifikatet innehåller ingen objektidentifierare som specificerar den).

3.3.2 *Utfärdade certifikat*

CSM_018 Det utfärdade certifikatet är en digital signatur med delvis återskapande av certifikatinnehåll i enlighet med ISO/IEC 9796-2 (med undantag för dess bilaga A4), med certifieringsinstansens referens (CAR) tillagd.

$$X.C = X.CA.SK[\text{‘6A’} \parallel C_r \parallel \mathit{Hash}(Cc) \parallel \text{‘BC’}] \parallel C_n \parallel X.CAR$$

Med certifikatinnehåll = Cc = C_r || C_n

106 byte 58 byte

Anmärkningar:

1. Detta certifikat är 194 byte långt.
2. CAR, som döljs av signaturen, är också tillagd till signaturen, så att certifieringsinstansens öppna nyckel kan väljas för verifiering av certifikatet.
3. Certifikatverifieraren ska indirekt känna till den algoritm som används av certifieringsinstansen för att signera certifikatet.
4. Startlistan (*header list*) för detta utfärdade certifikat ser ut på följande sätt:

‘7F 21’	‘09’	‘5F 37’	‘81 80’	‘5F 38’	‘3A’	‘42’	‘08’
Tagg för certifikatets konstanta vektor (CV, Constant Vector; konstruerad)	Längd för efterföljande dataobjekt	Tagg för signatur	Längd för signatur	Tagg för återstod	Längd för återstod	CAR-tagg	CAR-längd

▼B

3.3.3 *Verifiering och uppackning av certifikat*

Verifiering och uppackning består i att signaturen verifieras i enlighet med ISO/IEC 9796-2, att certifikatinnehållet hämtas, inklusive den ingående öppna nyckeln X.PK = X.CA.PKo X.C, och att certifikatets giltighet verifieras.

CSM_019 Detta inbegriper följande steg:

Verifiera signatur och hämta innehåll:

— Hämta Sign, C_n 'and CAR' från X.C: X.C = Sign || C_n' || CAR'

128 byte 58 byte 8 byte

— Välj lämplig öppen nyckel för certifieringsinstansen med hjälp av CAR' (såvida detta inte redan är gjort på annat sätt).

— Öppna Sign med certifieringsinstansens öppna nyckel: Sr'= X.CA.PK [Sign],

— Kontrollera att Sr' börjar med '6A' och slutar med 'BC'.

— Beräkna C_r' och H′ med hjälp av Sr' = '6A' || C_r' || H' || 'BC'

106 byte 20 byte

— Återskapa certfikatinnehåll C' = C_r' || C_n'.

— Kontrollera *Hash*(C′) = H′.

Om kontrollerna är OK är certifikatet äkta och dess innehåll är C′.

Verifiera giltighet. Från C′:

— Kontrollera, i förekommande fall, sista giltighetsdag.

Hämta och lagra öppen nyckel, nyckelidentifierare, certifikatinnehavarens auktorisering (CHA) och certifikatets sista giltighetsdag från C′:

— X.PK = *n* || *e*

— X.KID = CHR

— X.CHA = CHA

— X.EOV = EOV

4. ÖMSESIDIG AUTENTISERINGSMEKANISM

Ömsesidig autentisering mellan kort och fordonsenheter bygger på följande princip:

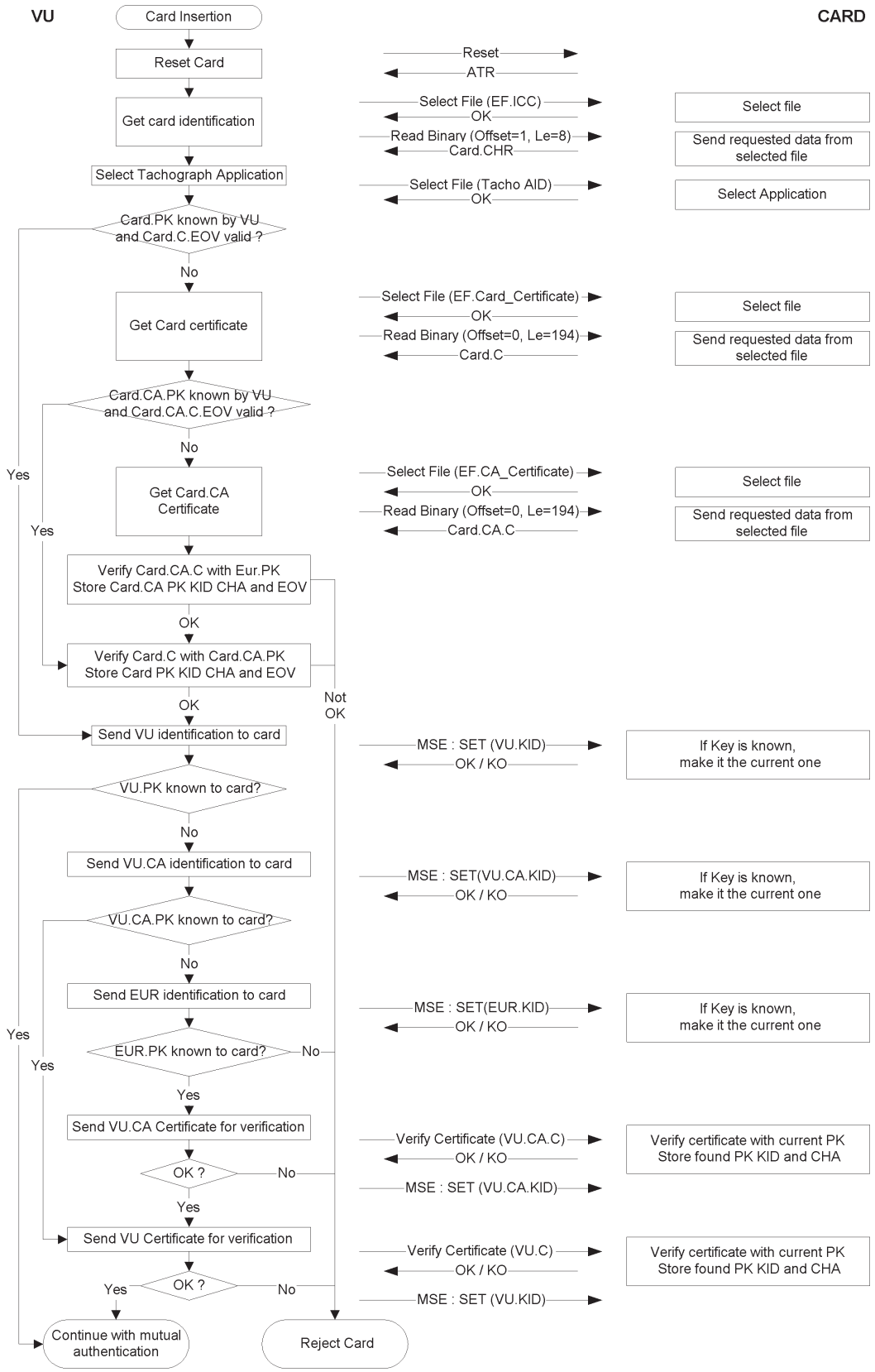
Varje part ska demonstrera för den andra att den äger ett giltigt nyckelpar, vars öppna nyckel har certifierats av en certifieringsinstans i en medlemsstat, som i sin tur har certifierats av den europeiska certifieringsinstansen.

Detta görs genom att man med den privata nyckeln signerar ett slumptal som sänts av den andra parten, som måste återskapa det sända slumptalet när signaturen verifieras.

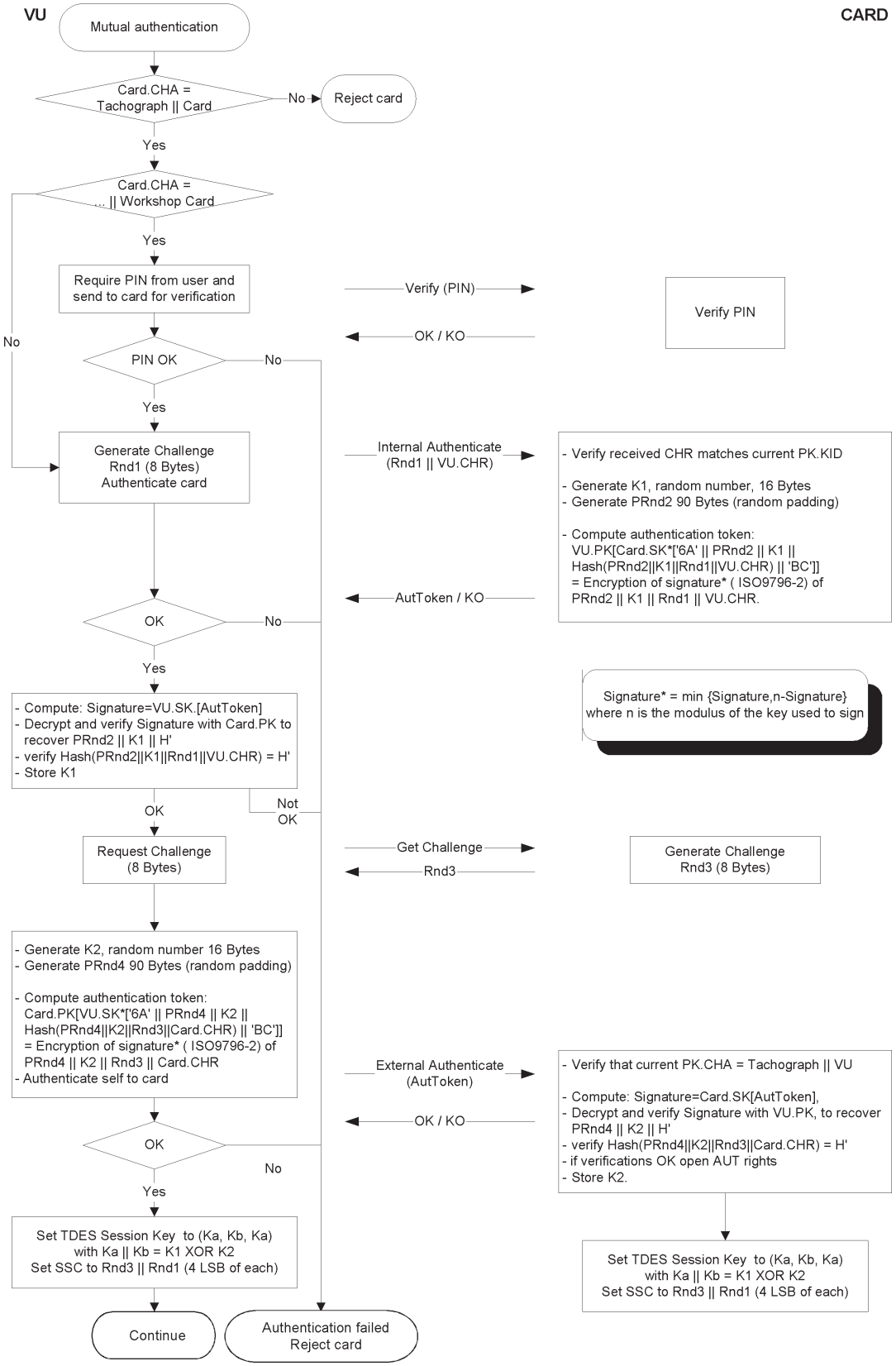
Mekanismen utlöses av fordonsenheten när ett kort sätts in. Den börjar med utbyte av certifikat och uppackning av öppna nycklar och slutar med fastställande av en sessionsnyckel.

▼B

CSM_020 Följande protokoll ska användas (pilar anger kommandon och data som utväxlas (se tillägg 2)):



▼B


VU
CARD
Mutual authentication
Card.CHA = Tachograph || Card
No
Reject card
Yes
Card.CHA = ... || Workshop Card
Yes
Require PIN from user and send to card for verification
Verify (PIN)
Verify PIN
OK / KO
No
PIN OK
No
Yes
Generate Challenge Rnd1 (8 Bytes) Authenticate card
Internal Authenticate (Rnd1 || VU.CHR)
- Verify received CHR matches current PK.KID
- Generate K1, random number, 16 Bytes
- Generate PRnd2 90 Bytes (random padding)
- Compute authentication token: VU.PK[Card.SK*['6A' || PRnd2 || K1 || Hash(PRnd2||K1||Rnd1||VU.CHR) || 'BC']] = Encryption of signature* (ISO9796-2) of PRnd2 || K1 || Rnd1 || VU.CHR.
AutToken / KO
OK
No
Yes
Signature* = min {Signature,n-Signature} where n is the modulus of the key used to sign
- Compute: Signature=VU.SK.[AutToken]
- Decrypt and verify Signature with Card.PK to recover PRnd2 || K1 || H'
- verify Hash(PRnd2||K1||Rnd1||VU.CHR) = H'
- Store K1
OK
Not OK
Request Challenge (8 Bytes)
Get Challenge
Rnd3
Generate Challenge Rnd3 (8 Bytes)
- Generate K2, random number 16 Bytes
- Generate PRnd4 90 Bytes (random padding)
- Compute authentication token: Card.PK[VU.SK*['6A' || PRnd4 || K2 || Hash(PRnd4||K2||Rnd3||Card.CHR) || 'BC']] = Encryption of signature* (ISO9796-2) of PRnd4 || K2 || Rnd3 || Card.CHR
- Authenticate self to card
External Authenticate (AutToken)
- Verify that current PK.CHA = Tachograph || VU
- Compute: Signature=Card.SK[AutToken],
- Decrypt and verify Signature with VU.PK, to recover PRnd4 || K2 || H'
- verify Hash(PRnd4||K2||Rnd3||Card.CHR) = H'
- if verifications OK open AUT rights
- Store K2.
OK / KO
OK
No
Yes
Set TDES Session Key to (Ka, Kb, Ka) with Ka || Kb = K1 XOR K2 Set SSC to Rnd3 || Rnd1 (4 LSB of each)
Set TDES Session Key to (Ka, Kb, Ka) with Ka || Kb = K1 XOR K2 Set SSC to Rnd3 || Rnd1 (4 LSB of each)
Continue
Authentication failed Reject card

▼B

5. MEKANISMER FÖR SEKRETESS, INTEGRITET OCH AUTENTISERING VID ÖVERFÖRING AV DATA MELLAN FORDONSENHET OCH KORT

5.1. **Säker meddelandehantering**

CSM_021 Integriteten vid överföring av data mellan fordonsenhet och kort ska skyddas genom säker meddelandehantering (*secure messaging*) i enlighet med referenserna [ISO/IEC 7816-4] och [ISO/IEC 7816-8].

CSM_022 När data behöver skyddas vid överföring ska ett dataobjekt för kryptografisk kontrollsumma (*Cryptographic Checksum Data Object*) fogas till de dataobjekt som sänds inom kommandot eller svaret. Den kryptografiska kontrollsumman ska verifieras av mottagaren.

CSM_023 Den kryptografiska kontrollsumman hos data som sänds inom ett kommando ska integrera kommandots startdel (*command header*) och samtliga sända dataobjekt (=> CLA = ‘0C’, och samtliga dataobjekt ska kapslas in med taggar i vilka b1 = 1).

CSM_024 Byte för information om svarets status ska skyddas av en kryptografisk kontrollsumma om svaret inte innehåller något datafält.

CSM_025 Kryptografiska kontrollsummor ska ha en längd på 4 byte.

Strukturen för kommandon och svar vid användning av säker meddelandehantering är därför följande:

De dataobjekt som används är en delmängd av de dataobjekt för säker meddelandehantering som beskrivs i ISO/IEC 7816-4:

Tagg	Memosymbol (*mnemonic*)	Betydelse
‘81’	T_{PV}	Klarvärde (PV, *Plain Value*); ej BER-TLV-kodade data (skyddas av CC).
‘97’	$\mathbf{T_{LE}}$	Värde för Le i det oskyddade kommandot (skyddas av CC).
‘99’	T_{SW}	Statusinformation (skyddas av CC).
‘8E’	T_{CC}	Kryptografisk kontrollsumma
‘87’	$T_{PI\ CG}$	Byte för indikering av utfyllnad (PI, *Padding Indicator*) || Kryptogram (klarvärde, ej BER-TLV-kodat).

▼B

Antag följande oskyddade par med kommando och svar:

Kommando – startdel (*header*)				Kommando – nyttodel (*body*)		
CLA	INS	P1	P2	[L_c-fält]	[Datafält]	[L_e-fält]
4 byte				L byte, benämnda B_1 till B_L		

Svar – nyttodel (*body*)	Svar – slutdel (*trailer*)	
[Datafält]	SW1	SW2
L_r byte med data	2 byte	

Det motsvarande skyddade paret med kommando och svar är följande:

Skyddat kommando:

Kommando – startdel (CH, *Command Header*)				Kommando – nyttodel (*body*)										
CLA	INS	P1	P2	[Nytt L_c-fält]	[Nytt datafält]									[Nytt L_e-fält]
‘OC’				Längd för nytt datafält	T_{PV}	L_{PV}	PV	T_{LE}	L_{LE}	L_e	T_{CC}	L_{CC}	CC	‘00’
					‘81’	L_c	Datafält	‘97’	‘01’	L_e	‘8E’	‘04’	CC	

Data som ska ingå i kontrollsumman = CH || PB || T_{PV} || L_{PV} || PV || T_{LE} || L_{LE} || L_e || PB

PB (byte för utfyllnad, *Padding Bytes*) = (80 .. 00) i enlighet med ISO-IEC 7816-4 och ISO 9797, metod 2.

Dataobjekten PV och LE förekommer endast när det finns motsvarande data i det oskyddade kommandot.

Skyddat svar:

1. Fall där svarsdatafältet inte är tomt och inte behöver sekretesskyddas:

Svar – nyttodel (*body*)						Svar – slutdel (*trailer*)
[Nytt datafält]						Nya SW1 SW2
T_{PV}	L_{PV}	PV	T_{CC}	L_{CC}	CC	
‘81’	L_r	Datafält	‘8E’	‘04’	CC	

Data som ska ingå i kontrollsumman = T_{PV} || L_{PV} || PV || PB

2. Fall där svarsdatafältet inte är tomt och behöver sekretesskyddas:

▼B

Svar – nyttodel (*body*)						Svar – slutdel (*trailer*)
[Nytt datafält]						Nya SW1 SW2
$T_{PI\ CG}$	$L_{PI\ CG}$	PI CG	T_{CC}	L_{CC}	CC	
‘87’		PI || CG	‘8E’	‘04’	CC	

Data som ska ingå i kryptogrammet (CG): icke BER-TLV-kodade data och utfyllnadsbyte.

Data som ska ingå i kontrollsumman = $T_{PI\ CG}$ || $L_{PI\ CG}$ || PI CG || PB

3. Fall där svarsdatafältet är tomt:

Svar – nyttodel (*body*)						Svar – slutdel (*trailer*)
[Nytt datafält]						Nya SW1 SW2
T_{SW}	L_{SW}	SW	T_{CC}	L_{CC}	CC	
‘99’	‘02’	Nya SW1 SW2	‘8E’	‘04’	CC	

Data som ska ingå i kontrollsumman = T_{SW} || L_{SW} || SW || PB

5.2. **Felhantering avseende säker meddelandehantering**

CSM_026 När färdskrivarkortet känner av ett fel avseende säker meddelandehantering vid tolkning av ett kommando måste byte för status återsändas utan säker meddelandehantering. Enligt ISO/IEC 7816-4 definieras följande byte för status för att ange fel avseende säker meddelandehantering:

‘66 88’: Misslyckad verifiering av kryptografisk kontrollsumma.

‘69 87’: Förväntade dataobjekt för säker meddelandehantering saknas.

‘69 88’: Felaktiga dataobjekt för säker meddelandehantering.

CSM_027 När färdskrivarkortet returnerar byte för status utan dataobjekt för säker meddelandehantering eller med ett felaktigt dataobjekt för säker meddelandehantering måste sessionen avbrytas av fordonsenheten.

5.3. **Algoritm för beräkning av kryptografiska kontrollsummor**

CSM_028 Kryptografiska kontrollsummor byggs med hjälp av *retail MACs* enligt ANSI X9.19 med DES:

— Första steget: Det första kontrollblocket y0 är E(Ka, SSC).

— Följande steg: Kontrollblocken y1, ..., yn beräknas med hjälp av Ka.

— Sista steget: Den kryptografiska kontrollsumman beräknas från det sista kontrollblocket yn på följande sätt: E(Ka, D(Kb, yn))

där E() betyder kryptering med DES, och D() betyder dekryptering med DES.

De fyra mest signifikanta bytarna i den kryptografiska kontrollsumman överförs.

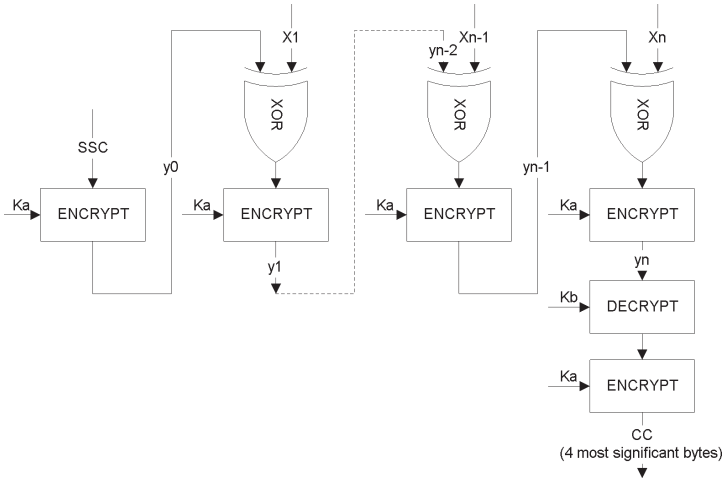
▼B

CSM_029 Räknaren för sekvenssändning (SSC, *Send Sequence Counter*) ska initieras vid förfarandet för överenskommelse om nyckel till:

Första SSC: Rnd3 (4 minst signifikanta byte) || Rnd1 (4 minst signifikanta byte)

CSM_030 SSC ska ökas med 1 varje gång innan en MAC beräknas (dvs. SSC för första kommando är första SSC+1, SSC för det första svaret är första SSC+2).

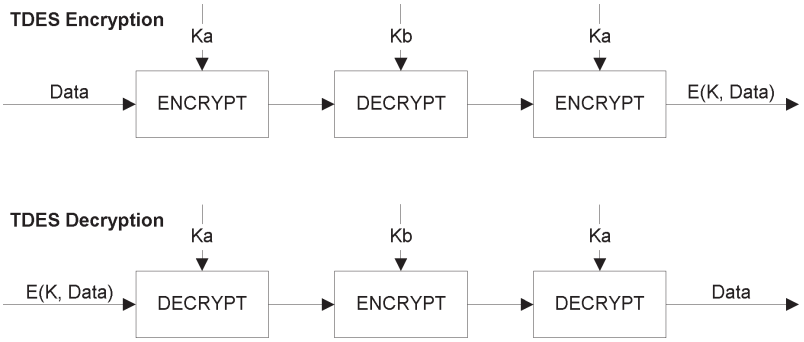
I följande figur visas beräkningen av *retail MAC*:



5.4. **Algoritm för att beräkna kryptogram för sekretessdataobjekt**

CSM_031 Kryptogram beräknas med hjälp av TDEA i TCBC-läge enligt referenserna [TDES] och [TDES-OP] och med nollvektorn som block med startvärde (*Initial Value*).

I följande figur visas tillämpningen av nycklar i TDES:



▼B

6. MEKANISMER FÖR DIGITAL SIGNATUR VID DATAÖVERFÖRING

CSM_032 IDE-enheten (*Intelligent Dedicated Equipment*) lagrar data som tas emot från en utrustning (fordonsenhet eller kort) under en överföringssession inom en (1) fysisk datafil. Denna fil måste innehålla certifikaten MS_i.C och EQT.C. Filen innehåller digitala signaturer för datablock enligt specifikation i tillägg 7 om protokoll för dataöverföring.

CSM_033 Digitala signaturer för överförda data ska använda ett schema för digitala signaturer med tillägg så att överförda data kan läsas utan att dekrypteras om så önskas.

6.1. **Generering av signatur**

CSM_034 Utrustningens generering av datasignaturer ska följa det signaturschema med tillägg som definieras i referens [PKCS1] med SHA-1 hashfunktion:

Signatur = EQT.SK[‘00’ || ‘01’ || *PS* || ‘00’ || DER(SHA-1(Data))]

PS = Utfyllnadssträng med oktetter med värdet ‘FF’ så att längden blir 128.

DER(SHA-1(*M*)) (*Distinguished Encoding Rules*) är kodningen av algoritm-ID för hashfunktionen och hashvärdet till ett ASN.1-värde av typen DigestInfo:

‘30’||‘21’||‘30’||‘09’||‘06’||‘05’||‘2B’||‘0E’||‘03’||‘02’||‘1A’||‘05’ ||‘00’||‘04’||‘14’||Hashvärde

6.2. **Verifiering av signatur**

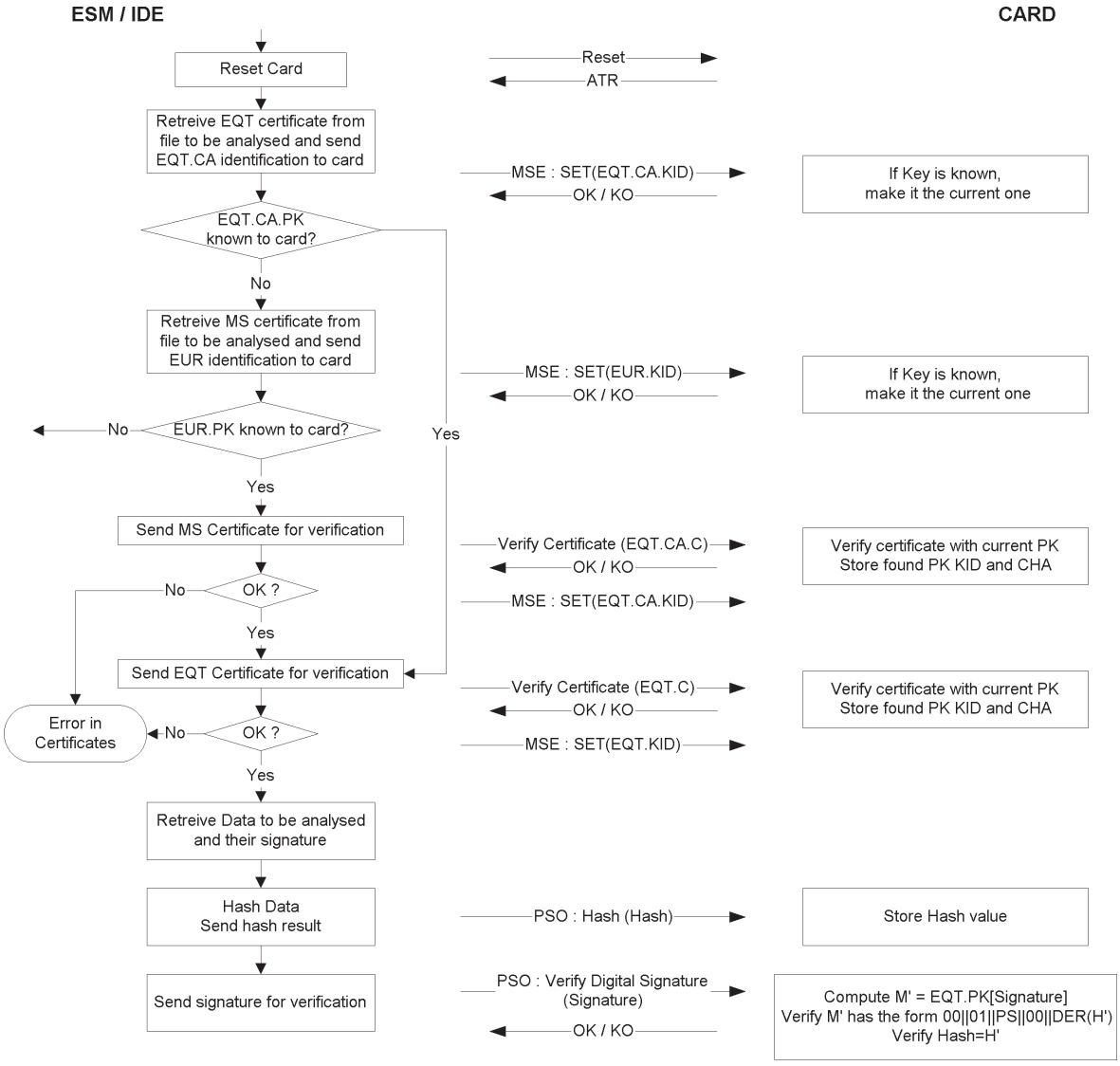
CSM_035 Verifiering av datasignaturer för överförda data ska följa det signaturschema med tillägg som definieras i referens [PKCS1] med SHA-1 hashfunktion:

Den som verifierar måste oberoende känna igen (och lita på) den europeiska öppna nyckeln EUR.PK.

I följande tabell återges det protokoll som en IDE-enhet med ett kontrollkort kan följa för att verifiera integriteten hos data som överförs och lagras på det externa lagringsmediet (ESM, *External Storage Media*). Kontrollkortet används för att dekryptera digitala signaturer. Denna funktion får i detta fall inte införas i IDE-enheten.

Den utrustning som har överfört och signerat de data som ska analyseras betecknas EQT.

▼B



DEL B

ANDRA GENERATIONENS FÄRDSKRIVARSYSTEM

7. INLEDNING

7.1. **Referenser**

Följande referenser används i denna del av detta tillägg:

AES	National Institute of Standards and Technology (NIST), FIPS PUB 197: Advanced Encryption Standard (AES), November 26, 2001
DSS	National Institute of Standards and Technology (NIST), FIPS PUB 186-4: Digital Signature Standard (DSS), July 2013
ISO 7816-4	ISO/IEC 7816-4, Identification cards – Integrated circuit cards – Part 4: Organization, security and commands for interchange. Third edition 2013-04-15
ISO 7816-8	ISO/IEC 7816-8, Identification cards – Integrated circuit cards – Part 8: Commands for security operations. Second edition 2004-06-01

▼B

ISO 8825-1	ISO/IEC 8825-1, Information technology – ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER). Fourth edition, 2008-12-15
ISO 9797-1	ISO/IEC 9797-1, Information technology – Security techniques – Message Authentication Codes (MACs) – Part 1: Mechanisms using a block cipher. Second edition, 2011-03-01
ISO 10116	ISO/IEC 10116, Information technology – Security techniques – Modes of operation of an *n*-bit block cipher. Third edition, 2006-02-01
ISO 16844-3	ISO/IEC 16844-3, Road vehicles – Tachograph systems – Part 3: Motion sensor interface. First edition 2004, including Technical Corrigendum 1 2006
RFC 5480	Elliptic Curve Cryptography Subject Public Key Information, March 2009
RFC 5639	Elliptic Curve Cryptography (ECC) – Brainpool Standard Curves and Curve Generation, 2010
RFC 5869	HMAC-based Extract-and-Expand Key Derivation Function (HKDF), May 2010
SHS	National Institute of Standards and Technology (NIST), FIPS PUB 180-4: Secure Hash Standard, March 2012
SP 800-38B	National Institute of Standards and Technology (NIST), Special Publication 800-38B: Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication, 2005
TR-03111	BSI Technical Guideline TR-03111, Elliptic Curve Cryptography, version 2.00, 2012-06-28

7.2. **Beteckningar och förkortningar**

Följande beteckningar och förkortningar används i detta tillägg:

AES	*Advanced Encryption Standard* (standardiserad krypteringsalgoritm)
CA	*Certification Authority* (certifieringsinstans)
CAR	*Certification Authority Reference* (certifieringsinstansens referens)
CBC	*Cipher Block Chaining* (kedjeanvändande blockchiffer)
CH	*Command Header* (startdel av ett kommando)
CHA	*Certificate Holder Authorisation* (certifikatinnehavarens auktorisering)
CHR	*Certificate Holder Reference* (certifikatinnehavarens referens)
CV	*Constant Vector* (konstant vektor)
DER	*Distinguished Encoding Rules* (regelsamling för kodning)
DO	*Data Object* (dataobjekt)
DSRC	*Dedicated Short Range Communication* (radiokommunikation över korta avstånd)
ECC	*Elliptic Curve Cryptography* (elliptisk kryptering)
ECDSA	*Elliptic Curve Digital Signature Algorithm* (krypteringsalgoritm)
ECDH	*Elliptic Curve Diffie-Hellman* (algoritm för överenskommelse mellan nycklar)
EGF	*External GNSS Facility* (extern GNSS-anordning)
EQT	*Equipment* (utrustning)

▼B

IDE	*Intelligent Dedicated Equipment* (t.ex. persondator)
K_M	Huvudnyckel för rörelsesensor, möjliggör parning av en fordonsenhet och en rörelsesensor.
K_{M-VU}	Nyckel som installeras i en fordonsenhet så att fordonsenheten kan härleda rörelsesensorns huvudnyckel om ett verkstadskort sätts in i fordonsenheten.
K_{M-WC}	Nyckel som installeras i ett verkstadskort så att en fordonsenhet kan härleda rörelsesensorns huvudnyckel om verkstadskortet sätts in i fordonsenheten.
MAC	Message Authentication Code
MoS	*Motion Sensor* (rörelsesensor)
MSB	*Most Significant Bit* (mest signifikanta bit)
PKI	*Public Key Infrastructure* (infrastruktur för öppen nyckel)
RCF	*Remote Communication Facility* (kommunikationsanordning för fjärravläsning)
SSC	*Send Sequence Counter* (räknare för sekvenssändning)
SM	*Secure Messaging* (säker meddelandehantering)
TDES	*Triple Data Encryption Standard* (krypteringsstandard)
TLV	*Tag Length Value* (tagglängd)
VU	*Vehicle Unit* (fordonsenhet)
X.C	Certifikat för den öppna nyckel som innehas av användare X
X.CA	Certifieringsinstans som utfärdat certifikat för användare X
X.CAR	Referens för certifieringsinstans, nämns i certifikat för användare X
X.CHR	Referens för certifikatinnehavare, nämns i certifikat för användare X
X.PK	Öppen nyckel för användare X
X.SK	Privat nyckel för användare X
$X.PK_{eph}$	Tillfällig (*ephemeral*) öppen nyckel för användare X
$X.SK_{eph}$	Tillfällig (*ephemeral*) privat nyckel för användare X
‘xx’	Hexadecimalt värde
||	Konkateneringsoperator

7.3. **Definitioner**

De termer och definitioner som används i detta tillägg finns i avsnitt I i bilaga 1C.

8. KRYPTOSYSTEM OCH ALGORITMER

8.1. **Kryptosystem**

CSM_38 Fordonsenheter och färdskrivarkort ska använda ett kryptosystem med öppna nycklar, baserat på elliptisk kryptering, för att tillhandahålla följande säkerhetstjänster:

— Ömsesidig autentisering mellan en fordonsenhet och ett kort.

▼B

— Överenskommelse om AES-sessionsnycklar mellan en fordonsenhet och ett kort.

— Säkerställande av autenticitet, integritet och oavvislighet avseende data som överförs från fordonsenheter och färdskrivarkort till externa media.

CSM_39 Fordonsenheter och externa GNSS-anordningar ska använda ett kryptosystem med öppna nycklar, baserat på elliptisk kryptering, för att tillhandahålla följande säkerhetsmekanismer:

— Koppling av en fordonsenhet och en extern GNSS-anordning.

— Ömsesidig autentisering mellan en fordonsenhet och en extern GNSS-anordning.

— Överenskommelse om en AES-sessionsnyckel mellan en fordonsenhet och en extern GNSS-anordning.

CSM_40 Fordonsenheter och färdskrivarkort ska använda ett AES-baserat, symmetriskt kryptosystem för att tillhandahålla följande säkerhetsmekanismer:

— Säkerställande av autenticitet och integritet avseende data som utväxlas mellan en fordonsenhet och ett färdskrivarkort.

— Säkerställande, i förekommande fall, av sekretess avseende data som utväxlas mellan en fordonsenhet och ett färdskrivarkort.

CSM_41 Fordonsenheter och externa GNSS-anordningar ska använda ett AES-baserat, symmetriskt kryptosystem för att tillhandahålla följande säkerhetsmekanismer:

— Säkerställande av autenticitet och integritet avseende data som utväxlas mellan en fordonsenhet och en extern GNSS-anordning.

CSM_42 Fordonsenheter och rörelsesensorer ska använda ett AES-baserat, symmetriskt kryptosystem för att tillhandahålla följande säkerhetsmekanismer:

— Parning av en fordonsenhet och en rörelsesensor.

— Ömsesidig autentisering mellan en fordonsenhet och en rörelsesensor.

— Säkerställande av sekretess avseende data som utväxlas mellan en fordonsenhet och en rörelsesensor.

CSM_43 Fordonsenheter och kontrollkort ska använda ett AES-baserat, symmetriskt kryptosystem för att tillhandahålla följande säkerhetsmekanismer i fjärrkommunikationsgränssnittet:

— Säkerställande av sekretess, autenticitet och integritet avseende data som överförs från en fordonsenhet till ett kontrollkort.

Anmärkningar:

— Egentligen överförs data från en fordonsenhet till en fjärravläsare som sköts av en kontrolltjänsteman, med hjälp av en kommunikationsanordning för fjärravläsning som kan vara intern eller extern i förhållande till fordonsenheten (se tillägg 14). Fjärravläsaren sänder dock mottagna data

▼B

till ett kontrollkort för dekryptering och validering av autenticitet. Ur säkerhetssynvinkel är kommunikationsanordningen för fjärravläsning och fjärravläsaren helt transparenta.

— Ett verkstadskort erbjuder samma säkerhetsmekanismer för DSRC-gränssnittet som ett kontrollkort. Det ger möjlighet för en verkstad att kontrollera att kommunikationsgränssnittet för fjärravläsning i en fordonsenhet fungerar korrekt, inklusive i fråga om säkerhet. Se avsnitt 9.2.2 för mer information.

8.2. **Kryptografiska algoritmer**

8.2.1 *Symmetriska algoritmer*

CSM_44 Fordonsenheter, färdskrivarkort, rörelsesensorer och externa GNSS-anordningar ska stödja AES-algoritmen såsom den definieras i [AES], med nyckellängderna 128, 192 och 256 bitar.

8.2.2 *Asymmetriska algoritmer och standardiserade domänparametrar*

CSM_45 Fordonsenheter, färdskrivarkort och externa GNSS-anordningar ska stödja elliptisk kryptering med nyckelstorlek på 256, 384 och 512/521 bitar.

CSM_46 Fordonsenheter, färdskrivarkort och externa GNSS-anordningar ska stödja signeringsalgoritmen ECDSA, såsom den specificeras i [DSS].

CSM_47 Fordonsenheter, färdskrivarkort och externa GNSS-anordningar ska stödja algoritmen ECKA-EG för nyckelöverenskommelse, såsom den specificeras i [TR 03111].

CSM_48 Fordonsenheter, färdskrivarkort och externa GNSS-anordningar ska stödja samtliga standardiserade domänparametrar som anges i Table 1 nedan för elliptisk kryptering (ECC).

Tabell 1

Standardiserade domänparametrar

Namn	Storlek (bitar)	Referens	Objektidentifierare
NIST P-256	256	[DSS], [RFC 5480]	`secp256r1`
BrainpoolP256r1	256	[RFC 5639]	`brainpoolP256r1`
NIST P-384	384	[DSS], [RFC 5480]	`secp384r1`
BrainpoolP384r1	384	[RFC 5639]	`brainpoolP384r1`
BrainpoolP512r1	512	[RFC 5639]	`brainpoolP512r1`
NIST P-521	521	[DSS], [RFC 5480]	`secp521r1`

▼B

Anm.: De objektidentifierare som nämns i den sista kolumnen i Table 1 specificeras i [RFC 5639] för Brainpool-kurvor och i [RFC 5480] för NIST-kurvor.

Exempel 1: Objektidentifieraren för kurvan BrainpoolP256r1 är `{iso(1) identified-organization(3) teletrust(36) algorithm(3) signaturealgorithm(3) ecSign(2) ecStdCurvesAndGeneration (8) ellipticCurve(1) versionOne(1) 7}`.

Eller med punktnotation: 1.3.36.3.3.2.8.1.1.7.

Exempel 2: Objektidentifieraren för kurvan NIST P-384 är

`{iso(1) identified-organization(3) certicom(132) curve(0) 34}`.

Eller med punktnotation: 1.3.132.0.34.

8.2.3 *Hashalgoritmer*

CSM_49 Fordonsenheter och färdskrivarkort ska stödja algoritmerna SHA-256, SHA-384 och SHA-512 som specificeras i [SHS].

8.2.4 *Chifferföljder*

CSM_50 Om en symmetrisk algoritm, en assymmetrisk algoritm och/eller en hashalgoritm används tillsammans för att utgöra ett säkerhetsprotokoll ska deras respektive nyckellängder och hashstorlekar ge ungefär likvärdig styrka. I Table 2 visas de tillåtna chifferföljderna:

Tabell 2

Tillåtna chifferföljder

Identifierare för chifferföljd	Nyckelstorlek för elliptisk kryptering (ECC) (bitar)	Nyckellängd för AES (bitar)	Hashalgoritm	MAC-längd (byte)
CS#1	256	128	SHA-256	8
CS#2	384	192	SHA-384	12
CS#3	512/521	256	SHA-512	16

Anmärkning: ECC-nycklar med storlek 512 bitar och 521 bitar anses ge likvärdig styrka för alla syften som omfattas av detta tillägg.

9. NYCKLAR OCH CERTIFIKAT

9.1. **ASYMMETRISKA NYCKELPAR OCH CERTIFIKAT FÖR ÖPPNA NYCKLAR**

9.1.1 *Allmänt*

Anmärkning: De nycklar som beskrivs i detta avsnitt används för ömsesidig autentisering och säker meddelandehantering mellan fordonsenheter och färdskrivarkort och mellan fordonsenheter och externa GNSS-anordningar. Dessa processer beskrivs i detalj i kapitlen 10 och 11 i detta tillägg.

CSM_51 Inom det europeiska smarta färdskrivarsystemet ska nyckelpar för elliptisk kryptering (ECC) och motsvarande certifikat genereras och förvaltas med hjälp av följande tre hierarkiska funktionsnivåer:

— Europeisk nivå.

— Medlemsstatsnivå.

— Utrustningsnivå.

▼B

CSM_52 Inom hela det europeiska smarta färdskrivarsystemet ska öppna och privata nycklar och certifikat genereras, förvaltas och överlämnas med hjälp av standardiserade och säkra metoder.

9.1.2 *Europeisk nivå*

CSM_53 På europeisk nivå ska ett enda unikt nyckelpar för elliptisk kryptering genereras och benämnas EUR. Det ska bestå av en privat nyckel (EUR.SK) och en öppen nyckel (EUR.PK). Detta nyckelpar ska utgöra rotnyckelpar för hela infrastrukturen för öppna nycklar (PKI, *Public Key Infrastructure*) inom hela det europeiska smarta färdskrivarsystemet. Dessa arbetsuppgifter ska utföras av en europeisk rotcertifieringsinstans (Erca, *European Root Certificate Authority*), under Europeiska kommissionens överinseende och ansvar.

CSM_54 Erca ska använda den europiska öppna nyckeln för att signera ett (självsignerat) rotcertifikat från den europiska öppna nyckeln och överlämna detta europeiska rotcertifikat till alla medlemsstater.

CSM_55 Erca ska använda den europiska privata nyckeln för att på begäran signera medlemsstaternas certifikat. Erca ska föra ett register över alla signerade certifikat för öppna nycklar på medlemsstatsnivå.

CSM_56 Erca ska, såsom visas i Figure 1 i avsnitt 9.1.7, generera ett nytt europeiskt rotnyckelpar vart sjuttonde år. Varje gång Erca genererar ett nytt europeiskt rotnyckelpar ska man också skapa ett nytt självsignerat rotcertifikat för den nya europeiska öppna nyckeln. Giltighetstiden för ett europeiskt rotcertifikat ska vara 34 år plus 3 månader.

Anmärkning: Införandet av ett nytt rotnyckelpar innebär även att Erca genererar en ny huvudnyckel (*Master Key*) för rörelsesensorer och en ny huvudnyckel för DSRC (se avsnitten 9.2.1.2 och 9.2.2.2).

CSM_57 Erca ska, innan man genererar ett nytt europeiskt rotnyckelpar, genomföra en analys av den kryptografiska styrka som behövs för det nya nyckelparet, med tanke på att det ska bibehålla sin säkerhet under de kommande 34 åren. Erca ska om så är nödvändigt byta till en chifferföljd som är starkare än den nuvarande, såsom anges i CSM_50.

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. Detta visas även i Figure 1 i avsnitt 9.1.7.

Anmärkning: Eftersom ett länkcertifikat innehåller Ercas öppna nyckel av generation *X* och är signerat med Ercas privata nyckel av generation *X-1* innebär länkcertifikatet att utrustning som utfärdats inom generation *X-1* får möjlighet att förlita sig på utrustning som utfärdas inom generation *X*.

CSM_59 Erca får inte använda den privata nyckeln i ett rotnyckelpar för något som helst ändamål från den tidpunkt då ett nytt rotnyckelcertifikat blir giltigt.

▼B

CSM_60 Erca ska alltid förfoga över följande kryptografiska nycklar och certifikat:

— Nuvarande EUR-nyckelpar och motvarande certifikat.

— Alla tidigare EUR-certifikat som använts för verifiering av MSCA-certifikat som fortfarande är giltiga.

— Länkcertifikat för samtliga generationer av EUR-certifikat utom det första.

9.1.3 *Medlemsstatsnivå*

CSM_61 På medlemsstatsnivå ska alla medlemsstater som måste signera certifikat för färdskrivarkort generera ett unikt eller flera unika nyckelpar för elliptisk kryptering som benämns MSCA_Card. Alla medlemsstater som måste signera certifikat för fordonsenheter eller externa GNSS-anordningar ska dessutom generera ett unikt eller flera unika nyckelpar för elliptisk kryptering som benämns MSCA_VU-EGF.

CSM_62 Arbetsuppgiften att generera medlemsstatens nyckelpar ska utföras av en certifieringsinstans i medlemsstaten (MSCA, *Member State Certificate Authority*). Varje gång medlemsstatens certifieringsinstans genererar ett nyckelpar för medlemsstaten ska den sända den öppna nyckeln till Erca för att få ett motsvarande medlemsstatscertifikat signerat av Erca.

CSM_63 En medlemsstats certifieringsinstans ska välja styrka för medlemsstatens nyckelpar så att den är likvärdig med styrkan hos det europeiska rotnyckelpar som används för att signera motsvarande medlemsstatscertifikat.

CSM_64 Ett eventuellt MSCA_VU-EGF-nyckelpar ska bestå av en privat nyckel benämnd MSCA_VU-EGF.SK och en öppen nyckel benämnd MSCA_VU-EGF.PK. En medlemsstats certifieringsinstans ska använda den privata nyckeln MSCA_VU-EGF.SK endast för att signera certifikaten för öppna nycklar till fordonsenheter och externa GNSS-anordningar.

CSM_65 Ett eventuellt MSCA_Card-nyckelpar ska bestå av en privat nyckel benämnd MSCA_Card.SK och en öppen nyckel benämnd MSCA_Card.PK. En medlemsstats certifieringsinstans ska använda den privata nyckeln MSCA_Card.SK endast för att signera certifikaten för öppna nycklar till färdskrivarkort.

CSM_66 En medlemsstats certifieringsinstans ska föra ett register över alla signerade certifikat för fordonsenheter, externa GNSS-anordningar och kort, tillsammans med identifiering av den utrustning som respektive certifikat är avsett för.

CSM_67 Giltighetstiden för ett MSCA_VU-EGF-certifikat ska vara 17 år plus 3 månader. Giltighetstiden för ett MSCA_Card-certifikat ska vara 7 år plus 1 månad.

CSM_68 Såsom visas i Figure 1 avsnitt 9.1.7 ska den privata nyckeln i ett MSCA_VU-EGF-nyckelpar och den privata nyckeln i ett MSCA_Card-nyckelpar ha en användningsperiod på två år.

▼B

CSM_69 En medlemsstats certifieringsinstans (MSCA) får inte använda den privata nyckeln i ett MSCA_VU-EGF-nyckelpar för något som helst ändamål efter det att dess användningsperiod har löpt ut. En medlemsstats certifieringsinstans får inte heller använda den privata nyckeln i ett MSCA_Card-nyckelpar för något som helst ändamål efter det att dess användningsperiod har löpt ut.

CSM_70 En medlemsstats certifieringsinstans ska alltid förfoga över följande kryptografiska nycklar och certifikat:

— Nuvarande MSCA_Card-nyckelpar och motvarande certifikat.

— Alla tidigare MSCA_Card-certifikat som använts för verifiering av certifikat till färdskrivarkort som fortfarande är giltiga.

— Det nuvarande EUR-certifikatet som krävs för verifiering av det nuvarande MSCA-certifikatet.

— Alla tidigare EUR-certifikat som krävs för verifiering av samtliga MSCA-certifikat som fortfarande är giltiga.

CSM_71 Om en medlemsstats certifieringsinstans måste signera certifikat för fordonsenheter eller externa GNSS-anordningar ska den dessutom förfoga över följande nycklar och certifikat:

— Nuvarande MSCA_VU-EGF-nyckelpar och motvarande certifikat.

— Alla tidigare öppna nycklar för MSCA_VU-EGF som använts för verifiering av certifikat till fordonsenheter eller externa GNSS-anordningar som fortfarande är giltiga.

9.1.4 *Utrustningsnivå: Fordonsenheter*

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 certifieringsinstansen i den medlemsstat där parten har sitt säte för att få ett motsvarande certifikat för fordonsenheten signerat av medlemsstatens certifieringsinstans. Den privata nyckeln får endast användas av fordonsenheten.

CSM_73 VU_MA- och VU_Sign-certifikaten för en viss fordonsenhet ska ha samma första giltighetsdag.

CSM_74 En tillverkare av fordonsenheter ska välja styrka för fordonsenhetens nyckelpar så att den är likvärdig med styrkan hos det MSCA-nyckelpar som används för att signera motsvarande certifikat för fordonsenheten.

CSM_75 En fordonsenhet ska använda sitt VU_MA-nyckelpar, bestående av en privat nyckel (VU_MA.SK) och en öppen nyckel (VU_MA.PK) endast för att utföra autentisering av fordonsenheten gentemot färdskrivarkort och externa GNSS-anordningar såsom anges i avsnitten 10.3 och 11.4 i detta tillägg.

CSM_76 En fordonsenhet ska kunna generera tillfälliga (*ephemeral*) nyckelpar för elliptisk kryptering och ska använda ett tillfälligt nyckelpar endast för att genomföra överenskommelse om sessionsnyckel med ett färdskrivarkort eller en extern GNSS-anordning såsom anges i avsnitten 10.4 och 11.4 i detta tillägg.

▼B

CSM_77 En fordonsenhet ska använda den privata nyckeln VU_Sign.SK i sitt VU_Sign-nyckelpar endast för att signera överförda datafiler såsom anges i kapitel 14 i detta tillägg. Motsvarande öppna nyckel VU_Sign.PK ska användas endast för att verifiera signaturer som skapas av fordonsenheten.

CSM_78 Giltighetstiden för ett VU_MA-certifikat ska vara 15 år plus 3 månader, såsom visas i Figure 1 i avsnitt 9.1.7. Giltighetstiden för ett VU_Sign-certifikat ska också vara 15 år plus 3 månader.

Anmärkningar:

— Den förlängda giltighetstiden för ett VU_Sign-certifikat gör det möjligt för en fordonsenhet att skapa giltiga signaturer för överförda data under de tre första månaderna efter det att certifikatet har löpt ut, såsom krävs i förordning (EU) nr 581/2010.

— Den förlängda giltighetstiden för ett VU_MA-certifikat behövs för att fordonsenheten ska kunna autentisera gentemot ett kontrollkort eller ett företagskort under de tre första månaderna efter det att certifikatet har löpt ut, så att det är möjligt att genomföra en dataöverföring.

CSM_79 En fordonsenhet får inte använda den privata nyckeln i sitt nyckelpar för något som helst ändamål efter det att det motsvarande certifikatet har löpt ut.

CSM_80 Fordonsenhetens nyckelpar (med undantag för tillfälliga nyckelpar) och motsvarande certifikat för en viss fordonsenhet får inte ersättas eller förnyas på fältet efter det att fordonsenheten har tagits i drift.

Anmärkningar:

— Tillfälliga (*ephemeral*) nyckelpar omfattas inte av detta krav eftersom ett nytt tillfälligt nyckelpar genereras av en fordonsenhet vid varje chipautentisering och överenskommelse om sessionsnyckel (se avsnitt 10.4). Notera att tillfälliga nyckelpar inte har några motsvarande certifikat.

— Detta krav utesluter inte möjligheten att ersätta statiska nyckelpar för fordonsenheten vid en renovering eller en reparation i en säker miljö som kontrolleras av fordonsenhetens tillverkare.

CSM_81 Fordonsenheter ska när de tas i drift innehålla följande kryptografiska nycklar och certifikat:

— Den privata nyckeln för VU_MA och motsvarande certifikat.

— Den privata nyckeln för VU_Sign och motsvarande certifikat.

— MSCA_VU-EGF-certifikatet som innehåller den öppna nyckeln MSCA_VU-EGF.PK som ska användas för verifiering av VU_MA- och VU_Sign-certifikaten.

▼B

— EUR-certifikatet som innehåller den öppna nyckeln EUR.PK som ska användas för verifiering av MSCA_VU-EGF-certifikatet.

— EUR-certifikatet vars giltighetstid direkt föregår giltighetstiden för det EUR-certifikat som ska användas för verifiering av MSCA_VU-EGF-certifikatet, i förekommande fall.

— Det länkcertifikat som länkar dessa två EUR-certifikat, i förekommande fall.

CSM_82 Fordonsenheter ska också, utöver de kryptografiska nycklar och certifikat som förtecknas i CSM_81 innehålla de nycklar och certifikat som anges i del A i detta tillägg och som möjliggör att en fordonsenhet kan samverka med första generationens färdskrivarkort.

9.1.5 *Utrustningsnivå: färdskrivarkort*

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 dessutom 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 certifieringsinstansen i den medlemsstat där parten har sitt säte för att få ett motsvarande certifikat för kortet signerat av medlemsstatens certifieringsinstans. Den privata nyckeln får endast användas av färdskrivarkortet.

CSM_84 Card_MA- och Card_Sign-certifikaten för ett visst förarkort eller verkstadskort ska ha samma första giltighetsdag.

CSM_85 En tillverkare av kort eller en användaranpassare av kort ska välja styrka för kortets nyckelpar så att den är likvärdig med styrkan hos det MSCA-nyckelpar som används för att signera motsvarande kortcertifikat.

CSM_86 Ett färdskrivarkort ska använda sitt Card_MA-nyckelpar, bestående av en privat nyckel (Card_MA.SK) och en öppen nyckel (Card_MA.PK) endast för att utföra ömsesidig autentisering och överenskommelse om sessionsnyckel gentemot fordonsenheter såsom anges i avsnitten 10.3 och 10.4 i detta tillägg.

CSM_87 Ett förarkort eller verkstadskort ska använda den privata nyckeln Card_Sign.SK i sitt Card_Sign-nyckelpar endast för att signera överförda datafiler såsom anges i kapitel 14 i detta tillägg. Motsvarande öppna nyckel Card_Sign.PK ska användas endast för att verifiera signaturer som skapas av kortet.

CSM_88 Giltighetstiden för ett CARD_MA-certifikat ska vara följande:

— För förarkort: 5 år

— För företagskort: 2 år

— För kontrollkort: 2 år

— För verkstadskort: 1 år

▼B

CSM_89 Giltighetstiden för ett CARD_Sign-certifikat ska vara följande:

— För förarkort: 5 år och 1 månad

— För verkstadskort: 1 år och 1 månad

Anmärkning: Den förlängda giltighetstiden för ett Card_Sign-certifikat gör det möjligt för ett förarkort att skapa giltiga signaturer för överförda data under den första månaden efter det att certifikatet har löpt ut. Detta är nödvändigt med tanke på förordning (EU) nr 581/2010, som kräver att en dataöverföring från ett förarkort måste vara möjlig upp till 28 dagar efter den sista registreringen av data.

CSM_90 Nyckelparen och motsvarande certifikat för ett visst färdskrivarkort får inte ersättas eller förnyas efter det att kortet utfärdats.

CSM_91 Färdskrivarkort ska när de utfärdas innehålla följande kryptografiska nycklar och certifikat:

— Den privata nyckeln för Card_MA och motsvarande certifikat.

— Dessutom, endast för förarkort och verkstadskort: den privata nyckeln Card_Sign och motsvarande certifikat.

— MSCA_Card-certifikatet som innehåller den öppna nyckeln MSCA_Card.PK som ska användas för verifiering av Card_MA- och Card_Sign-certifikaten.

— EUR-certifikatet som innehåller den öppna nyckeln EUR.PK som ska användas för verifiering av MSCA_Card-certifikatet.

— EUR-certifikatet vars giltighetstid direkt föregår giltighetstiden för det EUR-certifikat som ska användas för verifiering av MSCA_Card-certifikatet, i förekommande fall.

— Det länkcertifikat som länkar dessa två EUR-certifikat, i förekommande fall.

CSM_92 Färdskrivarkort ska också, utöver de kryptografiska nycklar och certifikat som förtecknas i CSM_91 innehålla de nycklar och certifikat som anges i del A i detta tillägg och som möjliggör att dessa kort kan samverka med första generationens fordonsenheter.

9.1.6 *Utrustningsnivå: externa GNSS-anordningar*

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 EGF_MA-nyckelpar genereras ska den öppna nyckeln sändas till certifieringsinstansen i den medlemsstat där nyckelparet hör hemma för att få ett motsvarande EGF_MA-certifikat signerat av medlemsstatens certifieringsinstans. Den privata nyckeln får endast användas av den externa GNSS-anordningen.

CSM_94 En tillverkare av externa GNSS-anordningar ska välja styrka för ett EGF_MA-nyckelpar så att den är likvärdig med styrkan hos det MSCA-nyckelpar som används för att signera motsvarande EGF_MA-certifikat.

▼B

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 avsnitten 11.4 och 11.4 i detta tillägg.

CSM_96 Giltighetstiden för ett EGF_MA-certifikat ska vara 15 år.

CSM_97 En extern GNSS-anordning får inte använda den privata nyckeln i sitt EGF_MA-nyckelpar för koppling till en fordonsenhet efter det att det motsvarande certifikatet har löpt ut.

Anmärkning: Såsom förklaras i avsnitt 11.3.3 kan en extern GNSS-anordning eventuellt använda sin privata nyckel för ömsesidig autentisering gentemot den fordonsenhet till vilken den redan är kopplad, även efter det att det motsvarande certifikatet har löpt ut.

CSM_98 EGF_MA-nyckelparet och motsvarande certifikat för en viss extern GNSS-anordning får inte ersättas eller förnyas på fältet efter det att den externa GNSS-anordningen har tagits i drift.

Anmärkning: Detta krav utesluter inte möjligheten att ersätta EGF-nyckelpar vid en renovering eller en reparation i en säker miljö som kontrolleras av tillverkaren av den externa GNSS-anordningen.

CSM_99 En extern GNSS-anordning ska när den tas i drift innehålla följande kryptografiska nycklar och certifikat:

— Den privata nyckeln för EGF_MA och motsvarande certifikat.

— MSCA_VU-EGF-certifikatet som innehåller den öppna nyckeln MSCA_VU-EGF.PK som ska användas för verifiering av EGF_MA-certifikatet.

— EUR-certifikatet som innehåller den öppna nyckeln EUR.PK som ska användas för verifiering av MSCA_VU-EGF-certifikatet.

— EUR-certifikatet vars giltighetstid direkt föregår giltighetstiden för det EUR-certifikat som ska användas för verifiering av MSCA_VU-EGF-certifikatet, i förekommande fall.

— Det länkcertifikat som länkar dessa två EUR-certifikat, i förekommande fall.

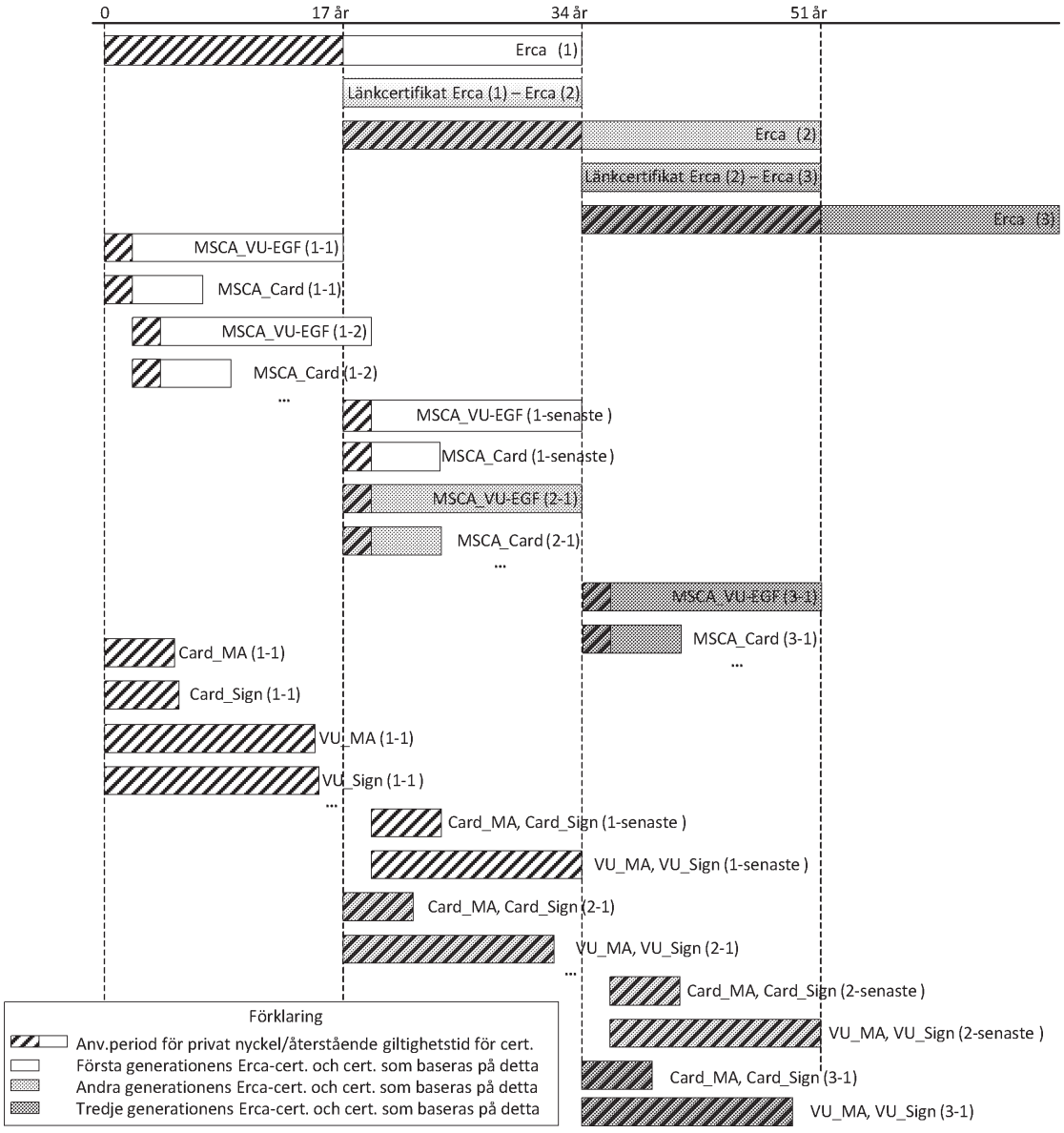
9.1.7 *Översikt: Ersättning av certifikat*

Figure 1 nedan visar med en tidslinje hur olika generationer av Erca-rotcertifikat, Erca-länkcertifikat, MSCA-certifikat och utrustningscertifikat (för fordonsenhet och kort) utfärdas och används.

▼B

Figur 1

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



Anmärkningar till Figure 1:

1. Olika generationer av rotcertifikatet anges av ett nummer inom parentes. Exempelvis är Erca (1) den första generationens Erca-rotcertifikat, Erca (2) den andra osv.

2. Andra certifikat anges med två nummer inom parentes, där det första numret anger generationen för det rotcertifikat under vilket certifikaten är utfärdade och det andra numret generationen för det aktuella certifikatet. Exempelvis är MSCA_Card (1-1) det första MSCA_Card-certifikatet som utfärdats på grundval av Erca (1), MSCA_Card (2-1) det första MSCA_Card-certifikatet som utfärdats på grundval av Erca (2), MSCA_Card (2-senaste) det senaste MSCA_Card-certifikatet som utfärdats på grundval av Erca (2), Card_MA (2-1) det första kortcertifikatet för ömsesidig autentisering som utfärdats på grundval av Erca (2), osv.

▼B

3. Certifikaten MSCA_Card (2-1) och MSCA_Card (1-senaste) utfärdas nästan men inte exakt samma datum. MSCA_Card (2-1) är det första MSCA_Card-certifikatet som utfärdats på grundval av Erca (2) och kommer att utfärdas något senare än MSCA_Card (1-senaste), det senaste MSCA_Card-certifikatet som utfärdats på grundval av Erca (1).

4. Såsom visas i figuren kommer de första fordonsenhets- och kortcertifikaten som utfärdats på grundval av Erca (2) att finnas nästan två år innan de sista fordonsenhets- och kortcertifikaten som utfärdats på grundval av Erca (1) kommer att finnas. Detta beror på det faktum att fordonsenhets- och kortcertifikat utfärdas på grundval av ett MSCA-certifikat, inte direkt på grundval av Erca-certifikatet. MSCA (2-1)-certifikatet kommer att utfärdas direkt efter det att Erca (2) blir giltigt, men MSCA (1-senaste)-certifikatet kommer att utfärdas endast något före den tidpunkten, precis i slutet av den tidsperiod när Erca (1)-certifikatet fortfarande är giltigt. Därför kommer dessa två MSCA-certifikat att ha nästan samma giltighetsperiod, trots att de tillhör olika generationer.

5. Den visade giltighetstiden för kort är giltighetstiden för förarkort (5 år).

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

9.2. **Symmetriska nycklar**

9.2.1 *Nycklar för att säkra kommunikation mellan fordonsenhet och rörelsesensor*

9.2.1.1 *Allmänt*

Anmärkning: Läsare av detta avsnitt förutsätts känna till innehållet i [ISO 16844-3] som beskriver gränssnittet mellan en fordonsenhet och en rörelsesensor. Parningsprocessen mellan en fordonsenhet och en rörelsesensor beskrivs i detalj i kapitel 12 i detta tillägg.

CSM_100 Ett antal symmetriska nycklar behövs för parning av fordonsenheter och rörelsesensorer, för ömsesidig autentisering mellan fordonsenheter och rörelsesensorer och för kryptering av kommunikation mellan fordonsenheter och rörelsesensorer (se Table 3). Alla dessa nycklar ska vara AES-nycklar, med en nyckellängd som är lika med längden på rörelsesensorns huvudnyckel, som ska vara kopplad till längden på det (förväntade) europeiska rotnyckelparet enligt beskrivningen i CSM_50.

Tabell 3

Nycklar för att säkra kommunikation mellan fordonsenhet och rörelsesensor

Nycklar	Symbol	Genererad av	Genereringsmetod	Lagras av
Huvudnyckel för rörelsesensor – fordonsenhetsdelen	$K_{M\text{-}VU}$	Erca	Slumpmässig	Erca, medlemsstaternas certifieringsinstanser (MSCA) som är involverade i utfärdandet av certifikat för fordonsenheter, tillverkare av fordonsenheter, fordonsenheter
Huvudnyckel för rörelsesensor – verkstadsdelen	$K_{M\text{-}WC}$	Erca	Slumpmässig	Erca, medlemsstaternas certifieringsinstanser (MSCA), korttillverkare, verkstadskort

▼B

Nycklar	Symbol	Genererad av	Genereringsmetod	Lagras av
Nycklar för rörelsesensorer	M	Ej självständigt genererad	Beräknas som $K_M = K_{M\text{-}VU}$ XOR $K_{M\text{-}WC}$	Erca, medlemsstaternas certifieringsinstanser som är involverade i utfärdandet av nycklar för rörelsesensorer (frivilligt) (*)
Identifieringsnyckel	K_{ID}	Ej självständigt genererad	Beräknas som $K_{ID} = K_M$ XOR CV, där CV specificeras i CSM_106	Erca, medlemsstaternas certifieringsinstanser som är involverade i utfärdandet av nycklar för rörelsesensorer (frivilligt) (*)
Parningsnyckel	K_P	Gränssnitt för rörelsesensorer	Slumpmässig	Inbyggd rörelsesensor
Sessionsnyckel	K_S	Fordonsenhet (vid parning av fordonsenhet och rörelsesensor)	Slumpmässig	En fordonsenhet och en rörelsesensor

(*) Lagring av K_M och K_{ID} är frivillig, eftersom dessa nycklar kan härledas från $K_{M\text{-}VU}$, $K_{M\text{-}WC}$ och CV (*Constant Vector*).

CSM_101 Europeiska rotcertifieringsinstansen (Erca) ska generera $K_{M\text{-}VU}$ och $K_{M\text{-}WC}$, två slumpmässigt genererade och unika AES-nycklar från vilka rörelsesensorns huvudnyckel K_M kan beräknas som $K_{M\text{-}VU}$ XOR $K_{M\text{-}WC}$. Erca ska överlämna K_M, $K_{M\text{-}VU}$ och $K_{M\text{-}WC}$ till certifieringsinstanser i medlemsstaterna (MSCA) på de sistnämndas begäran.

CSM_102 Erca ska tilldela varje rörelsesensors huvudnyckel K_M ett unikt versionsnummer, som också ska gälla för de i krypteringen ingående nycklarna $K_{M\text{-}VU}$ och $K_{M\text{-}WC}$ och för tillhörande identifieringsnyckel K_{ID}. Erca ska informera medlemsstaternas certifieringsinstanser (MSCA) om versionsnumret när Erca skickar $K_{M\text{-}VU}$ och $K_{M\text{-}WC}$ till dem.

Anmärkning: Versionsnumret används för att göra åtskillnad mellan olika generationer av dessa nycklar (se detaljerad förklaring i avsnitt 9.2.1.2).

CSM_103 En medlemsstats certifieringsinstans (MSCA) ska överlämna $K_{M\text{-}VU}$, tillsammans med dess versionsnummer, till fordonsenhetstillverkare på de sistnämndas begäran. Fordonsenhetstillverkarna ska installera $K_{M\text{-}VU}$ och dess versionsnummer i alla tillverkade fordonsenheter.

CSM_104 En certifieringsinstans i medlemsstaten ska säkerställa att $K_{M\text{-}WC}$, tillsammans med dess versionsnummer, installeras i varje verkstadskort som utfärdas under dess ansvar.

Anmärkningar:

— Se beskrivningen av datatypen `SensorInstallationSecData` i tillägg 2.

— Såsom förklaras i avsnitt 9.2.1.2 kan det i praktiken behöva installeras flera generationer av $K_{M\text{-}WC}$ i ett enda verkstadskort.

▼B

CSM_105 Utöver den AES-nyckel som specificeras i CSM_104 ska en medlemsstats certifieringsinstans (MSCA) säkerställa att TDES-nyckeln $Km_{WC,}$ som specificeras i krav CSM_037 i del A i detta tillägg, installeras i varje verkstadskort som utfärdas under dess ansvar.

Anmärkningar:

— Detta gör det möjligt att använda ett andra generationens verkstadskort för koppling av en första generationens fordonsenhet.

— Ett andra generationens verkstadskort kommer att innehålla två olika tillämpningar: en som uppfyller kraven i del B i detta tillägg och en som uppfyller kraven i del A. Den sistnämnda kommer att innehålla TDES-nyckeln $Km_{WC.}$

CSM_106 En medlemsstats certifieringsinstans (MSCA) som deltar i utfärdandet av rörelsesensorer ska härleda identifieringsnyckeln från rörelsesensorns huvudnyckel med hjälp av en XOR-operation med huvudnyckeln och en konstant vektor (CV) som de båda termerna. Värdet av den konstanta vektorn CV ska vara följande:

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

— För 192-bits huvudnycklar för rörelsesensor: CV = ‘72 AD EA FA 00 BB F4 EE F4 99 15 70 5B 7E EE BB 1C 54 ED 46 8B 0E F8 25’

— För 256-bits huvudnycklar för rörelsesensor: CV = ‘1D 74 DB F0 34 C7 37 2F 65 55 DE D5 DC D1 9A C3 23 D6 A6 25 64 CD BE 2D 42 0D 85 D2 32 63 AD 60’

Anmärkning: De konstanta vektorerna har genererats på följande sätt:

Pi_10 = de första 10 byte av decimaldelen i den matematiska konstanten π = ‘24 3F 6A 88 85 A3 08 D3 13 19’

CV_128-bits = första 16 byte av SHA-256(Pi_10)

CV_192-bits = första 24 byte av SHA-384(Pi_10)

CV_256-bits = första 32 byte av SHA-512(Pi_10)

CSM_107 Rörelsesensortillverkare ska generera en slumpmässig och unik parningsnyckel K_P för varje rörelsesensor, och ska överlämna varje parningsnyckel till en medlemsstats certifieringsinstans. Medlemsstatens certifieringsinstans ska kryptera varje parningsnyckel separat med rörelsesensorns huvudnyckel K_M och ska återsända den krypterade nyckeln till rörelsesensortillverkaren. För varje krypterad nyckel ska MSCA meddela rörelsesensortillverkaren versionsnumret för tillhörande K_M.

Anmärkning: Såsom förklaras i avsnitt 9.2.1.2 kan en rörelsesensortillverkare i praktiken behöva generera flera unika parningsnycklar för en enda rörelsesensor.

▼B

CSM_108 Rörelsesensortillverkare ska generera ett unikt serienummer för varje rörelsesensor, och ska överlämna alla serienummer till en medlemsstats certifieringsinstans. Medlemsstatens certifieringsinstans ska kryptera varje serienummer separat med identifieringsnyckeln K_{ID} och ska återsända det krypterade serienumret till rörelsesensortillverkaren. För varje krypterat serienummer ska MSCA meddela rörelsesensortillverkaren versionsnumret för tillhörande K_{ID}.

CSM_109 För kraven CSM_107 och CSM_108 ska MSCA använda AES-algoritmen i CBC-läge (*Cipher Block Chaining*), såsom definieras i [ISO 10116], med en *interleave*-parameter $m = 1$ och en initialiseringsvektor SV = '00' {16}, dvs. 16 byte med binärt värde 0. När det är nödvändigt ska MSCA använda utfyllnadsmetod 2 som definieras i [ISO 9797-1].

CSM_110 Rörelsesensortillverkaren ska lagra den krypterade parningsnyckeln och det krypterade serienumret i den avsedda rörelsesensorn, tillsammans med motsvarande klartextvärden och versionsnumret för K_M och K_{ID} som används för kryptering.

Anmärkning: Såsom förklaras i avsnitt 9.2.1.2 kan en rörelsesensortillverkare i praktiken behöva installera flera krypterade parningsnycklar och flera krypterade serienummer i en enda rörelsesensor.

CSM_111 Utöver de AES-baserade krypteringsuppgifter som specificeras i CSM_110 kan en rörelsesensortillverkare också lagra, i varje rörelsesensor, de TDES-baserade krypteringsuppgifter som specificeras i krav CSM_037 i del A i detta tillägg.

Anmärkning: Detta kommer att göra det möjligt att koppla en andra generationens rörelsesensor till en första generationens fordonsenhet.

CSM_112 Längden på sessionsnyckeln K_S, som genereras av en fordonsenhet vid parningen med en rörelsesensor, ska kopplas till längden på dess $K_{M\text{-}VU,}$ enligt beskrivningen i CSM_50.

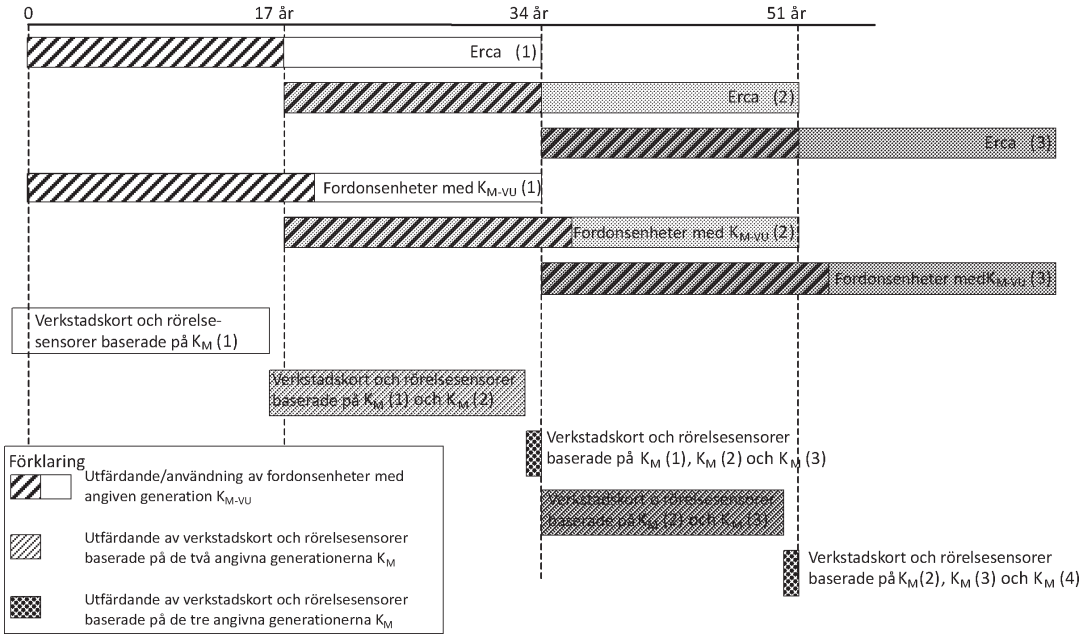
9.2.1.2 *Utbyte av rörelsesensorns huvudnyckel i andra generationens utrustning*

CSM_113 Varje huvudnyckel för en rörelsesensor och alla relaterade nycklar (se Table 3) är förbundna med en viss generation av Erca-rotnyckelparet. Dessa nycklar ska därför bytas ut vart 17:e år. Giltighetsperioden för varje generation av huvudnyckel för en rörelsesensor ska börja ett år innan det därmed förbundna Erca-rotnyckelparet blir giltigt och ska sluta när Erca-rotnyckelparet upphör att vara giltigt. Detta illustreras i Figure 2.

▼B

Figur 2

Utfärdande och användning av olika generationer av rörelsesensorns huvudnyckel i fordonsenheter, rörelsesensorer och verkstadskort



CSM_114 Minst ett år innan Erca genererar ett nytt europeiskt rotnyckelpar, såsom beskrivs i CSM_56, ska Erca generera en ny huvudnyckel K_M för rörelsesensorer genom att generera en ny K_{M-VU} och K_{M-WC}. Längden på rörelsesensorns huvudnyckel ska vara kopplad till den förutsedda styrkan hos det nya europeiska rotnyckelparet, i enlighet med CSM_50. Erca ska överlämna de nya K_M, K_{M-VU} och K_{M-WC}, tillsammans med deras versionsnummer, till medlemsstaternas certifieringsinstanser på deras begäran.

CSM_115 En MSCA ska säkerställa att alla giltiga generationer av K_{M-WC} lagras i varje verkstadskort som utfärdats under dess ansvar, tillsammans med deras versionsnummer, såsom visas i Figure 2.

Anmärkning: Detta innebär att verkstadskort, under det sista året av ett Erca-certifikats giltighetsperiod, kommer att utfärdas med tre olika generationer av K_{M-WC}, såsom visas i Figure 2.

CSM_116 Vad gäller den process som beskrivs i CSM_107 och CSM_108 ovan: En MSCA ska kryptera varje parningsnyckel K_P som den tar emot från en rörelsesensortillverkare separat med varje giltig generation av rörelsesensorns huvudnyckel K_M. En MSCA ska också kryptera varje serienummer som den tar emot från en rörelsesensortillverkare separat med varje giltig generation av identifieringsnyckeln K_{ID}. En rörelsesensortillverkare ska lagra alla krypteringar av parningsnyckeln och alla krypteringar av serienumret i den avsedda rörelsesensorn, tillsammans med motsvarande klartextvärden och versionsnumret/versionsnumren för K_M och K_{ID} som används för kryptering.

▼B

Anmärkning: Detta innebär att rörelsesensorer, under det sista året av ett Erca-certifikats giltighetsperiod, kommer att utfärdas med krypterade data baserade på tre olika generationer av K_M, såsom visas i Figure 2.

CSM_117 Vad gäller den process som beskrivs i CSM_107 ovan: Eftersom längden på parningsnyckeln K_P ska vara kopplad till längden på K_M (se CSM_100), kan en rörelsesensortillverkare behöva generera upp till tre olika parningsnycklar (med olika längder) för en rörelsesensor, om på varandra följande generationer av K_M har olika längder. I sådana fall ska tillverkaren överlämna varje parningsnyckel till MSCA. MSCA ska säkerställa att varje parningsnyckel krypteras med korrekt generation av rörelsesensorns huvudnyckel, dvs. den som har samma längd.

Anmärkning: Om rörelsesensortillverkaren väljer att generera en TDES-baserad parningsnyckel för en andra generationens rörelsesensor (se CSM_111), ska tillverkaren meddela MSCA att rörelsesensorns TDES-baserade huvudnyckel måste användas för kryptering av denna parningsnyckel. Detta beror på att längden på en TDES-nyckel kan vara lika med längden på en AES-nyckel, så att MSCA inte kan göra en bedömning på grundval av enbart nyckellängden.

CSM_118 Fordonsenhetstillverkare ska installera endast en generation av $K_{M\text{-}VU}$ i varje fordonsenhet, tillsammans med dess versionsnummer. Denna $K_{M\text{-}VU}$-generation ska vara kopplad till det Erca-certifikat som ligger till grund för fordonsenhetens certifikat.

Anmärkningar:

— En fordonsenhet som är baserad på generation *X* av Erca-certifikatet ska innehålla endast generation *X* av $K_{M\text{-}VU,}$ även om det är utfärdat efter det att giltighetsperioden för generation *X+1* av Erca-certifikatet har börjat. Detta visas i Figure 2.

— En fordonsenhet av generation *X* kan inte paras med en rörelsesensor av generation *X-1*.

— Eftersom verkstadskort har en giltighetsperiod på ett år är resultatet av CSM_113–CSM_118 att alla verkstadskort kommer att innehålla den nya $K_{M\text{-}WC}$ vid tidpunkten för utfärdandet av den första fordonsenheten som innehåller den nya $K_{M\text{-}VU}$. Därför kommer en sådan fordonsenhet alltid att kunna beräkna den nya K_M. Vid den tidpunkten kommer dessutom de flesta nya rörelsesensorer att innehålla även krypterade data som är baserade på den nya $K_{M.}$

9.2.2 *Nycklar för att säkra DSRC-kommunikation*

9.2.2.1 *Allmänt*

CSM_119 Autenticiteten och sekretessen avseende data som överlämnas från en fordonsenhet till en kontrollmyndighet via en fjärrkommunikationskanal i form av DSRC ska säkerställas med hjälp av en uppsättning AES-nycklar som är specifika för fordonsenheten och som härleds från en enda DSRC-huvudnyckel – KM_{DSRC}.

▼B

CSM_120 DSRC-huvudnyckeln KM_{DSRC} ska vara en AES-nyckel som på ett säkert sätt genereras, lagras och distribueras av Erca. Nyckellängden kan vara 128, 192 eller 256 bitar och ska vara kopplad till längden på det europeiska rotnyckelparet, såsom beskrivs i CSM_50.

CSM_121 Erca ska på ett säkert sätt överlämna DSRC-huvudnyckeln till certifieringsinstanser i medlemsstaterna på de sistnämndas begäran, för att göra det möjligt för dem att härleda DSRC-nycklar som är specifika för fordonsenheten och för att säkerställa att DSRC-huvudnyckeln installeras i alla kontrollkort och verkstadskort som utfärdas under deras ansvar.

CSM_122 Erca ska tilldela varje DSRC-huvudnyckel ett unikt versionsnummer. Erca ska informera medlemsstaternas certifieringsinstanser (MSCA) om versionsnumret när Erca skickar DSRC-huvudnyckeln till dem.

Anmärkning: Versionsnumret används för att göra åtskillnad mellan olika generationer av DSRC-huvudnyckeln (se detaljerad förklaring i avsnitt 9.2.2.2).

CSM_123 För varje fordonsenhet ska fordonsenhetstillverkaren skapa ett unikt serienummer och översända detta nummer till sin certifieringsinstans i medlemsstaten i en förfrågan om att få en uppsättning med två DSRC-nycklar som är specifika för fordonsenheten. Fordonsenhetens serienummer ska ha datatypen `VuSerialNumber`, och DER (*Distinguished Encoding Rules*) enligt [ISO 8825-1] ska användas för kodning.

CSM_124 Efter att ha tagit emot en förfrågan om specifika DSRC-nycklar för fordonsenheten ska MSCA härleda två AES-nycklar för fordonsenheten, benämnda $K_VU_{DSRC}_ENC$ och $K_VU_{DSRC}_MAC$. Dessa specifika nycklar för fordonsenheten ska ha samma längd som DSRC-huvudnyckeln. MSCA ska använda den funktion för nyckelhärledning som definieras i [RFC 5869]. Den hashfunktion som krävs för att instansiera HMAC-Hash-funktionen ska länkas till längden för DSRC-huvudnyckeln, såsom beskrivs i CSM_50. Funktionen för nyckelhärledning i [RFC 5869] ska användas på följande sätt:

Steg 1 (*Extract*):

— *PRK* = HMAC-Hash (*salt, IKM*) där *salt* är en tom sträng ‘’ och *IKM* är KM_{DSRC}.

Steg 2 (*Expand*):

— *OKM = T(1)*, där

T(1) = HMAC-Hash (*PRK*, *T(0)* || *info* || ‘01’) med

▼B

— *T(0)* = en tom sträng (‘’),

— *info* = fordonsenhetens serienummer såsom det anges i CSM_123,

— $K_VU_{DSRC}_ENC$ = de första *L* oktetterna i *OKM* och

$K_VU_{DSRC}_MAC$ = de sista *L* oktetterna i *OKM*

där *L* är den längd som krävs för $K_VU_{DSRC}_ENC$ och $K_VU_{DSRC}_MAC$ (i oktetter).

CSM_125 MSCA ska på ett säkert sätt distribuera $K_VU_{DSRC}_ENC$ och $K_VU_{DSRC}_MAC$ till fordonsenhetstillverkaren så att de kan installeras i den avsedda fordonsenheten.

CSM_126 Vid utfärdandet ska en fordonsenhet ha lagrat $K_VU_{DSRC}_ENC$ och $K_VU_{DSRC}_MAC$ i sitt skyddade minne, så att den kan säkerställa integritet, autenticitet och sekretess avseende data som översänds via fjärrkommunikationskanalen. En fordonsenhet ska också lagra versionsnumret för den DSRC-huvudnyckel som används för att härleda dessa nycklar som är specifika för fordonsenheten.

CSM_127 Vid utfärdandet ska kontrollkort och verkstadskort ha lagrat KM_{DSRC} i sitt skyddade minne, så att de kan verifiera integriteten och autenticiteten avseende data som översänds av en fordonsenhet via fjärrkommunikationskanalen och så att de kan dekryptera dessa data. Kontrollkort och verkstadskort ska också lagra DSRC-huvudnyckelns versionsnummer.

Såsom förklaras i avsnitt 9.2.2.2 kan det i praktiken behöva installeras flera generationer av KM_{DSRC} i ett enda verkstadskort eller kontrollkort.

CSM_128 MSCA ska föra ett register över alla fordonsenhetsspecifika DSRC-nyckar som den har genererat, tillsammans med deras versionsnummer och identifiering av den fordonsenhet för vilken varje nyckeluppsättning är avsedd.

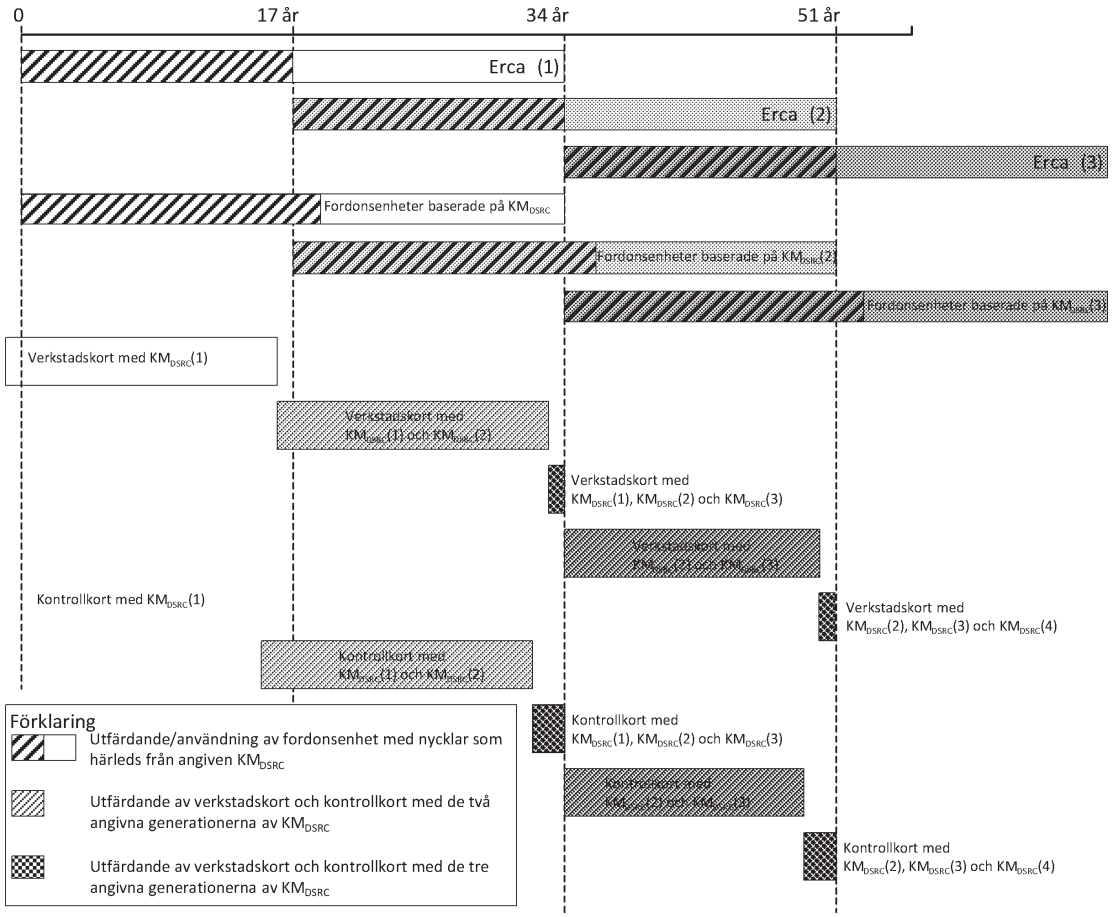
9.2.2.2 *Utbyte av DSRC-huvudnyckel*

CSM_129 Varje DSRC-huvudnyckel är förbunden med en viss generation av Erca-rotnyckelparet. Erca ska därför byta ut DSRC-huvudnyckeln vart 17:e år. Giltighetsperioden för varje generation av DSRC-huvudnyckel ska börja två år innan det därmed förbundna Erca-rotnyckelparet blir giltigt och ska sluta när Erca-rotnyckelparet upphör att vara giltigt. Detta illustreras i Figure 3.

▼B

Figur 3

Utfärdande och användning av olika generationer av DSRC-huvudnyckeln i fordonsenheter, verkstadskort och kontrollkort



CSM_130 Minst två år innan Erca genererar ett nytt europeiskt rotnyckelpar, såsom beskrivs i CSM_56, ska Erca generera en ny DSRC-huvudnyckel. Längden på DSRC-nyckeln ska vara kopplad till den förutsedda styrkan hos det nya europeiska rotnyckelparet, i enlighet med CSM_50. Erca ska överlämna den nya DSRC-huvudnyckeln, tillsammans med dess versionsnummer, till medlemsstaternas certifieringsinstanser på deras begäran.

CSM_131 En MSCA ska säkerställa att alla giltiga generationer av KM_{DSRC} lagras i varje kontrollkort som utfärdats under dess ansvar, tillsammans med deras versionsnummer, såsom visas i Figure 3.

Anmärkning: Detta innebär att kontrollkort, under de sista två åren av ett Erca-certifikats giltighetsperiod, kommer att utfärdas med tre olika generationer av KM_{DSRC}, såsom visas i Figure 3.

CSM_132 En MSCA ska säkerställa att alla generationer av KM_{DSRC} som har varit giltiga i minst ett år och som fortfarande är giltiga lagras i varje verkstadskort som utfärdats under dess ansvar, tillsammans med deras versionsnummer, såsom visas i Figure 3.

▼B

Anmärkning: Detta innebär att verkstadskort, under det sista året av ett Erca-certifikats giltighetsperiod, kommer att utfärdas med tre olika generationer av KM_{DSRC}, såsom visas i Figure 3.

CSM_133 Fordonsenhetstillverkare ska installera endast en uppsättning fordonsenhetsspecifika DSRC-nycklar i varje fordonsenhet, tillsammans med dess versionsnummer. Denna nyckeluppsättning ska härledas från den KM_{DSRC}-generation som är kopplad till det Erca-certifikat som ligger till grund för fordonsenhetens certifikat.

Anmärkningar:

— Detta innebär att en fordonsenhet som är baserad på generation *X* av Erca-certifikatet ska innehålla endast generation *X* av K_VU_{DSRC}_ENC och K_VU_{DSRC}_MAC, även om fordonsenheten utfärdas efter det att giltighetsperioden för generation *X+1* av Erca-certifikatet har börjat. Detta visas i Figure 3.

— Eftersom verkstadskort har en giltighetsperiod på ett år och kontrollkort en giltighetsperiod på två år, är resultatet av CSM_131–CSM_133 att alla verkstadskort och kontrollkort kommer att innehålla den nya DSRC-huvudnyckeln vid tidpunkten för utfärdandet av den första fordonsenheten som innehåller fordonsenhetsspecifika nycklar som är baserade på den huvudnyckeln.

9.3. **Certifikat**

9.3.1 *Allmänt*

CSM_134 Alla certifikat i det europeiska smarta färdskrivarsystemet ska vara självbeskrivande (*self-descriptive*), kortverifierbara (CV, *card-verifiable*) certifikat i enlighet med [ISO 7816-4] och [ISO 7816-8].

CSM_135 DER (*Distinguished Encoding Rules*) enligt [ISO 8825-1] ska användas för att koda både ASN.1-datastrukturer och (tillämpningsspecifika) dataobjekt inom certifikat.

Anmärkning: Denna kodning resulterar i en TLV-struktur (*Tag-Length-Value*) enligt följande:

Tagg: Taggen är kodad i en eller två oktetter och anger innehållet.

Längd: Längden kodas som ett heltal utan tecken i en, två eller tre oktetter, vilket resulterar i den maximala längden 65 535 oktetter. Det minsta antalet oktetter ska användas.

Värde: Värdet kodas i noll eller fler oktetter.

9.3.2 *Certifikatens innehåll*

CSM_136 Alla certifikat ska ha den struktur som visas i certifikatprofilen i Table 4.

Tabell 4

Certifikatprofil version 1

Fält	Fält-ID	Tagg	Längd (byte)	Datatyp i ASN.1 (se tillägg 1)
ECC-certifikat	C	‘7F 21’	var	
ECC Certificate Body	B	7F	var	

▼B

Fält	Fält-ID	Tagg	Längd (byte)	Datatyp i ASN.1 (se tillägg 1)
Certificate Profile Identifier (identifierare för certifikatprofil)	CPI	‘5F 29’	‘01’	`INTEGER(0..255)`
Certificate Authority Reference (certifieringsinstansens referens)	CAR	‘42’	‘08’	`KeyIdentifier`
Certificate Holder Authorisation (certifikatinnehavarens auktorisering)	CHA	‘5F 4C’	‘07’	`CertificateHolder Authorisation`
Public Key (öppen nyckel)	PK	‘7F 49’	var	
Domain Parameters (domänparametrar)	DP	‘06’	var	`OBJECT IDENTIFIER`
Public Point (öppen punkt)	PP	‘86’	var	`OCTET STRING`
Certificate Holder Reference (certifikatinnehavarens referens)	CHR	‘5F 20’	‘08’	`KeyIdentifier`
Certificate Effective Date (certifikatets första giltighetsdag)	CEfD	‘5F 25’	‘04’	`TimeReal`
Certificate Expiration Date (certifikatets sista giltighetsdag)	CExD	‘5F 24’	‘04’	`TimeReal`
ECC Certificate Signature	S	‘5F 37’	var	`OCTET STRING`

Anmärkning: Fält-ID kommer att användas i senare avsnitt i detta tillägg för att ange enskilda fält i ett certifikat (exempelvis är X.CAR den *Certificate Authority Reference* som nämns i certifikatet för användare X).

9.3.2.1 Certificate Profile Identifier (identifierare för certifikatprofil)

CSM_137 Certifikat ska använda en identifierare för certifikatprofil (*Certificate Profile Identifier*) för att ange vilken certifikatprofil som används. Version 1, enligt specifikationen i Table 4, ska identifieras med värdet ‘00’.

9.3.2.2 Certificate Authority Reference (certifieringsinstansens referens)

CSM_138 Certifieringsinstansens referens ska användas för att identifiera den öppna nyckel som ska användas för att verifiera certifikatsignaturen. Certifieringsinstansens referens ska därför vara identisk med certifikatinnehavarens referens i certifikatet från motsvarande certifieringsinstans.

CSM_139 Ett Erca-rotcertifikat ska vara självsignerat, dvs. certifieringsinstansens referens (CAR) och certifikatinnehavarens referens (CHR) i certifikatet ska vara identiska.

▼B

CSM_140 För ett Erca-länkcertifikat ska certifikatinnehavarens referens (CHR) vara identisk med CHR i det nya Erca-rotcertifikatet. Certifieringsinstansens referens (CAR) för ett länkcertifikat ska vara identisk med CHR i föregående Erca-rotcertifikat.

9.3.2.3 Certificate Holder Authorisation (certifikatinnehavarens auktorisering)

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.

9.3.2.4 Public Key (öppen nyckel)

Den öppna nyckeln innehåller två dataelement: de standardiserade domänparametrar som ska användas med den öppna nyckeln i certifikatet och värdet på den öppna punkten (*public point*).

CSM_142 Dataelementet *Domain Parameters* ska innehålla en av de objektidentifierare som specificeras i Table 1 som referens till en uppsättning standardiserade domänparametrar.

CSM_143 Dataelementet *Public Point* ska innehålla den öppna punkten. Öppna punkter på en elliptisk kurva (*elliptic curve public points*) ska omvandlas till oktettsträngar i enlighet med [TR-03111]. Det okomprimerade kodningsformatet ska användas. När en punkt på en elliptisk kurva (*elliptic curve point*) återskapas från sitt kodade format ska de valideringar som beskrivs i [TR-03111] alltid utföras.

9.3.2.5 Certificate Holder Reference (certifikatinnehavarens referens)

CSM_144 Certifikatinnehavarens referens är en identifierare för den öppna nyckel som tillhandahålls i certifikatet. Den ska användas i andra certifikat som referens till denna öppna nyckel.

CSM_145 När det gäller certifikat för kort och externa GNSS-anordningar ska certifikatinnehavarens referens ha datatyp `ExtendedSerialNumber` som specificeras i tillägg 1.

CSM_146 När en tillverkare efterfrågar certifikat för fordonsenheter är det tillverkarspecifika serienumret för den fordonsenhet för vilken certifikatet och tillhörande privata nyckel är avsedda antingen känt eller inte känt. I det första fallet ska certifikatinnehavarens referens ha datatyp `ExtendedSerialNumber` som specificeras i tillägg 1. I det senare fallet ska certifikatinnehavarens referens ha datatyp `CertificateRequestID` som specificeras i tillägg 1.

CSM_147 När det gäller Erca- och MSCA-certifikat ska certifikatinnehavarens referens ha datatypen `CertificationAuthorityKID` som specificeras i tillägg 1.

▼B

9.3.2.6 Certificate Effective Date (certifikatets första giltighetsdag)

CSM_148 Certifikatets första giltighetsdag anger startdatum och starttidpunkt för certifikatets giltighetsperiod. Certifikatets första giltighetsdag ska vara certifikatgenerationens datum.

9.3.2.7 Certificate Expiration Date (certifikatets sista giltighetsdag)

CSM_149 Certifikatets sista giltighetsdag anger slutdatum och sluttidpunkt för certifikatets giltighetsperiod.

9.3.2.8 Certificate Signature (certifikatsignatur)

CSM_150 Signaturen på certifikatet ska skapas för den kodade nyttodelen av certifikatet (*certificate body*), inklusive tagg och längd för denna. Signeringsalgoritmen ska vara ECDSA såsom den specificeras i [DSS], med användning av den hashalgoritm som är länkad till nyckelstorleken för den signerande instansen, såsom anges i CSM_50. Signaturformatet ska vara i klartext, såsom anges i [TR-03111].

9.3.3 *Förfrågan om certifikat*

CSM_151 I samband med förfrågan om ett certifikat ska sökanden skicka följande data till sin certifieringsinstans:

— Identifierare för certifikatprofil (*Certificate Profile Identifier*) för det begärda certifikatet.

— Certifieringsinstansens referens (CAR) som förväntas användas för signering av certifikatet.

— Den öppna nyckel (*Public Key*) som ska signeras.

CSM_152 Utöver de data som finns i CSM_151 ska en MSCA översända följande data i en certifikatförfrågan till Erca, vilket gör det möjligt för Erca att skapa certifikatinnehavarens referens (*Certificate Holder Reference*) för det nya MSCA-certifikatet:

— Certifieringsinstansens numeriska landskod (datatypen `NationNumeric`, definierad i tillägg 1).

— Certifieringsinstansens alfanumeriska landskod (datatypen `NationAlpha`, definierad i tillägg 1).

— Serienummer (1 byte) för att skilja certifieringsinstansens olika nycklar åt om man byter nycklar.

— Det fält (bestående av två byte) som innehåller ytterligare information som är specifik för certifieringsinstansen.

CSM_153 Utöver de data som finns i CSM_151 ska en utrustningstillverkare översända följande data i en certifikatförfrågan till MSCA, vilket gör det möjligt för MSCA att skapa certifikatinnehavarens referens (*Certificate Holder Reference*) för det nya utrustningscertifikatet:

— En tillverkarspecifik identifierare för utrustningstypen.

— 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.

▼B

— 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.

CSM_154 När en tillverkare efterfrågar certifikat för en fordonsenhet är det tillverkarspecifika serienumret för den fordonsenhet för vilken certifikatet och tillhörande privata nyckel är avsedda antingen känt eller inte känt. Om det är känt ska tillverkaren av fordonsenheten översända serienumret till MSCA. Om det inte är känt ska tillverkaren unikt identifiera varje certifikatförfrågan och översända detta serienummer för certifikatförfrågan till MSCA. Det utfärdade certifikatet kommer då att innehålla serienumret för certifikatförfrågan. Efter att ha installerat certifikatet i en specifik fordonsenhet ska tillverkaren underrätta MSCA om kopplingen mellan serienumret för certifikatförfrågan och identifieringen av fordonsenheten.

10. ÖMSESIDIG AUTENTISERING OCH SÄKER MEDDELANDEHANTERING MELLAN FORDONSENHET OCH KORT

10.1. **Allmänt**

CSM_155 På en hög nivå ska säker kommunikation mellan en fordonsenhet och ett färdskrivarkort vara baserad på följande steg:

— För det första ska varje part demonstrera för den andra att den äger ett giltigt certifikat för öppen nyckel, vilket ska vara signerat av en certifieringsinstans i en medlemsstat. Vidare måste certifieringsinstansens certifikat för öppen nyckel vara signerat av den europeiska rotcertifieringsinstansen. Detta steg kallas verifiering av certifikatskedja och specificeras i detalj i avsnitt 10.2.

— För det andra ska fordonsenheten demonstrera för kortet att den äger den privata nyckel som motsvarar den öppna nyckeln i det certifikat som överlämnas. Den gör detta genom att signera ett slumptal som översänds av kortet. Kortet verifierar signaturen för slumptalet. Om verifieringen lyckas är fordonsenheten autentiserad. Detta steg kallas autentisering av fordonsenhet och specificeras i detalj i avsnitt 10.3.

— För det tredje beräknar båda parter var för sig två AES-sessionsnycklar med hjälp av en asymmetrisk algoritm för nyckelöverenskommelse. Genom att använda en av dessa sessionsnycklar skapar kortet en kod för meddelandeautentisering (MAC, *Message Authentication Code*) för vissa data som översänds av fordonsenheten. Fordonsenheten verifierar MAC. Om verifieringen lyckas är kortet autentiserat. Detta steg kallas autentisering av kort och specificeras i detalj i avsnitt 10.4.

— För det fjärde ska fordonsenheten och kortet använda de överenskomna sessionsnycklarna för att säkerställa sekretess, integritet och autenticitet avseende alla utväxlade meddelanden. Detta steg kallas säker meddelandehantering och specificeras i detalj i avsnitt 10.5.

CSM_156 Den mekanism som beskrivs i CSM_155 ska utlösas av fordonsenheten när ett kort sätts in i en av dess kortplatser.

▼B

10.2. **Ömsesidig verifiering av certifikatskedja**

10.2.1 *Fordonsenhetens verifiering av kortets certifikatskedja*

CSM_157 Fordonsenheter ska använda det protokoll som visas i Figure 4 för att verifiera ett färdskrivarkorts certifikatskedja.

Anmärkningar till Figure 4:

— De kortcertifikat och öppna nycklar som nämns i figuren är de som används för ömsesidig autentisering. I avsnitt 9.1.5 betecknas dessa CARD_MA.

— De Card.CA-certifikat och öppna nycklar som nämns i figuren är de som används för signering av kortcertifikat, och detta anges i CAR för kortcertifikatet. I avsnitt 9.1.3 betecknas dessa MSCA_Card.

— Det Card.CA.EUR-certifikat som nämns i figuren är det europeiska rotcertifikat som anges i certifieringsinstansens referens (CAR) för Card.CA-certifikatet.

— Det Card.Link-certifikat som nämns i figuren är kortets länkcertifikat, om ett sådant finns. Såsom anges i avsnitt 9.1.2 är detta ett länkcertifikat för ett nytt europeiskt rotnyckelpar som skapats av Erca och signerats med den föregående europeiska privata nyckeln.

— Card.Link.EUR-certifikatet är det europeiska rotcertifikat som anges i certifieringsinstansens referens (CAR) för Card.Link-certifikatet.

CSM_158 Såsom illustreras i Figure 4 ska verifieringen av kortets certifikatskedja börja när kortet sätts in. Fordonsenheten ska läsa kortinnehavarens referens `cardExtendedSerialNumber` från EF ICC. Fordonsenheten ska kontrollera om den känner igen kortet, dvs. om den tidigare har lyckats verifiera kortets certifikatskedja och lagrat den för framtida behov. Om så är fallet, och kortcertifikatet fortfarande är giltigt, fortsätter processen med verifieringen av fordonsenhetens certifikatskedja. I andra fall ska fordonsenheten successivt läsa följande från kortet: MSCA_Card-certifikatet som ska användas för att verifiera kortcertifikatet, Card.CA.EUR-certifikatet som ska användas för att verifiera MSCA_Card-certifikatet, och eventuellt länkcertifikatet, tills den hittar ett certifikat den känner igen eller kan verifiera. Om ett sådant certifikat hittas ska fordonsenheten använda det för att verifiera de underliggande kortcertifikat som den har läst från kortet. Om detta lyckas fortsätter processen med verifieringen av fordonsenhetens certifikatskedja. Om detta inte lyckas ska fordonsenheten ignorera kortet.

▼B

Anmärkning: Det finns tre sätt på vilka fordonsenheten kan känna igen Card.CA.EUR-certifikatet:

— Card.CA.EUR-certifikatet är samma certifikat som fordonsenhetens eget EUR-certifikat.

— Card.CA.EUR-certifikatet föregår fordonsenhetens eget EUR-certifikat och fordonsenheten innehöll detta certifikat redan vid utfärdandet (se CSM_81).

— Card.CA.EUR-certifikatet kommer efter fordonsenhetens eget EUR-certifikat och fordonsenheten har tidigare mottagit ett länkcertifikat från ett annat färdskrivarkort, verifierat detta och lagrat det för framtida behov.

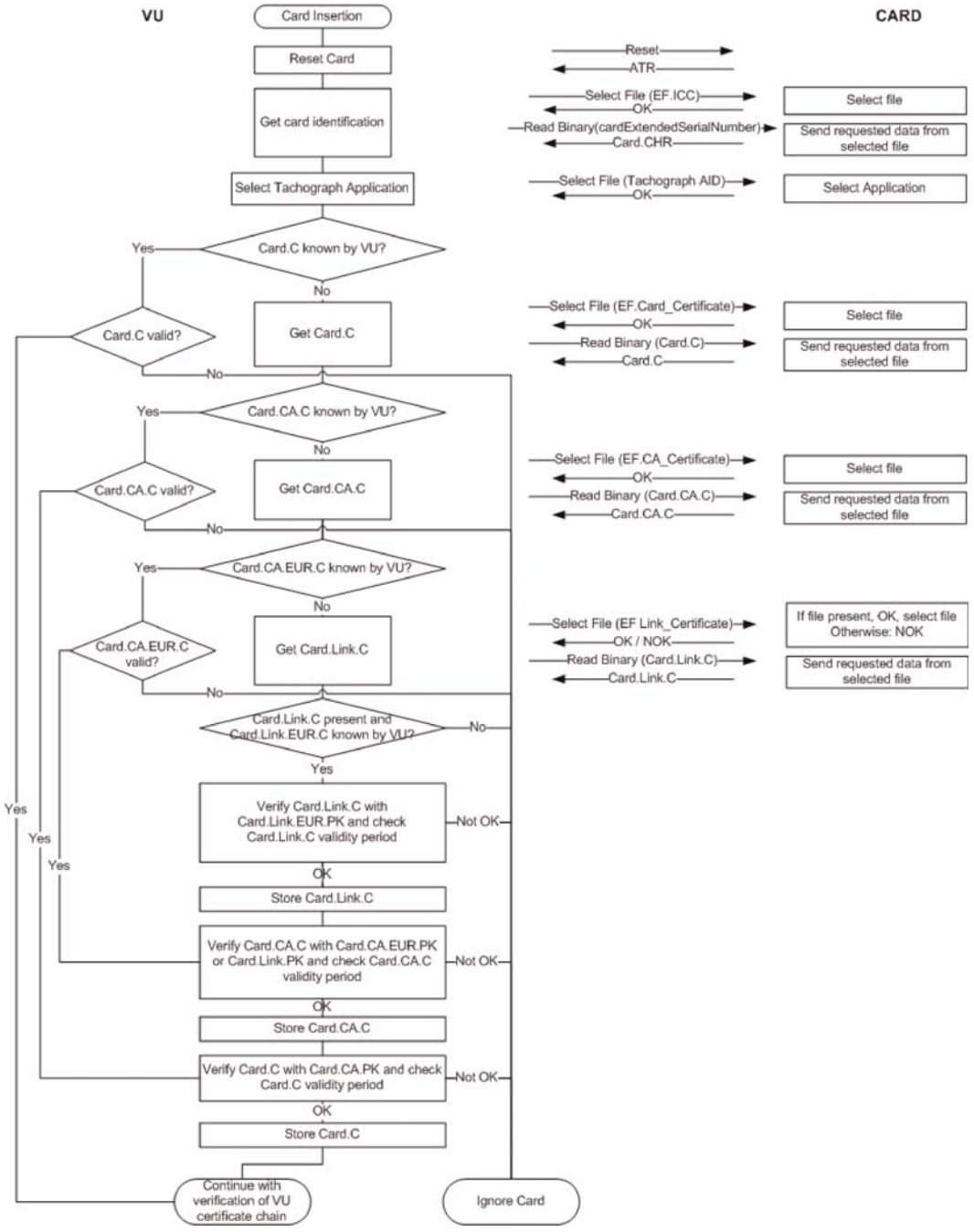
CSM_159 Såsom anges i Figure 4 får fordonsenheten, när den väl har verifierat autenticiteten och giltigheten hos ett tidigare okänt certifikat, lagra detta certifikat för framtida behov, så att den inte behöver verifiera certifikatets autenticitet igen om det överlämnas till fordonsenheten på nytt. I stället för att lagra hela certifikatet får en fordonsenhet välja att lagra endast innehållet i certifikatets nyttodel (*Certificate Body*), såsom specificeras i avsnitt 9.3.2.

CSM_160 Fordonsenheten ska verifiera den tidsmässiga giltigheten för alla certifikat som läses från kortet eller lagras i dess minne, och ska avvisa certifikat som löpt ut. För kontrollen av den tidsmässiga giltigheten hos ett certifikat som överlämnas av kortet ska en fordonsenhet använda sin interna klocka.

▼B

Figur 4

Protokoll för fordonsenhetens verifiering av kortets certifikatskedja



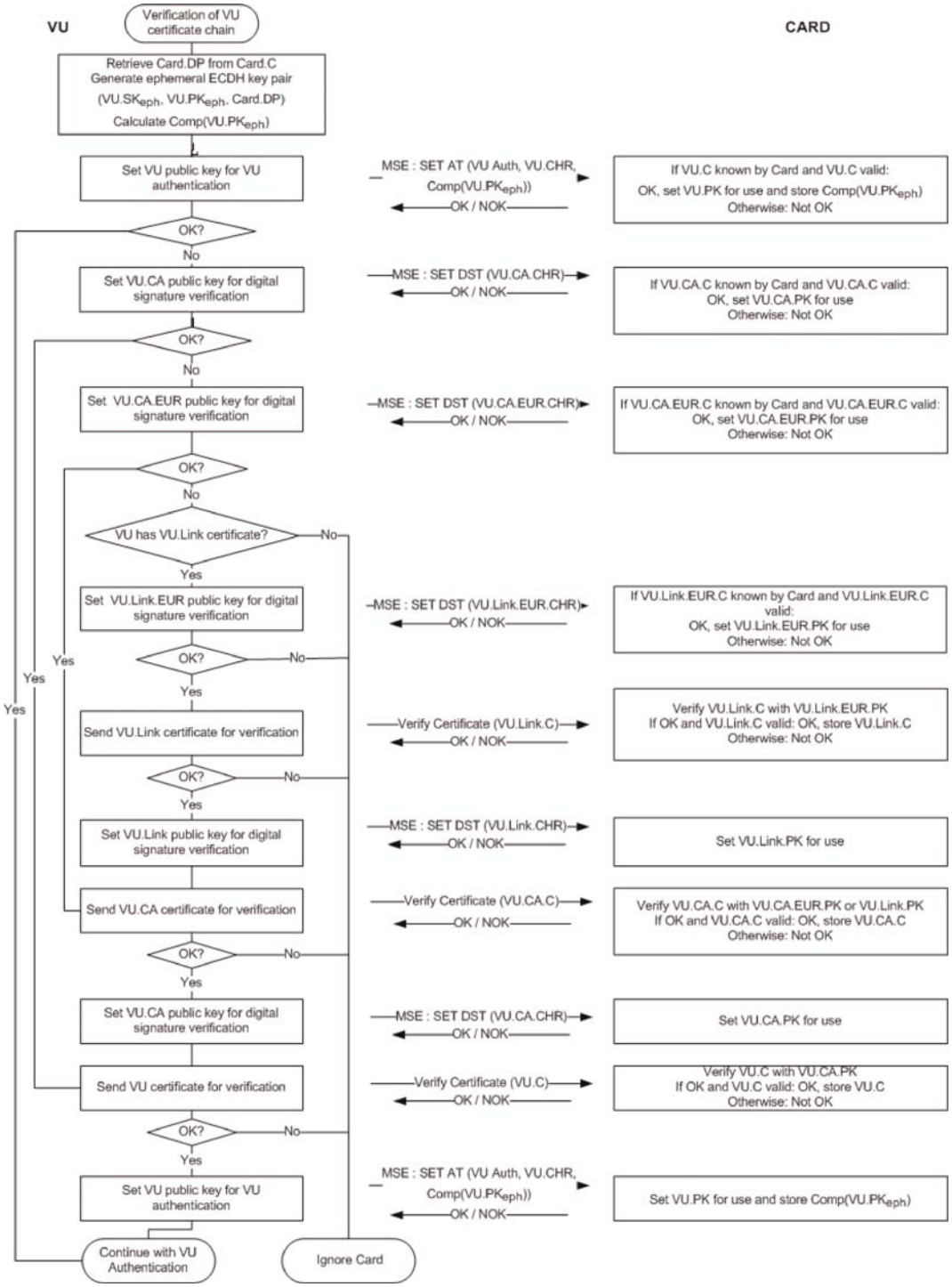
10.2.2 *Kortets verifiering av fordonsenhetens certifikatskedja*

CSM_161 Färdskrivarkort ska använda det protokoll som visas i Figure 5 för att verifiera en fordonsenhets certifikatskedja.

▼B

Figur 5

Protokoll för kortets verifiering av fordonsenhetens certifikatskedja



Anmärkningar till Figure 5:

— De fordonsenhetscertifikat och öppna nycklar som nämns i figuren är de som används för ömsesidig autentisering. I avsnitt 9.1.4 betecknas dessa VU_MA.

▼B

— De VU.CA-certifikat och öppna nycklar som nämns i figuren är de som används för signering av certifikat för fordonsenheter och externa GNSS-anordningar. I avsnitt 9.1.3 betecknas dessa MSCA_VU-EGF.

— Det VU.CA.EUR-certifikat som nämns i figuren är det europeiska rotcertifikat som anges i certifieringsinstansens referens (CAR) för VU.CA-certifikatet.

— Det VU.Link-certifikat som nämns i figuren är fordonsenhetens länkcertifikat, om ett sådant finns. Såsom anges i avsnitt 9.1.2 är detta ett länkcertifikat för ett nytt europeiskt rotnyckelpar som skapats av Erca och signerats med den föregående europeiska privata nyckeln.

— VU.Link.EUR-certifikatet är det europeiska rotcertifikat som anges i certifieringsinstansens referens (CAR) för VU.Link-certifikatet.

CSM_162 Såsom visas i Figure 5 ska verifieringen av fordonsenhetens certifikatskedja börja med att fordonsenheten försöker tillgängliggöra sin egen öppna nyckel för användning i färdskrivarkortet. Om detta lyckas innebär det att kortet tidigare har lyckats verifiera fordonsenhetens certifikatskedja och att kortet har lagrat fordonsenhetens certifikat för framtida bruk. I så fall tillgängliggörs fordonsenhetscertifikatet för användning, och processen fortsätter med autentisering av fordonsenhet. Om kortet inte känner igen fordonsenhetscertifikatet ska fordonsenheten successivt överlämna VU.CA-certifikatet som ska användas för att verifiera dess fordonsenhetscertifikat, VU.CA.EUR-certifikatet som ska användas för att verifiera VU.CA-certifikatet, och eventuellt länkcertifikatet, i syfte att hitta ett certifikat som kortet känner igen eller kan verifiera. Om ett sådant certifikat hittas ska kortet använda det för att verifiera de underliggande fordonsenhetscertifikat som överlämnas till kortet. Om detta lyckas ska fordonsenheten slutligen tillgängliggöra sin öppna nyckel för användning i färdskrivarkortet. Om detta inte lyckas ska fordonsenheten ignorera kortet.

Anmärkning: Det finns tre sätt på vilka kortet kan känna igen VU.CA.EUR-certifikatet:

— VU.CA.EUR-certifikatet är samma certifikat som kortets eget EUR-certifikat.

— VU.CA.EUR-certifikatet föregår kortets eget EUR-certifikat och kortet innehöll detta certifikat redan vid utfärdandet (se CSM_91).

— VU.CA.EUR-certifikatet kommer efter kortets eget EUR-certifikat och kortet har tidigare mottagit ett länkcertifikat från en annan fordonsenhet, verifierat detta och lagrat det för framtida behov.

CSM_163 Fordonsenheten ska använda kommandot MSE: SET AT för att tillgängliggöra sin öppna nyckel för användning i färdskrivarkortet. Såsom specificeras i tillägg 2 innehåller detta kommando en uppgift om vilken kryptografisk mekanism som kommer att användas med den nyckel som är inställd. Mekanismen ska vara ”autentisering av fordonsenheten med användning av ECDSA-algoritmen, i kombination med den hashalgoritm som är länkad till nyckelstorleken för fordonsenhetens VU_MA-nyckelpar, såsom anges i CSM_50”.

▼B

CSM_164 Kommandot MSE: SET AT innehåller också en uppgift om vilket tillfälligt nyckelpar som fordonsenheten kommer att använda i samband med överenskommelse om sessionsnyckel (se avsnitt 10.4). Innan kommandot MSE: SET AT skickas ska fordonsenheten därför generera ett tillfälligt ECC-nyckelpar. För att generera det tillfälliga nyckelparet ska fordonsenheten använda de standardiserade domänparametrar som anges i kortcertifikatet. Det tillfälliga nyckelparet betecknas ($VU.SK_{eph}$, $VU.PK_{eph}$, Card.DP). Fordonsenheten ska välja x-kordinaten för *ECDH ephemeral public point* som nyckelidentifiering; detta kallas den komprimerade representationen av den öppna nyckeln och betecknas $Comp(VU.PK_{eph})$.

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 $Comp(VU.PK_{eph})$. Om två eller flera lyckade MSE: Set AT-kommandon sänds innan överenskommelse om sessionsnyckel genomförs, ska kortet lagra endast senast mottagna $Comp(VU.PK_{eph})$.

CSM_166 Kortet ska verifiera den tidsmässiga giltigheten för alla certifikat som överlämnas av fordonsenheten eller som fordonsenheten refererar till medan de lagras i kortets minne, och ska avvisa certifikat som löpt ut.

CSM_167 För att verifiera den tidsmässiga giltigheten för ett certifikat som överlämnas av fordonsenheten ska varje färdskrivarkort internt lagra vissa data som betecknar aktuell tidpunkt. Dessa data ska inte vara direkt uppdaterbara för en fordonsenhet. Vid utfärdandet ska aktuell tid för ett kort ställas in så att den blir densamma som första giltighetsdag för kortets Card_MA-certifikat. Ett kort ska uppdatera sin aktuella tid om den första giltighetsdagen för ett autentiskt certifikat som utgör ”giltig tidskälla” och som överlämnas av en fordonsenhet anger en tidpunkt som infaller senare än kortets aktuella tid. I så fall ska kortet ställa in sin aktuella tid så att den blir den tid som anges som första giltighetsdag för det certifikatet. Kortet ska endast godta följande certifikat som en giltig tidskälla:

— Andra generationens Erca-länkcertifikat.

— Andra generationens MSCA-certifikat.

— Andra generationens fordonsenhetscertifikat som utfärdats av samma land som utfärdat kortets egna kortcertifikat (ett eller flera).

Anmärkning: Det sista kravet innebär att ett kort ska kunna känna igen CAR för fordonsenhetscertifikatet, dvs. MSCA_VU-EGF-certifikatet. Den kommer inte att vara densamma som CAR för kortets eget certifikat, vilket är MSCA_Card-certifikatet.

CSM_168 Såsom anges i Figure 5 får kortet, när det väl har verifierat autenticiteten och giltigheten hos ett tidigare okänt certifikat, lagra detta certifikat för framtida behov, så att den inte

▼B

behöver verifiera certifikatets autenticitet igen om det överlämnas till kortet på nytt. I stället för att lagra hela certifikatet får ett kort välja att lagra endast innehållet i certifikatets nyttodel (*Certificate Body*), såsom specificeras i avsnitt 9.3.2.

10.3. **Autentisering av fordonsenhet**

CSM_169 Fordonsenheter och kort ska använda det protokoll för autentisering av fordonsenhet som visas i Figure 6 för att autentisera fordonsenheten gentemot kortet. Autentiseringen av fordonsenheten gör det möjligt för färdskrivarkortet att explicit verifiera att fordonsenheten är autentisk. För att göra detta ska fordonsenheten använda sin privata nyckel för att signera en utmaning (*challenge*) som genererats av kortet.

CSM_170 Intill utmaningen från kortet ska fordonsenheten i signaturen inkludera den referens till kortinnehavaren som hämtas från kortcertifikatet.

Anmärkning: Detta säkerställer att det kort gentemot vilket fordonsenheten autentiserar sig är samma kort vars certifikatskedja fordonsenheten har verifierat tidigare.

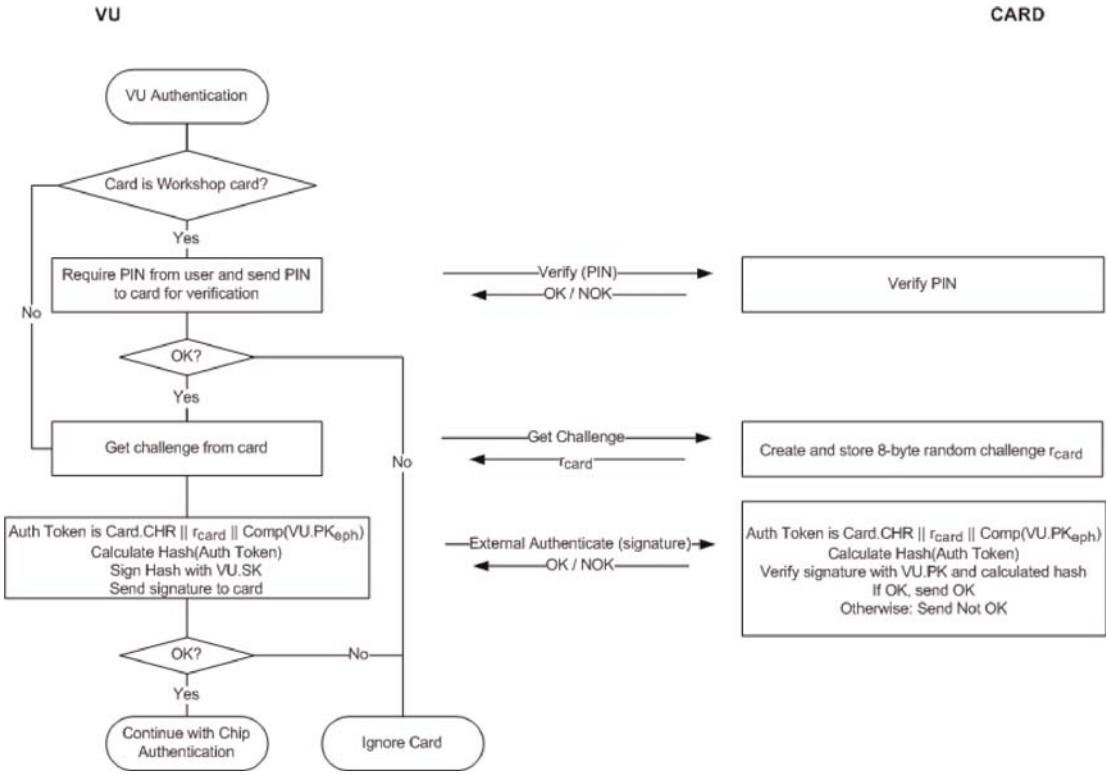
CSM_171 Fordonsenheten ska också i signaturen inkludera identifieraren för den tillfälliga öppna nyckeln Comp($VU.PK_{eph}$) som fordonsenheten kommer att använda för att upprätta säker meddelandehantering under den chipautentiseringsprocess som specificeras i avsnitt 10.4.

Anmärkning: Detta säkerställer att den fordonsenhet med vilken ett kort kommunicerar under en session med säker meddelandehantering är samma fordonsenhet som autentiserats av kortet.

▼B

Figur 6

Protokoll för autentisering av fordonsenhet (VU)



CSM_172 Om flera GET CHALLENGE-kommandon sänds från fordonsenheten under autentiseringen av fordonsenheten ska kortet varje gång sända tillbaka en ny slumpmässig utmaning på 8 byte, men lagra endast den senaste utmaningen.

CSM_173 Signeringsalgoritmen som används av fordonsenheten för autentisering av fordonsenheten ska vara ECDSA såsom den specificeras i [DSS], med användning av den hashalgoritm som är länkad till nyckelstorleken för fordonsenhetens VU_MA-nyckelpar, såsom anges i CSM_50. Signaturformatet ska vara i klartext, såsom anges i [TR-03111]. Fordonsenheten ska sända den genererade signaturen till kortet.

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 r_{card} och identifieraren för fordonsenhetens tillfälliga öppna nyckel Comp($VU.PK_{eph}$),

— beräkna hashvärdet för token för autentiseringen, med användning av den hashalgoritm som är länkad till nyckelstorleken för fordonsenhetens VU_MA-nyckelpar, såsom anges i CSM_50,

— verifiera fordonsenhetens signatur med användning av ECDSA-algoritmen i kombination med VU.PK och det beräknade hashvärdet.

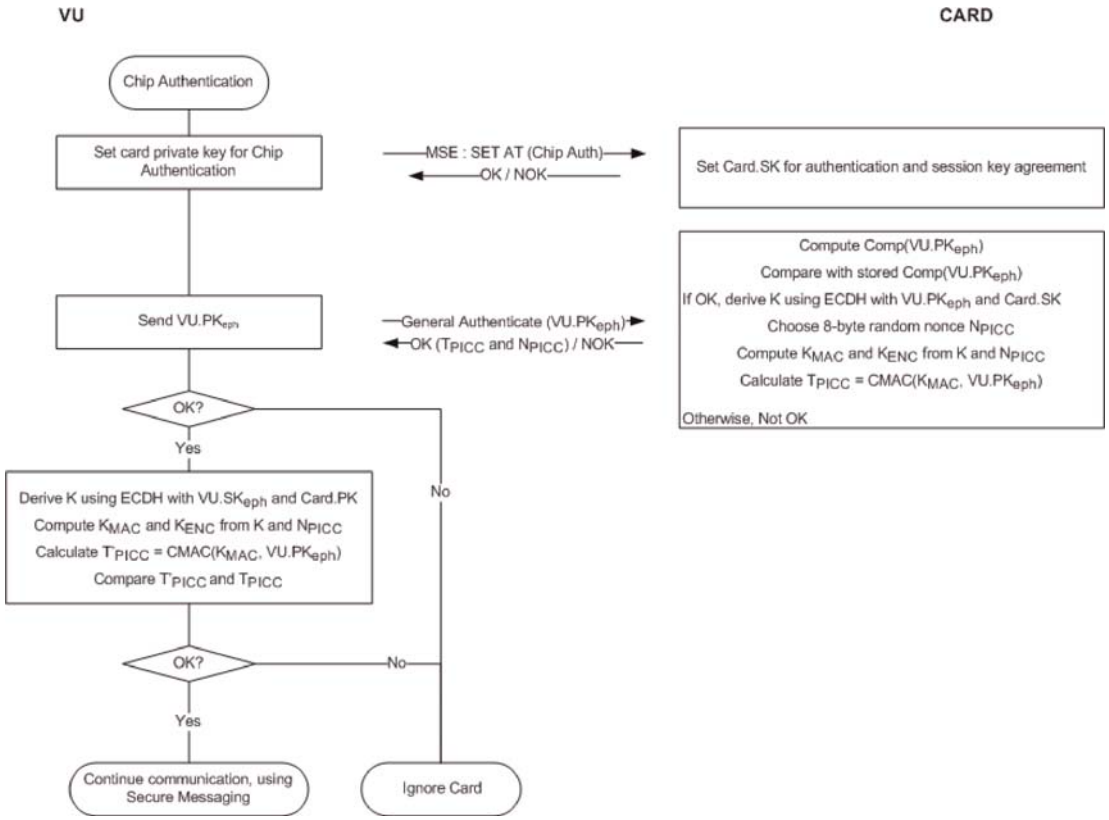
▼B

10.4. **Autentisering av chip och överenskommelse om sessionsnyckel**

CSM_175 Fordonsenheter och kort ska använda det protokoll för autentisering av chip som visas i **Figure 7** för att autentisera kortet gentemot fordonsenheten. Autentiseringen av chippet gör det möjligt för fordonsenheten att explicit verifiera att kortet är autentiskt.

Figur 7

Autentisering av chip och överenskommelse om sessionsnyckel



CSM_176 Fordonsenheten och kortet ska genomföra följande steg:

1. Fordonsenheten initierar processen för autentisering av chip genom att skicka kommandot MSE: SET AT som indikerar ”autentisering av chip med användning av ECDH-algoritmen, vilket resulterar i en AES-sessionsnyckel vars längd länkas till nyckelstorleken för kortets Card_MA-nyckelpar, såsom anges i CSM_50”. Fordonsenheten ska hämta storleken på kortets nyckelpar från kortcertifikatet.

2. Fordonsenheten översänder den öppna punkten (*public point*) $VU.PK_{eph}$ för sitt tillfälliga nyckelpar till kortet. Såsom förklaras i CSM_164 har fordonsenheten genererat detta tillfälliga nyckelpar före verifieringen av fordonsenhetens certifikatskedja. Fordonsenheten översände identifieraren av den tillfälliga öppna nyckeln $Comp(VU.PK_{eph})$ till kortet, och kortet lagrade den.

▼B

3. Kortet beräknar Comp($VU.PK_{eph}$) från $VU.PK_{eph}$ och jämför detta med det lagrade värdet av Comp($VU.PK_{eph}$).

4. Med användning av ECDH-algoritmen i kombination med kortets statiska privata nyckel och fordonsenhetens tillfälliga öppna nyckel beräknar kortet ett hemligt K.

5. Kortet väljer ett slumpmässigt tal (8 byte) som används en gång (*nonce*) N_{PICC} och använder det för att härleda två AES-sessionsnycklar K_{MAC} and K_{ENC} från K. Se CSM_179.

6. Med användning av K_{MAC} beräknar kortet en token för autentisering för identifieraren för fordonsenhetens tillfälliga öppna nyckel: $T_{PICC} = CMAC(K_{MAC}, VU.PK_{eph})$. Kortet översänder N_{PICC} och T_{PICC} till fordonsenheten.

7. Med användning av ECDH-algoritmen i kombination med kortets statiska öppna nyckel och fordonsenhetens tillfälliga privata nyckel beräknar fordonsenheten samma hemliga K som kortet gjorde i steg 4.

8. Fordonsenheten härleder sessionsnycklarna K_{MAC} och K_{ENC} från K och N_{PICC}; se CSM_179.

9. Fordonsenheten verifierar token T_{PICC} för autentisering.

CSM_177 I steg 3 ovan ska kortet beräkna Comp(VU.PKeph) som x-koordinaten för den öppna punkten (*public point*) i VU.PKeph.

CSM_178 I stegen 4 och 7 ovan ska kortet och fordonsenheten använda ECKA-EG-algoritmen som den definieras i [TR-03111].

CSM_179 I stegen 5 och 8 ovan ska kortet och fordonsenheten använda den funktion för nyckelhärledning för AES-sessionsnycklar som definieras i [TR-03111], med följande preciseringar och ändringar:

— Värdet på räknaren ska vara ‘00 00 00 01’ för K_{ENC} och ‘00 00 00 02’ för K_{MAC}.

— Det frivilliga talet *r* (*nonce*, som används en gång) ska användas och ska vara lika med N_{PICC}.

— För härledning av 128-bitars AES-nycklar ska den hashalgoritm som ska användas vara SHA-256.

— För härledning av 192-bitars AES-nycklar ska den hashalgoritm som ska användas vara SHA-384.

— För härledning av 256-bitars AES-nycklar ska den hashalgoritm som ska användas vara SHA-512.

Sessionsnycklarnas längd (dvs. den längd vid vilken hashvärdet trunkeras) ska vara länkad till storleken på Card_MA-nyckelparet, såsom anges i CSM_50.

▼B

CSM_180 I stegen 6 och 9 ovan ska kortet och fordonsenheten använda AES-algoritmen i CMAC-läge, såsom specificeras i [SP 800-38B]. Längden på T_{PICC} ska vara länkad till längden på AES-sessionsnycklarna, såsom specificeras i CSM_50.

10.5. **Säker meddelandehantering**

10.5.1 *Allmänt*

CSM_181 Alla kommandon och svar som utväxlas mellan en fordonsenhet och ett färdskrivarkort efter det att en lyckad chipautentisering genomförts och till dess att sessionen avslutats ska vara skyddade genom säker meddelandehantering (*Secure Messaging*).

CSM_182 Utom vid läsning från en fil med tillträdesvillkoret SM-R-ENC-MAC-G2 (se avsnitt 4 i tillägg 2) ska säker meddelandehantering användas i läge för endast autentisering (*authentication-only mode*). I detta läge ska en kryptografisk kontrollsumma (även kallad MAC) adderas till alla kommandon och svar för att säkerställa autenticitet och integritet för meddelanden.

CSM_183 Vid läsning från en fil med tillträdesvillkoret SM-R-ENC-MAC-G2 ska säker meddelandehantering användas i läge för kryptering följd av autentisering (*encrypt-then-authenticate mode*), dvs. först krypteras svarsdata för att säkerställa meddelandesekretess, och därefter beräknas en MAC för formaterade krypterade data för att säkerställa autenticitet och integritet.

CSM_184 Säker meddelandehantering ska använda AES såsom definierats i [AES] med sessionsnycklarna K_{MAC} och K_{ENC}, vilka fastställdes i samband med autentisering av chip.

CSM_185 Ett heltal utan tecken ska användas som SSC (*Send Sequence Counter*) för att förhindra återspelningsattacker. Storleken på SSC ska vara lika med AES-blockstorleken, dvs. 128 bitar. SSC ska vara i formatet mest signifikanta bit först (*MSB-first*). Räknaren för sekvenssändning (SSC) ska initialt ställas på noll (dvs. ‘00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00’) när säker meddelandehantering (*Secure Messaging*) startas. SSC ska ökas varje gång innan ett kommando eller svar (APDU) genereras (det innebär att eftersom startvärdet för SSC i en session med säker meddelandehantering är 0, kommer värdet på SSC i det första kommandot att vara 1). Värdet på SSC för det första svaret kommer att vara 2.

CSM_186 För kryptering av meddelanden ska K_{ENC} användas med AES i CBC-läge (*Cipher Block Chaining*) såsom definierats i [ISO 10116], med en *interleave*-parameter $m = 1$ och en initialiseringsvektor $SV = E(K_{ENC}, SSC)$, dvs. det aktuella värdet på SSC krypterat med K_{ENC}.

CSM_187 För meddelandeautentisering ska K_{MAC} användas med AES i CMAC-läge såsom specificeras i [SP 800-38B]. Längden på MAC ska vara länkad till längden på AES-sessionsnycklarna, såsom specificeras i CSM_50. SSC ska inkluderas i MAC genom att den läggs före det datagram som ska autentiseras.

▼B

10.5.2 *Säker meddelandestruktur*

CSM_188 Säker meddelandehantering ska endast använda dataobjekten för säker meddelandehantering (se [ISO 7816-4]) som förtecknas i Table 5. I alla meddelanden ska dessa dataobjekt användas i den ordning som anges i denna tabell.

Tabell 5

Dataobjekt för säker meddelandehantering

Dataobjekt	Tagg	Närvaro (O)bligatorisk, (V)illkorlig eller (F)örbjuden i	
		kommandon	svar
Data med klarvärde ej BER-TLV-kodade	‘81’	V	V
Data med klarvärde är BER-TLV-kodade, men inbegriper inte dataobjekt för säker meddelandehantering	‘B3’	V	V
Utfyllnadsindikator följd av kryptogram, data med klarvärde ej BER-TLV-kodade	‘87’	V	V
Skyddad Le	‘97’	V	F
Bearbetningsstatus	‘99’	F	O
Kryptografisk kontrollsumma	‘8E’	O	O

Anmärkning: Såsom anges i tillägg 2 kan färdskrivarkort stödja kommandona READ BINARY och UPDATE BINARY med udda INS-byte (‘B1’ resp. ‘D7’). Dessa kommandovarianter krävs för att läsa och uppdatera filer med 32 768 byte eller mer. Om en sådan variant används ska ett dataobjekt med taggen ‘B3’ användas i stället för ett objekt med taggen ‘81’. Se tillägg 2 för ytterligare information.

CSM_189 Alla dataobjekt för säker meddelandehantering ska DER TLV-kodas såsom specificeras i [ISO 8825-1]. Denna kodning resulterar i en TLV-struktur (*Tag-Length-Value*) enligt följande:

Tagg Taggen är kodad i en eller två oktetter och anger innehållet.

Längd Längden kodas som ett heltal utan tecken i en, två eller tre oktetter, vilket resulterar i den maximala längden 65 535 oktetter. Det minsta antalet oktetter ska användas.

Värde Värdet kodas i noll eller fler oktetter.

CSM_190 Dataenheter (APDU) som skyddas genom säker meddelandehantering ska skapas enligt följande:

— Kommandots startdel (*header*) ska inkluderas i MAC-beräkningen. Därför ska värdet ‘0C’ användas för CLA (*class byte*).

▼B

— Såsom anges i tillägg 2 ska alla INS-byte vara jämna, med det eventuella undantaget udda INS-byte för kommandona READ BINARY och UPDATE BINARY.

— Det faktiska värdet på Lc kommer att ändras till Lc' efter tillämpning av säker meddelandehantering.

— Datafältet ska bestå av dataobjekt för säker meddelandehantering.

— I den skyddade dataenheten (APDU) ska den nya Le (1 byte) sättas till ‘00’. Om så krävs ska ett dataobjekt ‘97’ inkluderas i datafältet för att förmedla det ursprungliga värdet på Le.

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 varje dataobjekt i dataenheten (APDU) också fyllas ut separat 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) med kryptering:	DO ‘81’ || DO ‘99’ || DO ‘8E’ || SW1SW2
Fall 2 eller 4 (jämn INS-byte) utan kryptering:	DO ‘87’ || DO ‘99’ || DO ‘8E’ || SW1SW2
Fall 2 eller 4 (udda INS-byte) utan kryptering:	DO ‘B3’ || DO ‘99’ || DO ‘8E’ || SW1SW2

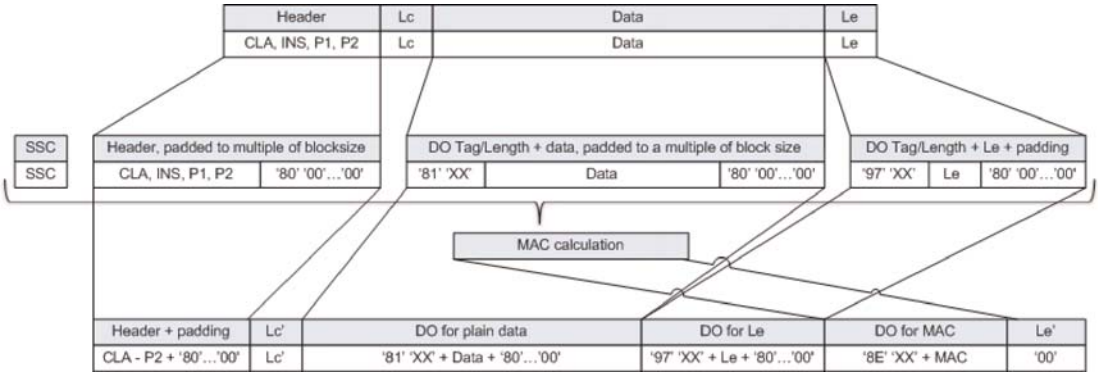
Anmärkning: Fall 2 eller 4 (udda INS-byte) med kryptering används aldrig i kommunikationen mellan en fordonsenhet och ett kort.

▼B

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

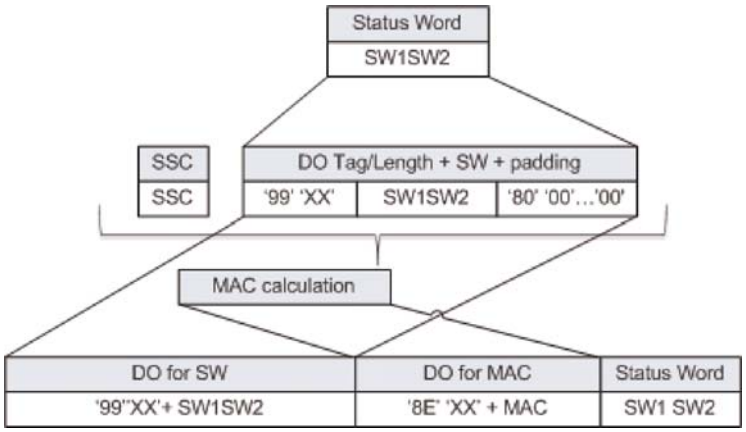
Figur 8

Omvandling av en autentiserad kommando-APDU i fall 4



Figur 9

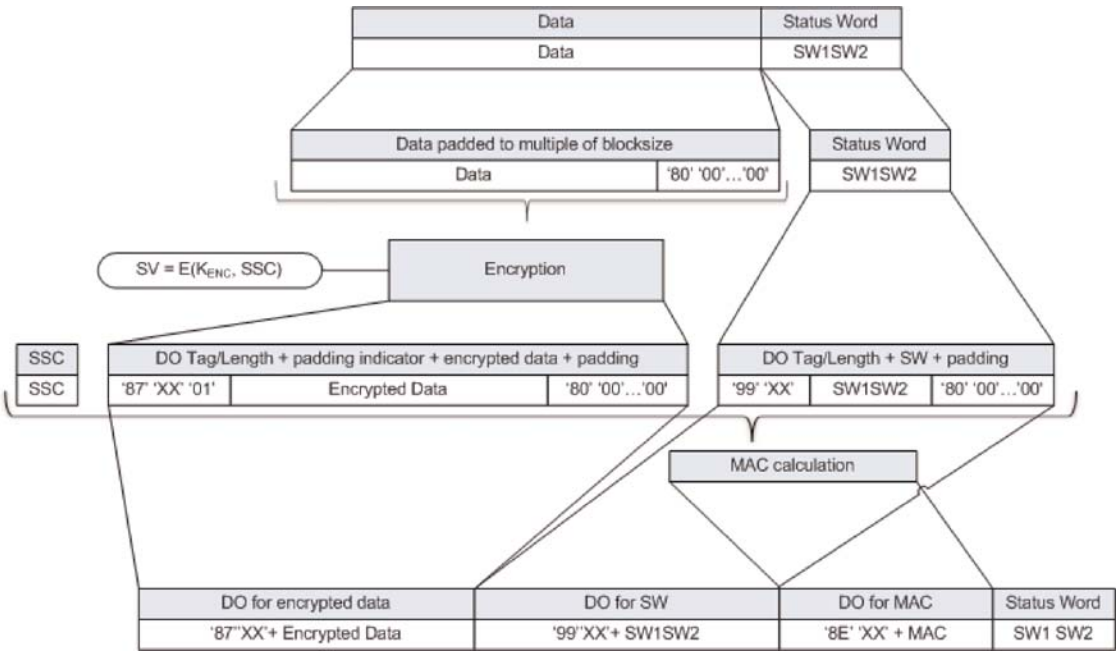
Omvandling av en autentiserad svars-APDU i fall 1/fall 3



▼B

Figur 10

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



10.5.3 *Avbryta en session med säker meddelandehantering*

CSM_192 En fordonsenhet ska avbryta en pågående session med säker meddelandehantering om, och endast om, ett av följande villkor är uppfyllt:

— Den tar emot en svars-APDU i klartext.

— Den upptäcker ett fel vid säker meddelandehantering i en svars-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, TLV-strukturen är felaktig eller utfyllnadsindikatorn i tagg ‘87’ är inte lika med ‘01’).

— Kortet sänder en byte för status som indikerar att det har upptäckt ett fel vid säker meddelandehantering (se CSM_194).

— Gränsen för antalet kommandon och tillhörande svar inom den aktuella sessionen har nåtts. För en bestämd fordonsenhet ska denna gräns fastställas av enhetens 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.

▼B

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 är strömlöst eller nollställt.

— Fordonsenheten väljer en tillämpning på kortet.

— 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.

CSM_194 Beträffande färdskrivarkorts hantering av fel vid säker meddelandehantering:

— Om – i en kommando-APDU – vissa förväntade dataobjekt för säker meddelandehantering saknas, dataobjektens ordningsföljd är felaktig eller okända dataobjekt är inkluderade, ska ett färdskrivarkort svara med följande två byte för status: ‘69 87’.

— Om – i en kommando-APDU – ett dataobjekt för säker meddelandehantering är felaktigt ska ett färdskrivarkort svara med följande två byte för status: ‘69 88’.

I sådana fall ska dessa byte för status återsändas utan användning av säker meddelandehantering.

CSM_195 Om en session med säker meddelandehantering mellan en fordonsenhet och ett färdskrivarkort avbryts, ska fordonsenheten och kortet

— på ett säkert sätt förstöra de lagrade sessionsnycklarna,

— omedelbart upprätta en ny session med säker meddelandehantering, såsom beskrivs i avsnitten 10.2–10.5.

CSM_196 Om fordonsenheten av någon anledning beslutar att starta om den ömsesidiga autentiseringen gentemot ett insatt kort, ska processen startas om med verifiering av kortets certifikatskedja, såsom beskrivs i avsnitt 10.2, och fortsätta såsom beskrivs i avsnitten 10.2–10.5.

▼B

11. KOPPLING, ÖMSESIDIG AUTENTISERING OCH SÄKER MEDDELANDEHANTERING MELLAN FORDONSENHETER OCH EXTERNA GNSS-ANORDNINGAR

11.1. **Allmänt**

CSM_197 Den GNSS-anordning som används av en fordonsenhet för att fastställa dess position kan vara intern (dvs. inbyggd inuti fordonsenhetens hölje och ej avtagbar), eller den kan vara en extern modul. I det första fallet finns det inget behov av att standardisera den interna kommunikationen mellan GNSS-anordningen och fordonsenheten, och kraven i detta kapitel är inte tillämpliga. I det senare fallet ska kommunikationen mellan fordonsenheten och den externa GNSS-anordningen vara standardiserad och skyddad såsom beskrivs i detta kapitel.

CSM_198 Säker kommunikation mellan en fordonsenhet och en extern GNSS-anordning ska ske på samma sätt som säker kommunikation mellan en fordonsenhet och ett färdskrivarkort, varvid den externa GNSS-anordningen (EGF, *External GNSS Facility*) har kortets roll. Alla krav som nämns i kapitel 10 för färdskrivarkort ska uppfyllas av en extern GNSS-anordning, med beaktande av de avvikelser, klargöranden och tillägg som nämns i det här kapitlet. I synnerhet ska ömsesidig verifiering av certifikatskedjan, autentisering av fordonsenhet och autentisering av chip utföras såsom beskrivs i avsnitten 11.3 och 11.4.

CSM_199 Kommunikation mellan en fordonsenhet och en extern GNSS-anordning skiljer sig från kommunikation mellan en fordonsenhet och ett kort på så sätt att en fordonsenhet och en extern GNSS-anordning måste kopplas en gång i en verkstad innan fordonsenheten och den externa GNSS-anordningen kan utbyta GNSS-baserade data under normal drift. Kopplingsprocessen beskrivs i avsnitt 11.2.

CSM_200 För kommunikation mellan en fordonsenhet och en extern GNSS-anordning ska APDU-kommandon och APDU-svar som är baserade på [ISO 7816-4] och [ISO 7816-8] användas. Den exakta strukturen hos dessa dataenheter (APDU) definieras i tillägg 2 till denna bilaga.

11.2. **Koppling mellan fordonsenhet och extern GNSS-anordning**

CSM_201 En fordonsenhet och en extern GNSS-anordning i ett fordon ska kopplas av en verkstad. Endast en kopplad fordonsenhet och extern GNSS-anordning ska kunna kommunicera under normal drift.

CSM_202 Koppling av en fordonsenhet och en extern GNSS-anordning ska endast vara möjlig om fordonsenheten är i kalibreringsläge. Kopplingen ska initieras av fordonsenheten.

CSM_203 En verkstad får när som helst göra en ny koppling av en fordonsenhet till en annan extern GNSS-anordning eller till samma externa GNSS-anordning. Vid en ny koppling ska fordonsenheten på ett säkert sätt förstöra det befintliga EGF_MA-certifikat som finns i dess minne och lagra EGF_MA-certifikatet för den externa GNSS-anordning till vilken den kopplas.

CSM_204 En verkstad får när som helst göra en ny koppling av en extern GNSS-anordning till en annan fordonsenhet eller till samma fordonsenhet. Vid en ny koppling ska den externa GNSS-anordningen på ett säkert sätt förstöra det befintliga VU_MA-certifikat som finns i dess minne och lagra VU_MA-certifikatet för den fordonsenhet till vilken den kopplas.

▼B

11.3. **Ömsesidig verifiering av certifikatskedja**

11.3.1 *Allmänt*

CSM_205 En ömsesidig verifiering av certifikatskedja mellan en fordonsenhet och en extern GNSS-anordning ska äga rum endast när de båda kopplas av en verkstad. Under normal drift ska inga certifikat verifieras mellan en fordonsenhet och en extern GNSS-anordning som är kopplade till varandra. Fordonsenheten och den externa GNSS-anordningen ska i stället förlita sig på de certifikat som lagrades vid kopplingen, efter att först ha kontrollerat den tidsmässiga giltigheten för dessa certifikat. Fordonsenheten och den externa GNSS-anordningen får under normal drift inte förlita sig på några andra certifikat för att skydda kommunikationen mellan de båda.

11.3.2 *Vid koppling av fordonsenhet och extern GNSS-anordning*

CSM_206 Vid koppling till en extern GNSS-anordning ska en fordonsenhet använda det protokoll som visas i Figure 4 (avsnitt 10.2.1) för att verifiera den externa GNSS-anordningens certifikatskedja.

Anmärkningar till Figure 4 i detta sammanhang:

— Kontroll av datakommunikationen ligger utanför detta tilläggs tillämpningsområde. En extern GNSS-anordning är dock inget smartkort och fordonsenheten kommer därför troligen inte att sända *Reset* för att initiera kommunikationen och inte heller ta emot ATR.

— De kortcertifikat och de öppna nycklar som nämns i figuren ska tolkas som den externa GNSS-anordningens certifikat och öppna nycklar för ömsesidig autentisering. I avsnitt 9.1.6 betecknas dessa EGF_MA.

— De Card.CA-certifikat och de öppna nycklar som nämns i figuren ska tolkas som MSCA-certifikaten och de öppna nycklarna för signering av certifikat för externa GNSS-anordningar. I avsnitt 9.1.3 betecknas dessa MSCA_VU-EGF.

— Det Card.CA.EUR-certifikat som nämns i figuren ska tolkas som det europeiska rotcertifikat som anges i certifieringsinstansens referens (CAR) för MSCA_VU-EGF-certifikatet.

— Det Card.Link-certifikat som nämns i figuren ska tolkas som den externa GNSS-anordningens länkcertifikat, om ett sådant finns. Såsom anges i avsnitt 9.1.2 är detta ett länkcertifikat för ett nytt europeiskt rotnyckelpar som skapats av Erca och signerats med den föregående europeiska privata nyckeln.

— Card.Link.EUR-certifikatet är det europeiska rotcertifikat som anges i certifieringsinstansens referens (CAR) för Card.Link-certifikatet.

— Fordonsenheten ska läsa `sensorGNSSserialNumber` i stället för `cardExtendedSerialNumber` från EF ICC.

— Fordonsenheten ska välja den externa GNSS-anordningens AID i stället för färdskrivarens AID.

— Att ”ignorera kort” ska tolkas som att ”ignorera extern GNSS-anordning”.

▼B

CSM_207 Fordonsenheten ska, när den har verifierat EGF_MA-certifikatet, lagra detta certifikat för användning under normal drift; se avsnitt 11.3.3.

CSM_208 Vid koppling till en fordonsenhet ska en extern GNSS-anordning använda det protokoll som visas i Figure 5 (avsnitt 10.2.2) för att verifiera fordonsenhetens certifikatskedja.

Anmärkningar till Figure 5 i detta sammanhang:

— Fordonsenheten ska generera ett nytt tillfälligt nyckelpar med användning av domänparametrarna i EGF-certifikatet.

— De fordonsenhetscertifikat och öppna nycklar som nämns i figuren är de som används för ömsesidig autentisering. I avsnitt 9.1.4 betecknas dessa VU_MA.

— De VU.CA-certifikat och öppna nycklar som nämns i figuren är de som används för signering av certifikat för fordonsenheter och externa GNSS-anordningar. I avsnitt 9.1.3 betecknas dessa MSCA_VU-EGF.

— Det VU.CA.EUR-certifikat som nämns i figuren är det europeiska rotcertifikat som anges i certifieringsinstansens referens (CAR) för VU.CA-certifikatet.

— Det VU.Link-certifikat som nämns i figuren är fordonsenhetens länkcertifikat, om ett sådant finns. Såsom anges i avsnitt 9.1.2 är detta ett länkcertifikat för ett nytt europeiskt rotnyckelpar som skapats av Erca och signerats med den föregående europeiska privata nyckeln.

— VU.Link.EUR-certifikatet är det europeiska rotcertifikat som anges i certifieringsinstansens referens (CAR) för VU.Link-certifikatet.

CSM_209 Med avvikelse från krav CSM_167 ska en extern GNSS-anordning använda GNSS-tiden för att verifiera den tidsmässiga giltigheten för alla certifikat som överlämnas.

CSM_210 När den har verifierat VU_MA-certifikatet ska den externa GNSS-anordningen lagra detta certifikat för användning under normal drift; se avsnitt 11.3.3.

11.3.3 *Under normal drift*

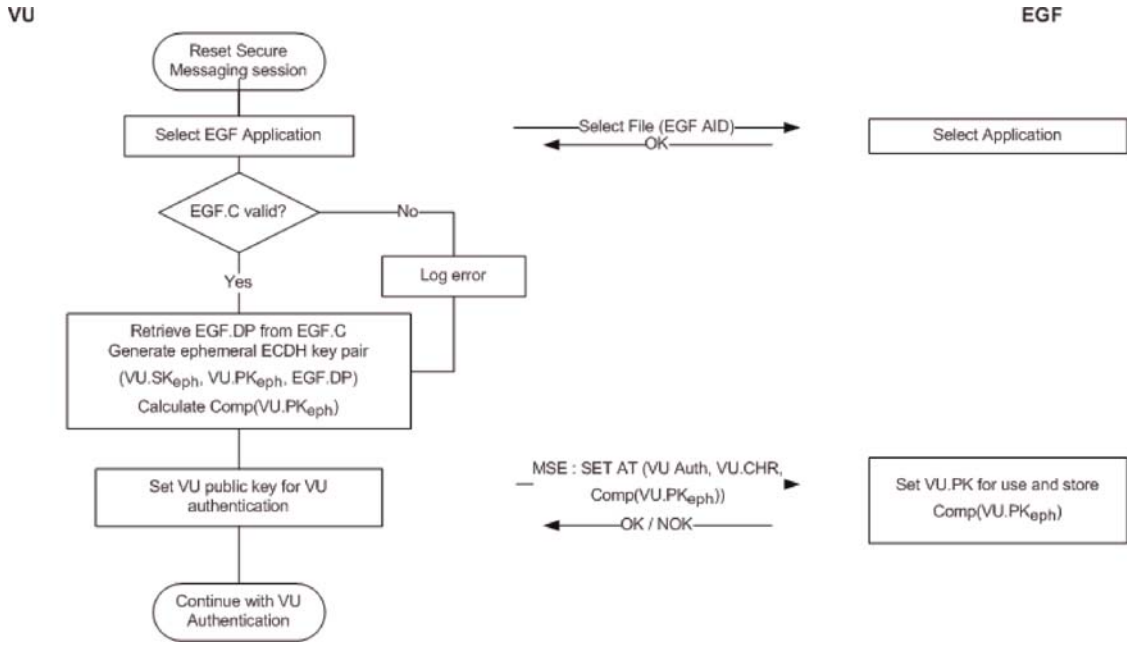
CSM_211 En fordonsenhet och en extern GNSS-anordning ska under normal drift använda det protokoll som visas i Figure 11 för att verifiera den tidsmässiga giltigheten för de lagrade EGF_MA- och VU_MA-certifikaten och för att bestämma den öppna nyckeln VU_MA för den påföljande autentiseringen av fordonsenheten. Ingen ytterligare ömsesidig verifiering av certifikatskedjorna ska äga rum under normal drift.

Notera att Figure 11 i huvudsak utgörs av de första stegen som visas i Figure 4 och Figure 5. Notera också att eftersom en extern GNSS-anordning inte är ett smartkort kommer fordonsenheten troligen inte att sända *Reset* för att initiera kommunikationen och inte heller ta emot ATR. Detta ligger i vilket fall som helst utanför detta tilläggs tillämpningsområde.

▼B

Figur 11

Ömsesidig verifiering av tidsmässig giltighet för certifikat under normal drift med fordonsenhet och extern GNSS-anordning



CSM_212 Såsom visas i Figure 11 ska fordonsenheten logga ett fel om EGF_MA-certifikatet inte längre är giltigt. Ömsesidig autentisering, överenskommelse om nyckel och påföljande kommunikation via säker meddelandehantering ska dock fortsätta normalt.

11.4. **Autentisering av fordonsenhet, autentisering av chip och överenskommelse om sessionsnyckel**

CSM_213 Autentisering av fordonsenhet, autentisering av chip och överenskommelse om sessionsnyckel mellan en fordonsenhet och en extern GNSS-anordning ska äga rum vid koppling och närhelst en session med säker meddelandehantering återupprättas under normal drift. Fordonsenheten och den externa GNSS-anordningen ska genomföra de processer som beskrivs i avsnitten 10.3 och 10.4. Alla krav i dessa avsnitt ska tillämpas.

11.5. **Säker meddelandehantering**

CSM_214 Alla kommandon och svar som utväxlas mellan en fordonsenhet och en extern GNSS-anordning efter det att en lyckad chipautentisering genomförts och till dess att sessionen avslutats ska vara skyddade genom säker meddelandehantering (*Secure Messaging*) i läge för endast autentisering (*authentication-only mode*). Alla krav i avsnitt 10.5 ska gälla.

CSM_215 Om en session med säker meddelandehantering mellan en fordonsenhet och en extern GNSS-anordning avbryts ska fordonsenheten omedelbart upprätta en ny session med säker meddelandehantering, såsom beskrivs i avsnitten 11.3.3 och 11.4.

12. PARNING AV OCH KOMMUNIKATION MELLAN FORDONSENHET OCH RÖRELSESENSOR

12.1. **Allmänt**

CSM_216 En fordonsenhet och en rörelsesensor ska kommunicera med hjälp av det gränssnittsprotokoll som specificeras i [ISO 16844-3] vid parning och vid normal drift, med de ändringar som beskrivs i detta kapitel och i avsnitt 9.2.1.

▼B

Anmärkning: Läsare av detta kapitel förväntas känna till innehållet i [ISO 16844-3].

12.2. **Parning av fordonsenhet och rörelsesensor med användning av olika nyckelgenerationer**

Såsom förklaras i avsnitt 9.2.1 görs regelbundna utbyten av rörelsesensorns huvudnyckel och alla tillhörande nycklar. Detta leder till närvaron av upp till tre rörelsesensorrelaterade AES-nycklar $K_{M\text{-}WC}$ (i på varandra följande nyckelgenerationer) i verkstadskorten. På liknande sätt kan det i rörelsesensorer finnas upp till tre olika AES-baserade krypteringar av data (på grundval av på varandra följande generationer av rörelsesensorns huvudnyckel K_M). En fordonsenhet innehåller endast en rörelsesensorrelaterad nyckel $K_{M\text{-}VU}$.

CSM_217 En andra generationens fordonsenhet och en andra generationens rörelsesensor ska paras enligt följande (jämför tabell 6 i [ISO 16844-3]):

1. Ett andra generationens verkstadskort sätts in i fordonsenheten och fordonsenheten ansluts till rörelsesensorn.

2. Fordonsenheten läser alla tillgängliga $K_{M\text{-}WC}$-nycklar från verkstadskortet, inspekterar deras nyckelversionsnummer och väljer den som matchar versionsnumret för fordonsenhetens $K_{M\text{-}VU}$-nyckel. Om den matchande $K_{M\text{-}WC}$-nyckeln inte är närvarande i verkstadskortet avbryter fordonsenheten parningsprocessen och visar ett lämpligt felmeddelande för innehavaren av verkstadskortet.

3. Fordonsenheten beräknar rörelsesensorns huvudnyckel K_M från $K_{M\text{-}VU}$ och $K_{M\text{-}WC}$, och identifieringsnyckeln K_{ID} från K_M, såsom specificeras i avsnitt 9.2.1.

4. Fordonsenheten sänder instruktioner för att initiera parningsprocessen gentemot rörelsesensorn, såsom beskrivs i [ISO 16844-3], och krypterar det serienummer den tar emot från rörelsesensorn med identifieringsnyckeln K_{ID}. Fordonsenheten sänder det krypterade serienumret tillbaka till rörelsesensorn.

5. Rörelsesensorn matchar det krypterade serienumret, i tur och ordning, med var och en de krypteringar av serienumret som den lagrar internt. Om en matchning lyckas är fordonsenheten autentiserad. Rörelsesensorn noterar den generation av K_{ID} som används av fordonsenheten och återsänder den matchande krypterade versionen av sin parningsnyckel, dvs. den kryptering som skapades med användning av samma generation av K_M.

6. Fordonsenheten dekrypterar parningsnyckeln med användning av K_M, genererar en sessionsnyckel K_S, krypterar den med parningsnyckeln och sänder resultatet till rörelsesensorn. Rörelsesensorn dekrypterar K_S.

7. Fordonsenheten samlar parningsinformationen såsom definieras i [ISO 16844-3], krypterar informationen med parningsnyckeln och sänder resultatet till rörelsesensorn. Rörelsesensorn dekrypterar parningsinformationen.

8. Rörelsesensorn krypterar den mottagna parningsinformationen med den mottagna K_S och återsänder den till fordonsenheten. Fordonsenheten verifierar att parningsinformationen är samma information som fordonsenheten skickade till rörelsesensorn i föregående steg. Om så är

▼B

fallet bevisar det att rörelsesensorn använde samma K_S som fordonsenheten och följaktligen i steg 5 skickade sin parningsnyckel krypterad med korrekt generation av K_M. Följaktligen är rörelsesensorn autentiserad.

Observera att steg 2 och 5 skiljer sig från standardprocessen i [ISO 16844-3]; övriga steg är standard.

Exempel: Antag att en parning äger rum under det första året av Erca (3)-certifikatets giltighetsperiod; se Figure 2 i avsnitt 9.2.1.2. Dessutom:

— Antag att rörelsesensorn utfärdades under det sista året av Erca (1)-certifikatets giltighetsperiod. Det kommer därför att innehålla följande nycklar och data:

  — $N_s[1]$: Dess serienummer krypterat med generation 1 för K_{ID}.

  — $N_s[2]$: Dess serienummer krypterat med generation 2 för K_{ID}.

  — $N_s[3]$: Dess serienummer krypterat med generation 3 för K_{ID}.

  — $K_P[1]$: Dess parningsnyckel (generation 1) ([1]), krypterad med generation 1 av K_M.

  — $K_P[2]$: Dess parningsnyckel (generation 2), krypterad med generation 2 av K_M.

  — $K_P[3]$: Dess parningsnyckel (generation 3), krypterad med generation 3 av K_M.

— Antag att verkstadskortet utfärdades under det första året av Erca (3)-certifikatets giltighetsperiod. Det kommer därför att innehålla generation 2 och generation 3 av nyckeln $K_{M\text{-}WC}$.

— Antag att fordonsenheten är en fordonsenhet i generation 2, som innehåller generation 2 av $K_{M\text{-}VU}$.

I detta fall kommer följande att hända i stegen 2–5:

— Steg 2: Fordonsenheten läser generation 2 och generation 3 av $K_{M\text{-}WC}$ från verkstadskortet och inspekterar deras versionsnummer.

— Steg 3: Fordonsenheten kombinerar $K_{M\text{-}WC}$ (generation 2) med sin $K_{M\text{-}VU}$ för att beräkna K_M och K_{ID}.

— Steg 4: Fordonsenheten krypterar det serienummer den tar emot från rörelsesensorn med K_{ID}.

— Steg 5: Rörelsesensorn jämför mottagna data med $N_s[1]$ och hittar ingen matchning. Därefter jämför den dessa data med $N_s[2]$ och hittar en matchning. Den drar slutsatsen att fordonsenheten är en fordonsenhet i generation 2, och skickar därför tillbaka $K_P[2]$.

([1]) Observera att parningsnycklarna (generation 1, generation 2 och generation 3) i själva verket kan vara samma nyckel, eller tre olika nycklar som har olika längder, såsom förklaras i CSM_117.

▼B

12.3. **Parning av och kommunikation mellan fordonsenhet och rörelsesensor med användning av AES**

CSM_218 Såsom specificeras i Table 3 i avsnitt 9.2.1 ska alla nycklar som är involverade i parningen av en (andra generationens) fordonsenhet och en rörelsesensor och i efterföljande kommunikation vara AES-nycklar, snarare än TDES-nycklar med dubbel längd såsom specificeras i [ISO 16844-3]. Dessa AES-nycklar kan ha en längd av 128, 192 eller 256 bitar. Eftersom AES-blockstorleken är 16 byte måste längden av ett krypterat meddelande vara en multipel av 16 byte, jämfört med 8 byte för TDES. Dessutom kommer några av dessa meddelanden att användas för att transportera AES-nycklar, vars längd kan vara 128, 192 eller 256 bitar. Därför ska antalet byte (med data) per instruktion i tabell 5 i [ISO 16844-3] ändras enligt Table 6:

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	16 / 32	16 / 32	16 / 32
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

CSM_219 Den parningsinformation som sänds i instruktionerna 43 (fordonsenhet, förfrågan) och 50 (rörelsesensor, svar) ska samlas såsom specificeras i avsnitt 7.6.10 i [ISO 16844-3], bortsett från att AES-algoritmen ska användas i stället för TDES-algoritmen i krypteringsschemat för parningsdata, vilket sålunda resulterar i två AES-krypteringar, varvid den utfyllnad som specificeras i CSM_220 anpassas för att passa med AES-blockstorleken. Nyckeln K'_p som används för denna kryptering ska genereras enligt följande:

— Om parningsnyckeln K_P är 16 byte lång: $K'_p = K_P$ XOR $(N_s||N_s)$

▼B

— Om parningsnyckeln K_P är 24 byte lång: $K'_p = K_P$ XOR $(N_s||N_s||N_s)$

— Om parningsnyckeln K_P är 32 byte lång: $K'_p = K_P$ XOR $(N_s||N_s||N_s||N_s)$

där N_s är serienumret (8 byte) för rörelsesensorn.

CSM_220 Om längden på klartextdata (vid användning av AES-nycklar) inte är en multipel av 16 byte ska utfyllnadsmetod 2, som definieras i [ISO 9797-1], användas.

Anmärkning: I [ISO 16844-3] är antalet byte med klartextdata alltid en multipel av 8, varför utfyllnad inte är nödvändig vid användning av TDES. Definitionen av data och meddelanden i [ISO 16844-3] ändras inte genom denna del av detta tillägg, och därför måste utfyllnad användas.

CSM_221 För instruktion 11 och om fler än ett datablock måste krypteras ska CBC-läge (*Cipher Block Chaining*) användas såsom definieras i [ISO 10116], med en *interleave*-parameter $m = 1$. Den initialiseringsvektor (IV) som ska användas ska vara följande:

— För instruktion 11: det autentiseringsblock om 8 byte som specificeras i avsnitt 7.6.3.3 i [ISO 16844-3], utfyllt med användning av utfyllnadsmetod 2 som definieras i [ISO 9797-1]; se även avsnitten 7.6.5 och 7.6.6 i [ISO 16844-3].

— För alla andra instruktioner i vilka mer än 16 byte överförs, såsom specificeras i Table 6: ‘00’ {16}, dvs. 16 byte med binärt värde 0.

Anmärkning: Såsom visas i avsnitten 7.6.5 och 7.6.6 i [ISO 16844-3], när rörelsesensorn krypterar datafiler för användning i instruktion 11, gäller följande för autentiseringsblocket:

— Det används som initialiseringsvektor för krypteringen av datafilerna i CBC-läge.

— Det är krypterat och inkluderat som det första blocket i de data som sänds till fordonsenheten.

12.4. **Parning av fordonsenhet och rörelsesensor för olika utrustningsgenerationer**

CSM_222 Såsom förklaras i avsnitt 9.2.1 kan en andra generationens rörelsesensor innehålla den TDES-baserade krypteringen av parningsdata (såsom definieras i del A i detta tillägg), vilket gör det möjligt för rörelsesensorn att paras med en första generationens fordonsenhet. Om detta är fallet ska en första generationens fordonsenhet och en andra generationens rörelsesensor paras såsom beskrivs i del A i detta tillägg och i [ISO 16844-3]. För parningsprocessen får antingen ett första generationens eller ett andra generationens verkstadskort användas.

Anmärkningar:

— Det är inte möjligt att para en andra generationens fordonsenhet med en första generationens rörelsesensor.

▼B

— Det är inte möjligt att använda ett första generationens verkstadskort för koppling av en andra generationens fordonsenhet till en rörelsesensor.

13. SÄKERHET FÖR FJÄRRKOMMUNIKATION VIA DSRC

13.1. **Allmänt**

Såsom specificeras i tillägg 14 genererar en fordonsenhet regelbundet RTM-data (*Remote Tachograph Monitoring*) och skickar dessa data till kommunikationsanordningen för fjärravläsning (RCF, *Remote Communication Facility*). Kommunikationsanordningen för fjärravläsning är ansvarig för att skicka dessa data via det DSRC-gränssnitt som beskrivs i tillägg 14 till fjärravläsaren. I tillägg 1 specificeras att RTM-data är en konkatenering av följande:

Krypterad nyttolast från färdskrivaren krypteringen av klartextnyttolast från färdskrivaren

DSRC-säkerhetsdata beskrivs nedan

Dataformatet för klartextnyttolast från färdskrivaren specificeras i tillägg 1 och beskrivs närmare i tillägg 14. I detta avsnitt beskrivs strukturen hos DSRC-säkerhetsdata; den formella specifikationen återfinns i tillägg 1.

CSM_223 De data i klartext som överlämnas med datatyp `tachographPayload` från fordonsenheten till en kommunikationsanordning för fjärravläsning (om denna inte är en del av fordonsenheten) eller från fordonsenheten till en fjärravläsare via DSRC-gränssnittet (om kommunikationsanordningen för fjärravläsning är en del av fordonsenheten) ska skyddas i läge för kryptering följd av autentisering (*encrypt-then-authenticate mode*), dvs. data som utgör nyttolast från färdskrivaren ska först krypteras för att säkerställa meddelandets sekretess, och därefter ska en MAC beräknas för att säkerställa autenticitet och integritet för dessa data.

CSM_224 DSRC-säkerhetsdata ska bestå av en konkatenering av följande dataelement i följande ordning (se även Figure 12):

Aktuellt datum och aktuell tid	Aktuellt datum och aktuell tid enligt fordonsenheten (datatyp `TimeReal`).
Räknare	En räknare på 3 byte (se CSM_225).
Fordonsenhetens serienummer	Fordonsenhetens serienummer (datatyp `VuSerialNumber`).
Versionsnummer för DSRC-huvudnyckel	Det versionsnummer på 1 byte för den DSRC-huvudnyckel från vilken fordonsenhetens specifika DSRC-nycklar härleddes (se avsnitt 9.2.2).
MAC	Det MAC-värde som beräknas från samtliga föregående byte i dessa RTM-data.

CSM_225 Räknaren (3 byte) i DSRC-säkerhetsdata ska vara i formatet mest signifikanta bit först (*MSB-first*). Första gången en fordonsenhet beräknar en uppsättning RTM-data efter det att den tagits i bruk, ska den sätta värdet på räknaren till 0. Fordonsenheten ska öka värdet på räknaren med 1 varje gång innan den beräknar nästa uppsättning RTM-data.

▼B

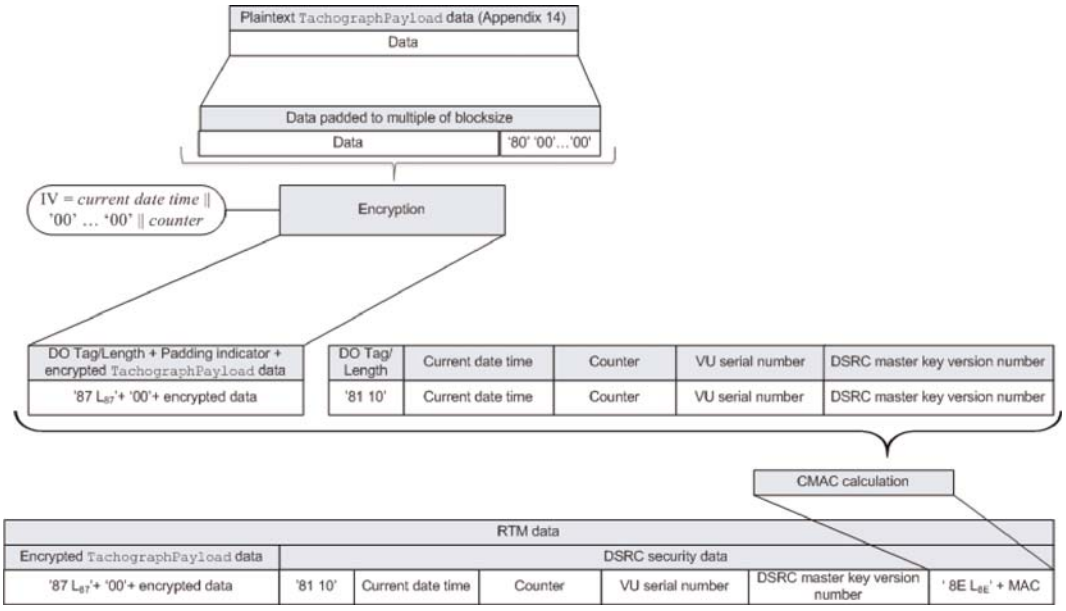
13.2. **Kryptering av nyttolast från färdskrivaren och MAC-generering**

CSM_226 Vid mottagning av ett dataelement i klartext med datatypen `TachographPayload`, såsom beskrivs i tillägg 14, ska en fordonsenhet kryptera dessa data såsom visas i Figure 12: fordonsenhetens DSRC-nyckel för kryptering $K_VU_{DSRC}_ENC$ (se avsnitt 9.2.2) ska användas med AES i CBC-läge (*Cipher Block Chaining*), enligt definitionen i [ISO 10116], med en *interleave*-parameter $m = 1$. Initialiseringsvektorn ska vara lika med aktuellt datum och aktuell tid (*IV = current date time)* || '*00 00 00 00 00 00 00 00*' || *counter*, där *current date time* och *counter* specificeras i CSM_224. De data som ska krypteras ska fyllas ut med användning av metod 2, som definieras i [ISO 9797-1].

CSM_227 En fordonsenhet ska beräkna MAC i DSRC-säkerhetsdata såsom visas i Figure 12: MAC ska beräknas för alla föregående byte i RTM-data, upp till och inklusive DSRC-huvudnyckelns versionsnummer, och inklusive dataobjektens taggar och längder. Fordonsenheten ska använda sin DSRC-nyckel för autenticitet $K_VU_{DSRC}_MAC$ (se avsnitt 9.2.2) med AES-algoritmen i CMAC-läge såsom specificeras i [SP 800-38B]. Längden på MAC ska vara länkad till längden på de fordonsenhetsspecifika DSRC-nycklarna, såsom specificeras i CSM_50.

Figur 12

Kryptering av nyttolast från färdskrivaren och MAC-generering



13.3. **Verifiering och dekryptering av nyttolast från färdskrivaren**

CSM_228 När en fjärravläsare tar emot RTM-data från en fordonsenhet ska den sända alla dessa data till ett kontrollkort i datafältet i ett PROCESS DSRC MESSAGE-kommando, såsom beskrivs i tillägg 2. Därefter gäller följande:

▼B

1. Kontrollkortet ska inspektera DSRC-huvudnyckelns versionsnummer i DSRC-säkerhetsdata. Om kontrollkortet inte känner igen den angivna DSRC-huvudnyckeln ska den återsända ett felmeddelande som specificeras i tillägg 2 och avbryta processen.

2. Kontrollkortet ska använda den angivna DSRC-huvudnyckeln i kombination med fordonsenhetens serienummer i DSRC-säkerhetsdata för att härleda de fordonsenhetsspecifika DSRC-nycklarna K_VU_{DSRC}_ENC och K_VU_{DSRC}_MAC, såsom specificeras i CSM_124.

3. Kontrollkortet ska använda K_VU_{DSRC}_MAC för att verifiera MAC i DSRC-säkerhetsdata, såsom specificeras i CSM_227. Om MAC-värdet är felaktigt ska kontrollkortet återsända ett felmeddelande som specificeras i tillägg 2 och avbryta processen.

4. Kontrollkortet ska använda K_VU_{DSRC}_ENC för att dekryptera den krypterade nyttolasten från färdskrivaren, såsom specificeras i CSM_226. Kontrollkortet ska ta bort utfyllnaden och återsända dekrypterade data som utgör nyttolast från färdskrivaren till fjärravläsaren.

CSM_229 För att förhindra återspelningsattacker ska fjärravläsaren verifiera att RTM-data är färska genom att verifiera att aktuellt datum och aktuell tid (*current date time*) i DSRC-säkerhetsdata inte avviker alltför mycket från fjärravläsarens aktuella tid.

Anmärkningar:

— Detta kräver att fjärravläsaren har en korrekt och tillförlitlig tidskälla.

— Eftersom tillägg 14 kräver att en fordonsenhet ska beräkna en ny uppsättning RTM-data var 60:e sekund, och fordonsenhetens klocka tillåts avvika 1 minut från realtid, är 2 minuter en lägre gräns för hur färska RTM-data kan vara. De krav som kan ställas på hur färska data ska vara beror också på precisionen hos fjärravläsarens klocka.

CSM_230 När en verkstad verifierar DSRC-funktionaliteten hos en fordonsenhet ska den sända alla RTM-data som mottagits från fordonsenheten till ett verkstadskort i datafältet i ett PROCESS DSRC MESSAGE-kommando, såsom beskrivs i tillägg 2. Verkstadskortet ska utföra alla kontroller och åtgärder som specificeras i CSM_228.

14. SIGNERING AV DATAÖVERFÖRINGAR OCH VERIFIERING AV SIGNATURER

14.1. **Allmänt**

CSM_231 IDE-enheten (*Intelligent Dedicated Equipment*) ska lagra data som tas emot från en fordonsenhet eller ett kort under en överföringssession inom en (1) fysisk datafil. Data kan lagras på ett externt lagringsmedium. Denna fil innehåller digitala signaturer för datablock, såsom specificeras i tillägg 7. Denna fil ska också innehålla följande certifikat (se avsnitt 9.1):

▼B

— Vid överföring från en fordonsenhet:

— VU_Sign-certifikatet.

— MSCA_VU-EGF-certifikatet som innehåller den öppna nyckel som ska användas för verifiering av VU_Sign-certifikatet.

— Vid överföring från ett kort:

— Card_Sign-certifikatet.

— MSCA_Card-certifikatet som innehåller den öppna nyckel som ska användas för verifiering av Card_Sign-certifikatet.

CSM_232 IDE-enheten ska även ha tillgång till följande:

— Om den använder ett kontrollkort för att verifiera signaturen, såsom visas i Figure 13: det länkcertifikat som länkar det senaste EUR-certifikatet till det EUR-certifikat vars giltighetsperiod direkt föregår giltighetstiden för det senaste, i förekommande fall.

— Om den verifierar signaturen själv: alla giltiga europeiska rotcertifikat.

Anmärkning: Den metod som IDE-enheten använder för att hämta dessa certifikat specificeras inte i detta tillägg.

14.2. **Generering av signatur**

CSM_233 Signeringsalgoritmen för att skapa digitala signaturer för överförda data ska vara ECDSA såsom den specificeras i [DSS], med användning av den hashalgoritm som är länkad till nyckelstorleken för fordonsenheten eller kortet, såsom anges i CSM_50. Signaturformatet ska vara i klartext, såsom anges i [TR-03111].

14.3. **Verifiering av signatur**

CSM_234 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. 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].

Anmärkningar till Figure 13:

— Den utrustning som har signerat de data som ska analyseras betecknas EQT.

— De EQT-certifikat (utrustningscertifikat) och öppna nycklar som nämns i figuren är de som används för signering, dvs. VU_Sign eller Card_Sign.

— De EQT.CA-certifikat och öppna nycklar som nämns i figuren är de som används för signering av fordonsenhets- eller kortcertifikat, beroende på vad som är tillämpligt.

— Det EQT.CA.EUR-certifikat som nämns i figuren är det europeiska rotcertifikat som anges i certifieringsinstansens referens (CAR) för EQT.CA-certifikatet.

▼B

— Det EQT.Link-certifikat som nämns i figuren är länkcertifikatet för EQT, om ett sådant finns. Såsom anges i avsnitt 9.1.2 är detta ett länkcertifikat för ett nytt europeiskt rotnyckelpar som skapats av Erca och signerats med den föregående europeiska privata nyckeln.

— EQT.Link.EUR-certifikatet är det europeiska rotcertifikat som anges i certifieringsinstansens referens (CAR) för EQT.Link-certifikatet.

CSM_235 För beräkning av hashvärdet M som sänds till kontrollkortet i kommandot PSO:HASH ska IDE-enheten använda den hashalgoritm som är länkad till nyckelstorleken för den fordonsenhet eller det kort varifrån dessa data överförs, såsom specificeras i CSM_50.

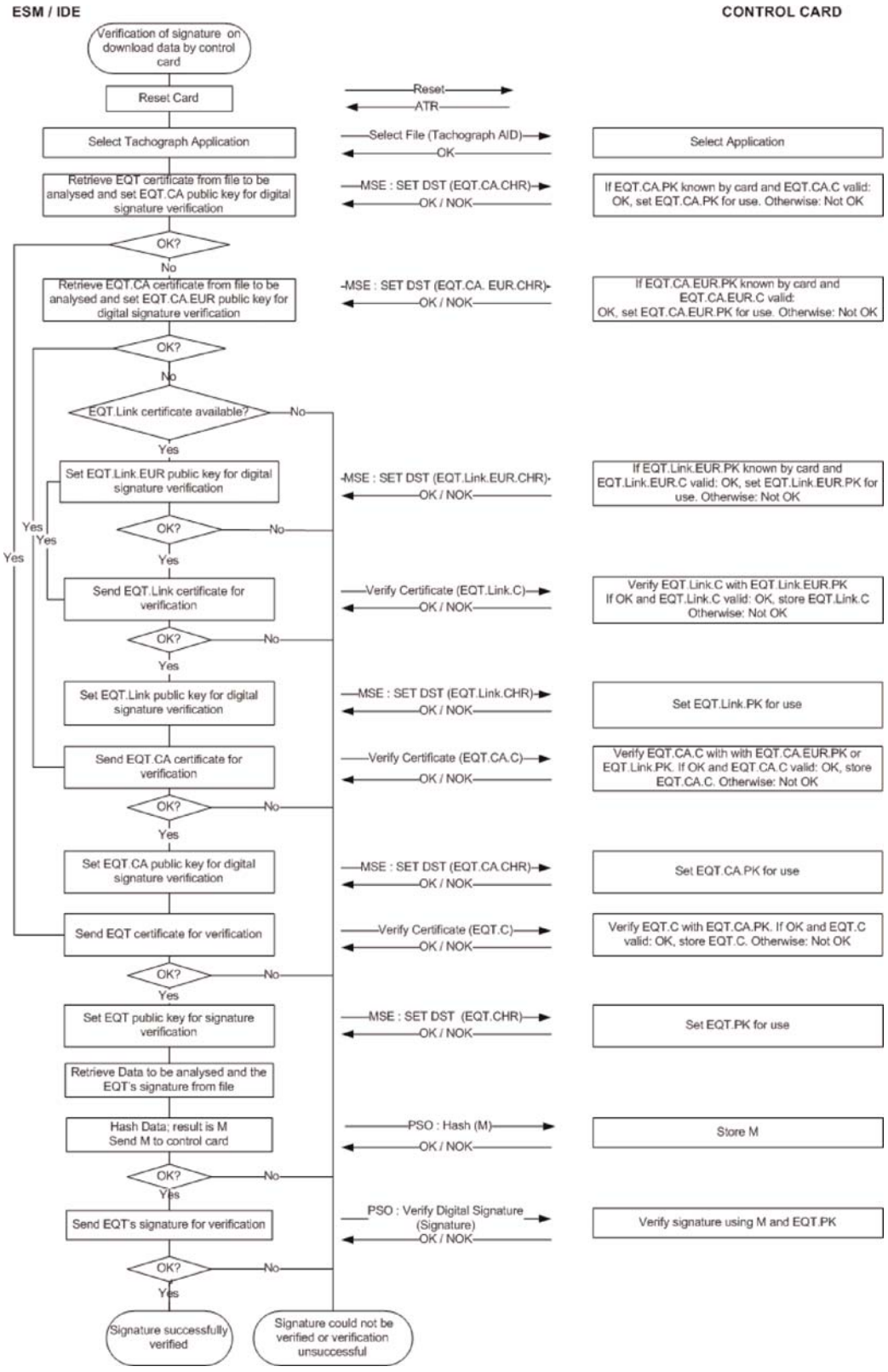
CSM_236 För verifiering av EQT-signaturen ska kontrollkortet följa det signaturschema som definieras i [DSS].

Anmärkning: Detta dokument specificerar inga åtgärder som ska vidtas om en signatur för överförda data inte kan verifieras eller om verifieringen inte lyckas.

▼B

Figur 13

Protokoll för verifiering av signaturen för en överförd datafil



▼B

Tillägg 12

POSITIONSBESTÄMNING BASERAD PÅ GNSS (GLOBAL NAVIGATION SATELLITE SYSTEM)

INNEHÅLLSFÖRTECKNING

1. INLEDNING

1.1. Tillämpningsområde

1.2. Förkortningar och beteckningar

2. SPECIFIKATION FÖR GNSS-MOTTAGARE

3. NMEA-SATSER

4. FORDONSENHET MED EN EXTERN GNSS-ANORDNING

4.1. Konfiguration

4.1.1 Huvudkomponenter och gränssnitt

4.1.2 Status för extern GNSS-anordning i slutet av produktionsprocessen

4.2. Kommunikation mellan den externa GNSS-anordningen och fordonsenheten

4.2.1 Kommunikationsprotokoll

4.2.2 Säker överföring av GNSS-data

4.2.3 Struktur för kommandot READ RECORD

4.3. Den externa GNSS-anordningens koppling, ömsesidiga autentisering och överenskommelse om sessionsnyckel med fordonsenheten

4.4. Felhantering

4.4.1 Fel i kommunikation med extern GNSS-anordning.

4.4.2 Brott mot den externa GNSS-anordningens fysiska integritet

4.4.3 Positionsinformation från GNSS-mottagare saknas

4.4.4 Certifikat för extern GNSS-anordning har löpt ut

5. FORDONSENHET UTAN EXTERN GNSS-ANORDNING

5.1. Konfiguration

5.2. Felhantering

5.2.1 Positionsinformation från GNSS-mottagare saknas

6. KONFLIKT AVSEENDE GNSS-TID

7. KONFLIKT I FORDONETS RÖRELSEDATA

1. INLEDNING

Detta tillägg innehåller de tekniska kraven för de GNSS-data som används av fordonsenheten, inklusive de protokoll som ska införas för att garantera en säker och korrekt dataöverföring av positionsinformation.

Dessa krav baseras huvudsakligen på följande artiklar i förordning (EU) nr 165/2014: Artikel 8 (”Registrering av fordonets position vid vissa punkter under den dagliga arbetsperioden”), artikel 10 (”Gränssnitt med intelligenta transportsystem”) och artikel 11 (”Detaljerade bestämmelser för smarta färdskrivare”).

▼B

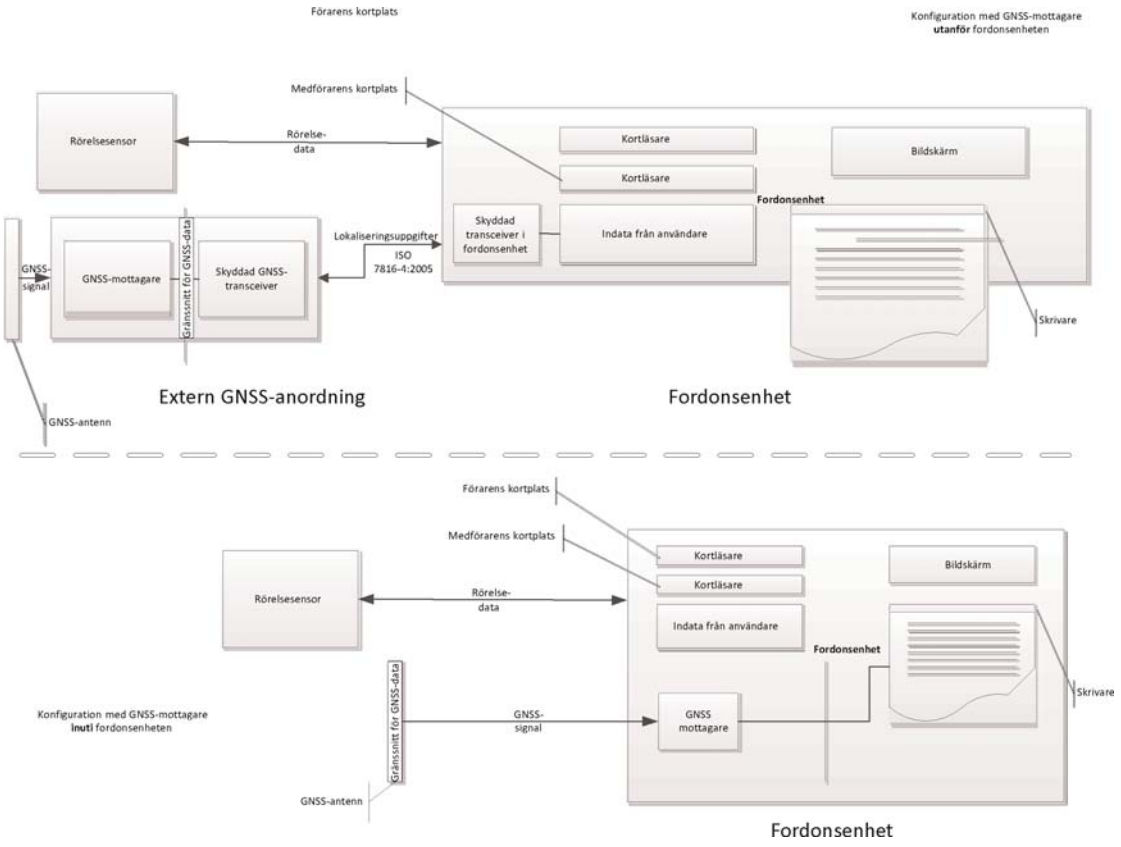
1.1. **Tillämpningsområde**

GNS_1 Fordonsenheten ska samla in lokaliseringsuppgifter från minst ett GNSS som stöd för genomförandet av artikel 8.

Fordonsenheten kan vara, men måste inte vara, utrustad med en extern GNSS-anordning såsom beskrivs i Figure 1.

Figur 1

Olika konfigurationer för GNSS-mottagare



1.2. **Förkortningar och beteckningar**

Följande förkortningar används i detta tillägg:

DOP *Dilution of Precision* (det geometriska bidraget till osäkerheten i en positionsbestämning)

EGF *Elementary file GNSS Facility* (elementfil för GNSS-anordning)

Egnos European Geostationary Navigation Overlay Service

GNSS *Global Navigation Satellite System* (globalt system för satellitnavigering)

GSA *GPS DOP and active satellites* (format för GNSS-positionering)

HDOP *Horizontal Dilution of Precision* (det geometriska bidraget i horisontalplanet till osäkerheten i en positionsbestämning)

ICD *Interface Control Document* (dokument för gränssnittskontroll)

NMEA *National Marine Electronics Association* (organisation verksam inom marinelektronik)

▼B

PDOP Position Dilution of Precision

RMC Recommended Minimum Specific

SIS Signal in Space

VDOP *Vertical Dilution of Precision* (det geometriska bidraget i vertikalplanet till osäkerheten i en positionsbestämning)

VU *Vehicle Unit* (fordonsenhet)

2. SPECIFIKATION FÖR GNSS-MOTTAGARE

Oavsett om en smart färdskrivare är konfigurerad med eller utan en extern GNSS-anordning är tillhandahållandet av säker och tillförlitlig positionsinformation en viktig del av färdskrivarens funktion. Det är därför ett lämpligt krav att den ska vara kompatibel med tjänsterna inom programmen Galileo och Egnos (*European Geostationary Navigation Overlay Service*) enligt Europaparlamentets och rådets förordning (EU) nr 1285/2013 ([1]). Det system som inrättades inom ramen för Galileoprogrammet är ett oberoende globalt satellitnavigeringssystem och det som inrättades inom ramen för Egnosprogrammet är ett regionalt satellitnavigeringssystem som förbättrar kvaliteten på GPS-signalen.

GNS_2 Tillverkarna ska se till att GNSS-mottagare i smarta färdskrivare är kompatibla med positionsbestämningstjänsterna inom Galileo- och Egnossystemen. Tillverkarna får välja om de även ska vara kompatibla med andra satellitnavigeringssystem.

GNS_3 GNSS-mottagaren ska kunna stödja Galileos tjänst *Authentication on the Open Service* när en sådan tillhandahålls av Galileosystemet och stöds av tillverkarna av GNSS-mottagare. Någon eftermontering kommer dock inte att krävas för smarta färdskrivare som inte klarar att stödja Galileos *Authentication on the Open Service* och som introduceras på marknaden innan de ovanstående förhållandena börjar gälla.

3. NMEA-SATSER

I detta avsnitt beskrivs de NMEA-satser som används i den smarta färdskrivarens funktioner. Avsnittet gäller konfigurationen av den smarta färdskrivaren, med eller utan en extern GNSS-anordning.

GNS_4 Lokaliseringsuppgifterna baseras på NMEA-satsen RMC (*Recommended Minimum Specific*) som omfattar GNSS-data i form av positionsinformation (latitud, longitud), tid i UTC-format (hhmmss.ss) och hastighet (*Speed Over Ground*) i knop samt ytterligare värden.

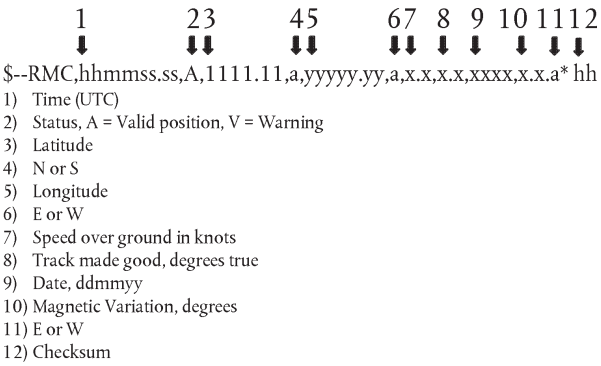
Följande format (från standarden NMEA V4.1) används för RMC-satsen:

([1]) Europaparlamentets och rådets förordning (EU) nr 1285/2013 av den 11 december 2013 om uppbyggnad och drift av de europeiska satellitnavigeringssystemen och om upphävande av rådets förordning (EG) nr 876/2002 och Europaparlamentets och rådets förordning (EG) nr 683/2008 (EUT L 347, 20.12.2013, s. 1).

▼B

Figur 2

RMC-satsens struktur



”Status” indikerar huruvida GNSS-signalen är tillgänglig. Så länge status inte har värdet A kan mottagna data (om t.ex. tid eller latitud/longitud) inte användas för att registrera fordonets position i fördonsenheten.

Positionens upplösning baseras på formatet för den RMC-sats som beskrivs ovan. Den första delen av fälten 3) och 5) (de första två tecknen) används för att representera antalet grader. Resterande tecken används för att representera antalet minuter med tre decimaler. Upplösningen är därmed 1/1000 av en minut eller 1/60000 av en grad (eftersom en minut är 1/60 grad).

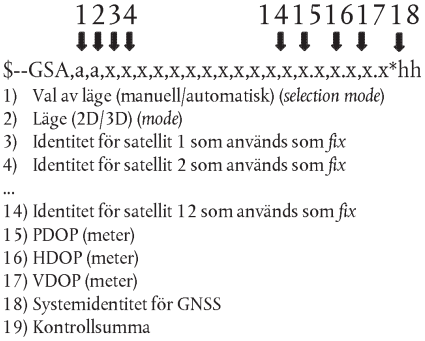
GNS_5 Fordonsenheten ska lagra positionsinformationen för latitud och longitud i sin databas med en upplösning på 1/10 minut eller 1/600 grad, såsom beskrivs i tillägg 1 för datatypen GeoCoordinates.

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 lokaliseringsuppgifter (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.

Systemidentiteten för GNSS anger om det gäller GPS, Glonass, Galileo, Beidou eller SBAS (*Satellite-Based Augmentation System*).

Figur 3

GSA-satsens struktur



▼B

”Läge” (*mode*) (2) anger om en *fix* inte är tillgänglig (Mode=1) eller om en *fix* är tillgänglig i 2D (Mode=2) eller 3D (Mode=3).

GNS_6 *GSA*-satsen ska lagras med postnummer ”06”.

GNS_7 De maximala storleken för NMEA-satser (t.ex. RMC, GSA eller andra), som kan användas för att definiera storleken i kommandot för att läsa poster (READ RECORD), ska vara 85 byte (se Table 1).

4. FORDONSENHET MED EN EXTERN GNSS-ANORDNING

4.1. **Konfiguration**

4.1.1 *Huvudkomponenter och gränssnitt*

I denna konfiguration är GNSS-mottagaren en del av den externa GNSS-anordningen.

GNS_8 Den externa GNSS-anordningens strömförsörjning ska ske med ett särskilt fordonsgränssnitt.

GNS_9 Den externa GNSS-anordningen ska bestå av följande komponenter (se Figure 4):

a) En kommersiell GNSS-mottagare som tillhandahåller positionsdata genom gränssnittet för GNSS-data. Gränssnittet för GNSS-data interface kan t.ex. följa NMEA-standarden V4.10 där GNSS-mottagaren fungerar som talare och överför NMEA-satser till den skyddade GNSS-transceivern (*GNSS Secure Transceiver*) med en frekvens på 1 Hz för en fördefinierad uppsättning av NMEA-satser, som ska omfatta åtminstone RMC- och GSA-satserna. Tillverkaren av den externa GNSS-anordningen avgör hur gränssnittet för GNSS-data ska utformas.

b) En transceiverenhet (nedan kallad *skyddad GNSS-transceiver*) som klarar att uppfylla standarden ISO/IEC 7816-4:2013 (se avsnitt 4.2.1) för kommunikation med fordonsenheten och att ge stöd till GNSS-mottagarens gränssnitt för GNSS-data. Enheten är försedd med ett minne där identifieringsdata lagras för GNSS-mottagaren och den externa GNSS-anordningen.

c) En inkapsling som har en funktion för upptäckt av manipulering och som omsluter både GNSS-mottagaren och den skyddade GNSS-transceivern. Funktionen för upptäckt av manipulering ska motsvara de säkerhets- och skyddsåtgärder som begärs i den smarta färdskrivarens skyddsprofil.

d) En GNSS-antenn som installeras på fordonet och ansluts till GNSS-mottagaren genom inkapslingen.

GNS_10 Den externa GNSS-anordningen har åtminstone följande externa gränssnitt:

a) Gränssnitt med den GNSS-antenn som är installerad på fordonet (om en extern antenn används).

b) Gränssnitt med fordonsenheten.

GNS_11 I fordonsenheten utgör fordonsenhetens skyddade transceiver den andra ändan av den skyddade kommunikationen med den skyddade GNSS-transceivern, och den ska stödja ISO/IEC 7816-4:2013 när det gäller anslutningen till den externa GNSS-anordningen.

▼B

GNS_12 När det gäller det fysiska skiktet för kommunikation med den externa GNSS-anordningen ska fordonsenheten stödja ISO/IEC 7816-12:2005 eller en annan standard som klarar att stödja ISO/IEC 7816-4:2013. (Se avsnitt 4.2.1).

4.1.2 *Status för extern GNSS-anordning i slutet av produktionsprocessen*

GNS_13 Den externa GNSS-anordningen ska när den lämnar fabriken lagra följande värden i den skyddade GNSS-transceiverns permanenta minne:

— Nuvarande EGF_MA-nyckelpar och motvarande certifikat.

— MSCA_VU-EGF-certifikatet som innehåller den öppna nyckeln MSCA_VU-EGF.PK som ska användas för verifiering av EGF_MA-certifikatet.

— EUR-certifikatet som innehåller den öppna nyckeln EUR.PK som ska användas för verifiering av MSCA_VU-EGF-certifikatet.

— EUR-certifikatet vars giltighetstid direkt föregår giltighetstiden för det EUR-certifikat som ska användas för verifiering av MSCA_VU-EGF-certifikatet, i förekommande fall.

— Det länkcertifikat som länkar dessa två EUR-certifikat, i förekommande fall.

— Den externa GNSS-anordningens förlängda serienummer.

— Identifierare för GNSS-anordningens operativsystem.

— Den externa GNSS-anordningens typgodkännandenummer.

— Identifierare för den externa GNSS-anordningens säkerhetskomponent.

4.2. **Kommunikation mellan den externa GNSS-anordningen och fordonsenheten**

4.2.1 *Kommunikationsprotokoll*

GNS_14 Protokollet för kommunikation mellan den externa GNSS-anordningen och fordonsenheten ska stödja tre funktioner:

1. Insamling och distribuering av GNSS-data (t.ex. position, tidsavpassning, hastighet).

2. Insamling av konfigurationsdata för den externa GNSS-anordningen.

3. Styrning, som stöd för koppling, ömsesidig autentisering och överenskommelse om sessionsnyckel mellan den externa GNSS-anordningen och fordonsenheten.

GNS_15 Kommunikationsprotokollet ska baseras på standarden ISO/IEC 7816-4:2013, med fordonsenhetens skyddade transceiver som ”master” och den skyddade GNSS-transceivern som ”slave”. Den fysiska anslutningen mellan den externa GNSS-anordningen och fordonsenheten baseras på ISO/IEC 7816-12:2005 eller en annan standard som klarar att stödja ISO/IEC 7816-4:2013.

▼B

GNS_16 Kommunikationsprotokollet stöder inte fält med utökad längd.

GNS_17 Kommunikationsprotokollet enligt ISO 7816 (gäller både ISO 7816 4:2013 och ISO 7816-12:2005) mellan den externa GNSS-anordningen och fordonsenheten ska ställas in så att T=1.

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-transceivern 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 kapitel 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 Table 1.

GNS_19 Den skyddade GNSS-transceivern ska lagra de data som kommer from GNSS-mottagaren och dess konfiguration i elementfilen EF.EGF. Detta är en linjär fil med poster med variabel längd och identifieraren ‘2F2F’ i hexadecimalt format.

GNS_20 Den skyddade GNSS-transceivern 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-transceivern utformas och realiseras.

Mappning av postnummer och data visas i Table 1. Notera att det finns fyra GSA-satser för de fyra satellitsystemen och för SBAS (*Satellite-Based Augmentation System*).

GNS_21 Filstrukturen visas i Table 1. För information om tillträdesvillkor (ALW, NEV, SM-MAC), se kapitel 3.5 i tillägg 2.

Tabell 1

Filstruktur

		Tillträdesvillkor		
Fil	Fil-ID	Läs (*Read*)	Uppdatera (*Update*)	Krypterad
MF	3F00			
EF.ICC	0002	ALW	NEV (gäller fordonsenhet)	Nej
DF GNSS Facility	0501	ALW	NEV	Nej
EF EGF_MACertificate	C100	ALW	NEV	Nej
EF CA_Certificate	C108	ALW	NEV	Nej
EF Link_Certificate	C109	ALW	NEV	Nej
EF.EGF	2F2F	SM-MAC	NEV (gäller fordonsenhet)	Nej

▼B

Fil/dataelement	Postnummer	Storlek (byte)		Standardvärden
		Min.	Max.	
MF		552	1 031	
EF.ICC				
sensorGNSSSerialNumber		8	8	
DF GNSS Facility		*612*	*1 023*	
EF EGF_MACertificate		*204*	*341*	
EGFCertificate		204	341	{00..00}
EF CA_Certificate		*204*	*341*	
MemberStateCertificate		204	341	{00..00}
EF Link_Certificate		*204*	*341*	
LinkCertificate		204	341	{00..00}
EF.EGF				
RMC-sats (NMEA)	‘01’	85	85	
GSA-sats nr 1 (NMEA)	‘02’	85	85	
GSA-sats nr 2 (NMEA)	‘03’	85	85	
GSA-sats nr 3 (NMEA)	‘04’	85	85	
GSA-sats nr 4 (NMEA)	‘05’	85	85	
GSA-sats nr 5 (NMEA)	‘06’	85	85	
Förlängt serienummer för den externa GNSS-anordningen, definierad i tillägg 1 som SensorGNSSSerialNumber.	‘07’	8	8	
Identifierare för operativsystemet i den skyddade GNSS-transceivern, definierad i tillägg 1 som SensorOSIdentifier.	‘08’	2	2	
Typgodkännandenummer för den externa GNSS-anordningen, definierat i tillägg 1 som SensorExternalGNSSApprovalNumber.	‘09’	16	16	
Identifierare för den externa GNSS-anordningens säkerhetskomponent, definierad i tillägg 1 som SensorExternalGNSSSCIdentifier.	‘10’	8	8	
RFU (*Reserved for Future Use*)	Från ‘11’ till ‘FD’			

4.2.2 *Säker överföring av GNSS-data*

GNS_22 En skyddad överföring av positionsdata från GNSS ska tillåtas endast under på följande villkor:

1. Kopplingsprocessen har slutförts såsom beskrivs i tillägg 11 om gemensamma säkerhetsmekanismer.

▼B

2. Den periodiska ömsesidiga autentiseringen och överenskommelsen om sessionsnycklar mellan fordonsenheten och den externa GNSS-anordningen, som också beskrivs i tillägg 11 om gemensamma säkerhetsmekanismer, har genomförts med den angivna frekvensen.

GNS_23 Fordonsenheten begär, med ett intervall på T sekunder där värdet för T är högst 10, och med undantag för när koppling, ömsesidig autentisering och överenskommelse om sessionsnyckel pågår, positionsinformation från den externa GNSS-anordningen, baserat på följande flöde:

1. Fordonsenheten begär lokaliseringsuppgifter från den externa GNSS-anordningen tillsammans med DOP-data (från GSA-satsen enligt NMEA). Fordonsenhetens skyddade transceiver ska använda kommandona SELECT och READ RECORD(S) enligt ISO/IEC 7816-4:2013 för säker meddelandehantering och endast autentisering (*secure messaging authentication-only mode*) såsom beskrivs i avsnitt 11.5 i tillägg 11, med filidentifierare ”2F2F” och postnummer (RECORD) ‘01’ för RMC-satsen enligt NMEA och‘02’,‘03’,‘04’,‘05’ respektive ‘06’ för respektive GSA-sats enligt NMEA.

2. De senast mottagna lokaliseringsuppgifterna lagras i elementfilen med identifierare ‘2F2F’ och posterna som beskrivs i Table 1 lagras i den skyddade GNSS-transceivern allt eftersom den tar emot NMEA-data från GNSS-mottagaren med en frekvens på minst 1 Hz via gränssnittet för GNSS-data.

3. Den skyddade GNSS-transceivern sänder ett svar till fordonsenhetens skyddade transceiver med hjälp av ett svarsmeddelande (APDU) med säker meddelandehantering och endast autentisering såsom beskrivs i avsnitt 11.5 i tillägg 11.

4. Fordonsenhetens skyddade transceiver kontrollerar det mottagna svarets autenticitet och integritet. Om resultatet är positivt överförs lokaliseringsuppgifterna till fordonsenhetens processor via gränssnittet för GNSS-data.

5. Fordonsenhetens processor kontrollerar mottagna data genom att hämta information (t.ex. latitud, longitud 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 medelvärdet från de tillgängliga satellitsystemen (dvs. när en *fix* är tillgänglig).

6. Fordonsenhetens processor lagrar den mottagna och bearbetade informationen, t.ex. latitud, longitud, tid och hastighet, i fordonsenheten och i det format som definieras i tillägg 1 om datakatalogen. Den lagras som GeoCoordinates tillsammans med HDOP-värdet beräknat som det minsta av de HDOP-värden som samlas in från de tillgängliga GNSS-systemen.

▼B

4.2.3 *Struktur för kommandot READ RECORD*

I detta avsnitt beskrivs strukturen för kommandot READ RECORD i detalj. Säker meddelandehantering och endast autentisering läggs till såsom beskrivs i tillägg 11 om gemensamma säkerhetsmekanismer.

GNS_24 Kommandot ska stödja säker meddelandehantering med endast autentisering – se tillägg 11.

GNS_25 Kommandomeddelande

Byte	Längd	Värde	Beskrivning
CLA	1	‘0Ch’	Säker meddelandehantering efterfrågad.
INS	1	‘B2h’	Läs post (READ RECORD)
P1	1	‘XXh’	Postnummer (‘00’ hänvisar till den aktuella posten).
P2	1	‘04h’	Läs posten med det postnummer som anges i P1.
Le	1	‘XXh’	Längd på förväntade data. Antal byte som skall läsas

GNS_26 Den post som anges i P1 blir aktuell post.

Byte	Längd	Värde	Beskrivning
#1-#X	X	‘XX..XXh’	Läs data
SW	2	‘XXXXh’	Statusregister (SW1,SW2)

— Om kommandot lyckas återsänder den skyddade GNSS-transceivern ‘**9000**’.

— Om den aktuella filen inte är avsedd för poster återsänder den skyddade GNSS-transceivern ‘**6981**’.

— Om kommandot används med P1 = ‘00’ men det inte finns någon elementfil som aktuell fil återsänder den skyddade GNSS-transceivern ‘**6986**’ (kommandot ej tillåtet).

— Om posten inte kan hittas återsänder den skyddade GNSS-transceivern ‘**6A 83**’.

— Om den externa GNSS-anordningen har upptäckt manipulering ska den återsända ‘**66 90**’ som statusregister.

GNS_27 Den skyddade GNSS-transceivern ska stödja följande kommandon för färdskrivare i generation 2, som specificeras i tillägg 2:

Kommando	Referens
Select	Tillägg 2 kapitel 3.5.1
READ BINARY	Tillägg 2 kapitel 3.5.2
GET CHALLENGE	Tillägg 2 kapitel 3.5.4
PSO: VERIFY CERTIFICATE	Tillägg 2 kapitel 3.5.7
EXTERNAL AUTHENTICATE	Tillägg 2 kapitel 3.5.9
GENERAL AUTHENTICATE	Tillägg 2 kapitel 3.5.10
MSE:SET	Tillägg 2 kapitel 3.5.11

▼B

4.3. **Den externa GNSS-anordningens koppling, ömsesidiga autentisering och överenskommelse om sessionsnyckel med fordonsenheten**

Den externa GNSS-anordningens koppling, ömsesidiga autentisering och överenskommelse om sessionsnyckel med fordonsenheten beskrivs i kapitel 11 i tillägg 11 om gemensamma säkerhetsmekanismer.

4.4. **Felhantering**

I detta avsnitt beskrivs hur möjliga feltillstånd avseende den externa GNSS-anordningen tas om hand och registreras i fordonsenheten.

4.4.1 *Fel i kommunikation med extern GNSS-anordning.*

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 ‘53’H *(Externt fel i GNSS-kommunikation)* 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.

4.4.2 *Brott mot den externa GNSS-anordningens fysiska integritet*

GNS_29 Om den externa GNSS-anordningen har öppnats fysiskt ska den skyddade GNSS-transceivern radera hela sitt minne, inklusive krypteringsuppgifter. Fordonsenheten ska påvisa manipulering om svaret har status ‘6690’, såsom beskrivs i GNS_25 och GNS_26. Fordonsenheten ska då generera en händelse med typen EventFaultType och värdet ‘55’H *(GNSS-manipulering upptäckt)*.

4.4.3 *Positionsinformation från GNSS-mottagare saknas*

GNS_30 Om den skyddade GNSS-transceivern inte tar emot data från GNSS-mottagaren under mer än tre sammanhängande timmar ska den skyddade GNSS-transceivern 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 ‘52’H (Externt fel i GNSS-mottagare), 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.

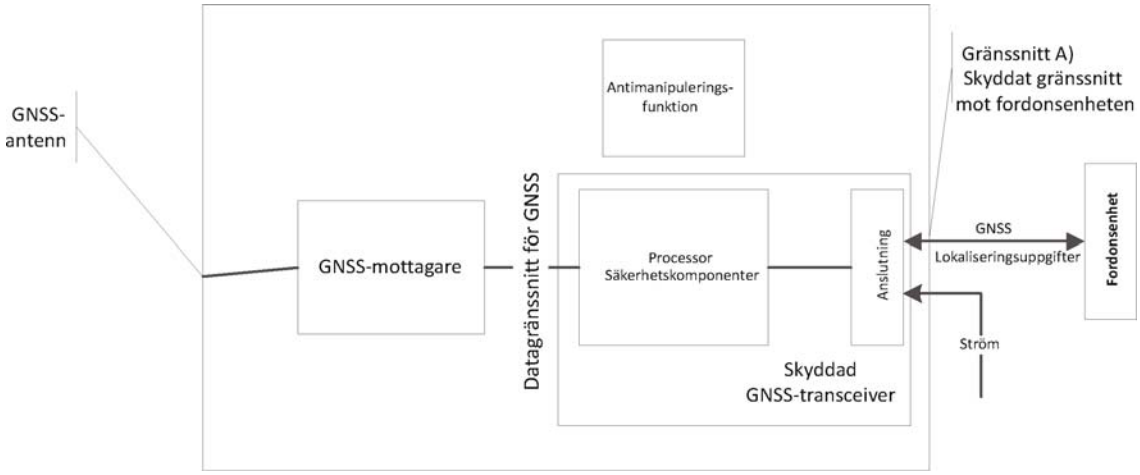
4.4.4 *Certifikat för extern GNSS-anordning har löpt ut*

GNS_31 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 ‘56’(Certifikat för extern GNSS-anordning har löpt ut), med den aktuella tiden som tidsstämpel. Fordonsenheten ska fortfarande använda mottagna positionsdata från GNSS.

▼B

Figur 4

Skiss av extern GNSS-anordning



5. FORDONSENHET UTAN EXTERN GNSS-ANORDNING

5.1. **Konfiguration**

I denna konfiguration ingår GNSS-mottagaren i fordonsenheten såsom visas i Figure 1.

GNS_32 GNSS-mottagaren ska fungera som talare och överföra NMEA-satser till fordonsenhetens processor, som ska fungera som lyssnare, med en frekvens på 1/10 Hz eller snabbare för en fördefinierad uppsättning av NMEA-satser som åtminstone ska omfatta RMC- och GSA-satserna.

GNS_33 En extern GNSS-antenn ska installeras på fordonet, eller en intern GNSS-antenn ska anslutas till fordonsenheten.

5.2. **Felhantering**

5.2.1 *Positionsinformation från GNSS-mottagare saknas*

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 ‘51’H (Internt fel i GNSS-mottagare), 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.

6. KONFLIKT AVSEENDE GNSS-TID

Om fordonsenheten upptäcker en avvikelse på mer än 1 minut mellan tiden i fordonsenhetens tidmätningsfunktion och den tid som har sitt ursprung i GNSS-mottagaren ska fordonsenheten registrera en händelse med typen EventFaultType och värdet ‘0B’H (Tidskonflikt (GNSS jämfört med fordonsenhetens interna klocka)). Denna händelse registreras tillsammans fordonsenhetens interna klockvärde och åtföljs av en automatisk tidsinställning. Efter det att en händelse av typen tidskonflikt har utlösts kommer fordonsenhet inte att kontrollera tidsavvikelsen under de närmast följande 12 timmarna. Denna händelse ska inte utlösas om GNSS-mottagaren inte känt av någon giltig GNSS-signal under de föregående 30 dagarna. Den automatiska tidsinställningen ska dock göras när positionsinformation från GNSS-mottagaren är tillgänglig igen.

▼B

7. KONFLIKT I FORDONETS RÖRELSEDATA

GNS_35 Fordonsenheten ska utlösa och registrera en händelse avseende konflikt i fordonets rörelsedata (se krav 84 i denna bilaga), med den aktuella tiden som tidsstämpel, om rörelseinformation som beräknas från rörelsesensorn motsägs av rörelseinformation som beräknas från den interna GNSS-mottagaren eller från den externa GNSS-anordningen. För att upptäcka sådana motsägelser ska medianvärdet för hastighetsskillnaderna mellan de olika källorna användas, såsom anges nedan:

— Var 10:e sekund eller oftare ska absolutvärdet för skillnaden mellan fordonets hastighet enligt GNSS och fordonets hastighet enligt rörelsesensorn beräknas.

— Samtliga beräknade värden inom ett tidsfönster som omfattar de senaste fem minuterna av rörelse ska användas för att beräkna medianvärdet.

— Medianvärdet ska baseras på 80 % av värdena, efter att de största absolutvärdena har tagits bort.

Händelsen avseende konflikt i fordonets rörelsedata ska utlösas om medianvärdet är mer än 10 km/h under fem minuter med fordonet i rörelse utan avbrott. Andra oberoende källor för avläsning av fordonsrörelse får användas som alternativ så att en mer tillförlitlig upptäckt av färdskrivarmanipulering tillhandahålls. (Anm.: Användningen av medianen för de senaste fem minuterna tillämpas för att minska risken med avvikande och transienta värden.) Denna händelse ska inte utlösas under följande omständigheter: a) under transport med färja/tåg; b) när positionsinformation från GNSS-mottagaren inte ska vara tillgänglig; c) i kalibreringsläge.

▼B

Tillägg 13

ITS-GRÄNSSNITT

INNEHÅLLSFÖRTECKNING

1. INLEDNING

2. TILLÄMPNINGSOMRÅDE

2.1. Förkortningar, definitioner och beteckningar

3. HÄNVISNINGAR TILL FÖRORDNINGAR OCH STANDARDER

4. GRÄNSSNITTETS FUNKTIONSSÄTT

4.1. Nödvändiga förutsättningar för dataöverföring via ITS-gränssnittet

4.1.1 Data som tillhandahålls genom ITS-gränssnittet

4.1.2 Datainnehåll

4.1.3 ITS-tillämpningar

4.2. Kommunikationsteknologi

4.3. PIN-auktorisering

4.4. Meddelandeformat

4.5. Förarens samtycke

4.6. Hämtning av standarddata

4.7. Hämtning av personuppgifter

4.8. Hämtning av data om händelser och fel

1. INLEDNING

I detta tillägg anges den utformning och de förfaranden som gäller för införande av gränssnittet med ITS (*Intelligent Transport Systems*) såsom krävs i artikel 10 i förordning (EU) nr 165/2014 (nedan kallad *förordningen*).

I *förordningen* anges att färdskrivare i fordon får vara utrustade med standardiserade gränssnitt så att de uppgifter som registrerats eller framställts av färdskrivaren kan användas i driftläge av en extern anordning, under förutsättning att följande villkor är uppfyllda:

a) Gränssnittet påverkar inte autenticiteten och integriteten hos uppgifterna i färdskrivaren.

b) Gränssnittet uppfyller de detaljerade bestämmelserna i artikel 11 i förordningen.

c) Den externa anordning som är ansluten till gränssnittet får tillgång till personuppgifter, inklusive positionsbestämningsuppgifter, först efter ett verifierbart samtycke från den förare uppgifterna gäller.

2. TILLÄMPNINGSOMRÅDE

Syftet med detta tillägg är att specificera hur tillämpningar i externa anordningar kan hämta *data* från en färdskrivare via en Bluetooth®-anslutning.

De *data* som är tillgängliga via detta gränssnitt beskrivs i bilaga 1 till detta tillägg. Detta gränssnitt förhindrar inte att andra gränssnitt (t.ex. via CAN-buss) införs för att överföra fordonenhetens data till andra databehandlingsenheter i fordonet.

▼B

I detta tillägg specificeras följande:

— De *data* som är tillgängliga genom ITS-gränssnittet.

— Den Bluetooth®-profil som används för att överföra data.

— Procedurer för förfrågan och överföring, samt i vilken ordning de olika operationerna sker.

— Parningsmekanismen mellan färdskrivaren och den externa anordningen.

— Den mekanism för samtycke som föraren har tillgång till.

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 det som gäller Bluetooth® (t.ex. kryptering) och som rör innehållet i *data* (dessa ska specificeras på annat ställe i *förordningen*, nämligen i tillägg 10 om gemensamma säkerhetsmekanismer).

— De Bluetooth®-protokoll som används av ITS-gränssnittet.

2.1. **Förkortningar, definitioner och beteckningar**

Följande förkortningar och definitioner som är särskilda för detta tillägg används i detta tillägg:

Kommunikation	Utbyte av information/data mellan en masterenhet (dvs. färdskrivaren) och en extern enhet via ITS-gränssnittet och Bluetooth®.
Data	De datamängder som specificeras i bilaga 1.
Förordningen	Europaparlamentets och rådets förordning (EU) nr 165/2014 av den 4 februari 2014 om färdskrivare vid vägtransporter, om upphävande av rådets förordning (EEG) nr 3821/85 om färdskrivare vid vägtransporter och om ändring av Europaparlamentets och rådets förordning (EG) nr 561/2006 om harmonisering av viss sociallagstiftning på vägtransportområdet.
BR	*Basic Rate* (bashastighet)
EDR	*Enhanced Data Rate* (förhöjd hastighet)
GNSS	*Global Navigation Satellite System* (globalt system för satellitnavigering)
IRK	*Identity Resolution Key* (nyckel för identitetsbestämning)
ITS	*Intelligent Transport System* (intelligent transportsystem)
LE	*Low Energy* (lågenergiversion av Bluetooth®)
PIN	*Personal Identification Number* (personligt identifieringsnummer)
PUC	*Personal Unblocking Code* (personlig avblockeringskod)
SID	*Service Identifier* (tjänsteidentifierare)
SPP	*Serial Port Profile* (serieportprofil)

▼B

SSP	*Secure Simple Pairing* (skyddad enkel parning)
TRTP	*Transfer Request Parameter* (parameter för begäran om överföring)
TREP	*Transfer Response Parameter* (parameter för överföringssvar)
VU	*Vehicle Unit* (fordonsenhet)

3. HÄNVISNINGAR TILL FÖRORDNINGAR OCH STANDARDER

Den specifikation som definieras i detta tillägg hänvisar till och är beroende av hela eller delar av följande förordningar och standarder. I respektive avsnitt i detta tillägg anges de relevanta standarderna eller de relevanta avsnitten i standarderna. I händelse av motstridiga uppgifter ska avsnitten i detta tillägg ha företräde.

I detta tillägg hänvisas till följande förordningar och standarder:

— Europaparlamentets och rådets förordning (EU) nr 165/2014 av den 4 februari 2014 om färdskrivare vid vägtransporter, om upphävande av rådets förordning (EEG) nr 3821/85 om färdskrivare vid vägtransporter och om ändring av Europaparlamentets och rådets förordning (EG) nr 561/2006 om harmonisering av viss sociallagstiftning på vägtransportområdet.

— Europaparlamentets och rådets förordning (EG) nr 561/2006 av den 15 mars 2006 om harmonisering av viss sociallagstiftning på vägtransportområdet och om ändring av rådets förordningar (EEG) nr 3821/85 och (EG) nr 2135/98 samt om upphävande av rådets förordning (EEG) nr 3820/85.

— ISO 16844 – 4: Road vehicles – Tachograph systems – Part 4: Can interface

— ISO 16844 – 7: Road vehicles – Tachograph systems – Part 7: Parameters

— Bluetooth® – Serial Port Profile – V1.2

— Bluetooth® – Core Version 4.2

— NMEA 0183 V4.1 protocol

4. GRÄNSSNITTETS FUNKTIONSSÄTT

4.1. **Nödvändiga förutsättningar för dataöverföring via ITS-gränssnittet**

Fordonsenheten ska ansvara för att data som lagras i fordonsenheten uppdateras och underhålls, utan någon inblandning av ITS-gränssnittet. Detta uppnås genom fordonsenhetens interna funktioner, som specificeras på annat ställe i förordningen och därför inte i detta tillägg.

4.1.1 *Data som tillhandahålls genom ITS-gränssnittet*

Fordonsenheten ska ansvara för att uppdatera de data som ska vara tillgängliga genom ITS-gränssnittet, med en frekvens som bestäms i fordonsenhetens procedurer och utan någon inblandning av ITS-gränssnittet. Data från fordonsenheten ska användas som grund för att populera och uppdatera *data.* Medlen för att åstadkomma detta anges i förordningen eller, om detta saknas, följer av produktens utformning, och specificeras inte i detta tillägg.

▼B

4.1.2 *Datainnehåll*

Innehållet i *data* ska vara det som specificeras i bilaga 1 till detta tillägg.

4.1.3 *ITS-tillämpningar*

ITS-tillämpningar kommer att använda de data som görs tillgängliga genom ITS-gränssnittet för att hantera t.ex. optimering av förarens aktiviteter, med hänsyn tagen till förordningen, för att upptäcka eventuella fel i färdskrivaren eller för att använda GNSS-data. Specifikationer för sådana tillämpningar ligger inte inom detta tilläggs tillämpningsområde.

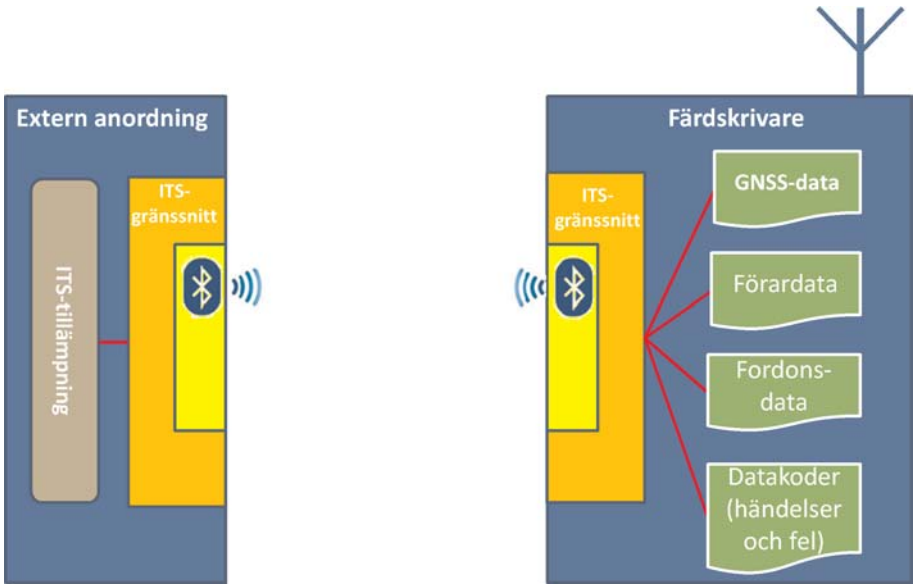
4.2. **Kommunikationsteknologi**

Utbyte av *data* med hjälp av ITS-gränssnittet ska utföras via ett Bluetooth®-gränssnitt som är kompatibelt med version 4.2 eller senare. Bluetooth® verkar inom det licensfria ISM-bandet (*Industrial, Scientific, Medical*, frekvensband för industriellt, vetenskapligt och medicinskt bruk) mellan 2,4 och 2,485 GHz. Bluetooth® 4.2 innebär förbättrade integritetsskydds- och säkerhetsmekanismer samt snabbare och mer tillförlitlig dataöverföring. I denna specifikation används Bluetooth® klass 2 med ett avstånd upp till 10 meter. Mer information om Bluetooth® 4.2 finns på www.bluetooth.com (https://www.bluetooth.org/en-us/specification/adopted-specifications?_ga=1.215147412.2083380574.1435305676).

Kommunikationen ska upprättas med kommunikationsutrustningen efter det att en parningsprocess slutförts med hjälp av en auktoriserad extern anordning. I Bluetooth® används en ”master-slave”-modell för att kontrollera när och varifrån externa anordningar kan sända data. Färdskrivaren utgör ”master” medan den externa anordningen utgör ”slave”.

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 att lägga till krypteringsmekanismer utöver dem som tillhandahålls genom Bluetooth®. Om ytterligare säkerhetsmekanismer ändå behövs kommer dessa att utformas i enlighet med tillägg 10 om gemensamma säkerhetsmekanismer.

Den övergripande kommunikationsprincipen visas i följande figur.



▼B

Serieportprofilen (SPP) enligt Bluetooth® ska användas för att överföra data från fordonsenheten till den externa anordningen.

4.3. **PIN-auktorisering**

Fordonsenheten ska av säkerhetsskäl genomföra en PIN-kodsauktorisering som är separerad 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.

Om anordningen klarar att ange PIN ska den registreras på ”vita listan”. Vita listan ska kunna lagra minst 64 anordningar som är parade med den berörda fordonsenheten.

Om anordningen misslyckas tre gånger i följd med att ange rätt PIN-kod ska den tillfälligt registreras på ”svarta listan”. Medan en anordning är svartlistad ska varje nytt försök till kommunikation från anordningen avvisas. Om anordningen på nytt misslyckas tre gånger i följd med att ange rätt PIN-kod ska svartlistningstiden förlängas (se tabell 1). Om rätt PIN-kod tillhandahålls ska svartlistningstiden och antalet försök återställas. I figur 1 i bilaga 2 visas ett sekvensdiagram för ett försök till PIN-validering.

Tabell 1

Svartlistningstid beroende på antal på varandra följande misslyckade försök att ge rätt PIN-kod

Antal misslyckade försök i följd	Svartlistningstid
3	30 sekunder
6	5 minuter
9	1 timme
12	24 timmar
15	Permanent

Om den externa anordningen (nedan även kallad ITS-enhet) misslyckas 15 (5 × 3) gånger i följd med att ange rätt PIN-kod ska den svartlistas permanent. Denna permanenta svartlistning kan upphävas enbart genom att rätt PUC anges.

PUC ska bestå av åtta siffror och tillhandahållas av tillverkaren tillsammans med fordonsenheten. Om ITS-enheten misslyckas tio gånger i följd med att ange rätt PUC ska svartlistningen vara oåterkallelig.

Även om tillverkaren får erbjuda ett alternativ där PIN-koden kan ändras direkt i fordonsenheten får det inte vara möjligt att ändra PUC. Om det är möjligt att ändra PIN-koden ska det krävas att den nuvarande PIN-koden matas in direkt i fordonsenheten.

Dessutom ska anordningar som finns på vita listan kvarstå tills de tas bort manuellt av användaren (t.ex. via fordonsenhetens människa-maskingränssnitt eller på annat sätt). På detta sätt kan förlorade eller stulna ITS-enheter tas bort från vita listan. Dessutom ska en ITS-enhet som finns utanför räckvidden för Bluetooth under mer än 24 timmar automatiskt strykas från fordonsenhetens vita lista, och rätt PIN-kod ska anges när anslutningen återupprättas.

▼B

Formatet för meddelanden mellan fordonsenhetens ITS-gränssnitt och fordonsenheten definieras inte här utan överlåts till tillverkaren att definiera. Tillverkaren ska dock säkerställa att formatet för meddelanden mellan ITS-enheten och fordonsenheten beaktas (se ASN.1-specifikationer).

Varje begäran om data ska därmed besvaras med en korrekt verifiering av avsändarens uppgifter före varje form av behandling. I figur 2 i bilaga 2 visas ett sekvensdiagram för denna procedur. En svartlistad anordning ska få ta emot en automatisk avvisning. En anordning som varken finns på svarta listan eller vita listan ska få ta emot en begäran om PIN-kod som ska uppfyllas innan några data sänds tillbaka som svar på begäran.

4.4. **Meddelandeformat**

Alla meddelanden som utbyts mellan ITS-enheten och fordonsenhets gränssnitt ska formateras med en struktur som består av följande tre delar: Startdel (*header*) bestående av en byte för mål (TGT), en byte för källa (SRC) och en byte för längd (LEN).

Datafält bestående av en byte för tjänsteidentifierare (SID) och ett varierande antal byte för data (maximalt 255).

Byte för kontrollsumma innehåller 1 bits-summorna modulo 256 av alla byte i meddelandet, med undantag för kontrollsumman själv.

Meddelandet ska ha byteordningen Big Endian.

Tabell 2

Allmänt meddelandeformat

Startdel (*header*)			Datafält					Kontrollsumma
TGT	SRC	LEN	SID	TRTP	CC	CM	DATA	CS
3 byte			Max. 255 byte					1 byte

Startdel (header)

TGT och SRC: Identitet för den anordning som utgör meddelandets mål (TGT) respektive källa (SRC). Fordonsenhetens gränssnitt ska som standardvärde ha identiteten ”EE”. Denna identitet kan inte ändras. ITS-enheten ska som standardvärde använda identiteten ”A0” i sitt första meddelande i kommunikationssessionen. Fordonsenhetens gränssnitt ska sedan tilldela en unik identitet till ITS-enheten och meddela denna till ITS-enheten, och ITS-enheten ska använda denna identitet i efterföljande meddelanden i sessionen.

Byte för LEN ska endast ta hänsyn till datadelen av datafältet (se tabell 2), inledande 4 byte är underförstådda.

Fordonsenhetens gränssnitt ska bekräfta autenticiteten för meddelandets avsändare genom att i sin egen identitetslista (*IDList*) med Bluetooth-data dubbelkontrollera att den ITS-enhet som hör samman med den tillhandahållna identiteten finns inom Bluetooth-anslutningens räckvidd.

Datafält

Utöver SID ska datafältet också innehålla andra parametrar: en TRTP för begäran om överföring och byte för räknare.

▼B

Om de data som behöver överföras är längre än det utrymme som finns tillgängligt i ett meddelande delas det upp i flera undermeddelanden. Varje undermeddelande ska 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.

Om CC och CM inte används ska de tilldelas värdet 0xFF.

Exempelvis ska meddelandet

HEADER	SID	TRTP	CC	CM	DATA	CS
3 byte	Längre än 255 byte					1 byte

överföras som

HEADER	SID	TRTP	01	n	DATA	CS
3 byte	255 byte					1 byte

HEADER	SID	TRTP	02	n	DATA	CS
3 byte	255 byte					1 byte

…

HEADER	SID	TRTP	N	N	DATA	CS
3 byte	Max. 255 byte					1 byte

Tabell 3 innehåller de meddelanden som fordonsenheten och ITS-enheten ska kunna utväxla. Innehållet i respektive parameter anges i hexadecimal form. För tydlighetens skull visas inte CC och CM i tabellen. Det fullständiga formatet visas ovan.

Tabell 3

Meddelandeinnehåll i detalj

Meddelande	Startdel (*header*)			DATA			Kontroll-summa
	TGT	SRC	LEN	SID	TRTP	DATA	
RequestPIN	*ITSID*	EE	00	01	FF		
SendITSID	*ITSID*	EE	01	02	FF	*ITSID*	
SendPIN	EE	*ITSID*	04	03	FF	4*INTEGER (0..9)	
PairingResult	*ITSID*	EE	01	04	FF	BOOLEAN (T/F)	
SendPUC	EE	*ITSID*	08	05	FF	8*INTEGER (0..9)	

▼B

Meddelande	Startdel (*header*)			DATA			Kontroll-summa
	TGT	SRC	LEN	SID	TRTP	DATA	
BanLiftingResult	*ITSID*	EE	01	06	FF	BOOLEAN (T/F)	
RequestRejected	*ITSID*	EE	08	07	FF	Tid	
RequestData							
standardTachData	EE	*ITSID*	01	08	01		
personalTachData	EE	*ITSID*	01	08	02		
gnssData	EE	*ITSID*	01	08	03		
standardEventData	EE	*ITSID*	01	08	04		
personalEventData	EE	*ITSID*	01	08	05		
standardFaultData	EE	*ITSID*	01	08	06		
manufacturerData	EE	*ITSID*	01	08	07		
ResquestAccepted	*ITSID*	EE	Len	09	TREP	Data	
DataUnavailable							
Inga data tillgängliga	*ITSID*	EE	02	0 A	TREP	10	
Personuppgifter delas inte	*ITSID*	EE	02	0 A	TREP	11	
NegativeAnswer							
Allmänt avvisande	*ITSID*	EE	02	0 B	SID Req	10	
Tjänsten stöds ej	*ITSID*	EE	02	0 B	SID Req	11	
Underfunktion stöds ej	*ITSID*	EE	02	0 B	SID Req	12	
Fel meddelande-längd	*ITSID*	EE	02	0 B	SID Req	13	
Fel omständigheter eller sekvensfel för begäran	*ITSID*	EE	02	0 B	SID Req	22	
Begäran utanför tillåtet intervall	*ITSID*	EE	02	0 B	SID Req	31	
Svar dröjer	*ITSID*	EE	02	0 B	SID Req	78	
ITSID stämmer inte	*ITSID*	EE	02	0 B	SID Req	FC	
ITSID saknas	*ITSID*	EE	02	0 B	SID Req	FB	

RequestPIN (SID 01)

Detta meddelande sänds från fordonsenhetens gränssnitt om en begäran om data tas emot från en ITS-enhet som varken finns på svarta listan eller vita listan.

▼B

SendITSID (SID 02)

Detta meddelande sänds från fordonsenhetens gränssnitt när en begäran om data tas emot från en ny anordning. Denna anordning ska som standardvärde använda identiteten ”A0” innan den tilldelas en unik identitet för kommunikationssessionen.

SendPIN (SID 03)

Detta meddelande sänds från ITS-enheten för att den ska vitlistas i fordonsenhetens gränssnitt. Meddelandet innehåller en kod på fyra heltal (INTEGER) mellan 0 och 9.

PairingResult (SID 04)

Detta meddelande sänds från fordonsenhetens gränssnitt till ITS-enheten för att meddela huruvida den PIN-kod som sänts var korrekt. Meddelandet ska innehålla ett booleskt (BOOLEAN) värde som är T (*True*) om PIN-koden var korrekt och F (*False*) i annat fall.

SendPUC (SID 05)

Detta meddelande sänds från ITS-enheten för att den ska strykas från svarta listan i fordonsenhetens gränssnitt. Meddelandet innehåller en kod på åtta heltal (INTEGER) mellan 0 och 9.

BanLiftingResult (SID 06)

Detta meddelande sänds från fordonsenhetens gränssnitt till ITS-enheten för att meddela huruvida den PUC som sänts var korrekt. Meddelandet innehåller ett booleskt (BOOLEAN) värde som är T (*True*) om PUC var korrekt och F (*False*) i annat fall.

RequestRejected (SID 07)

Detta meddelande sänds från fordonsenhetens gränssnitt som svar på alla meddelanden från en svartlistad ITS-enhet, med undantag för *SendPUC*. Meddelandet innehåller den återstående svartlistningstiden för ITS-enheten, med det tidsformat (*time sequence*) som definieras i bilaga 3.

RequestData (SID 08)

Detta meddelande om åtkomst till data sänds från ITS-enheten. En parameter för begäran om överföring (TRTP) på 1 byte anger vilken typ av data som krävs. Det finns flera typer av data:

— standardTachData (TRTP 01): Data som är tillgängliga i färdskrivaren och som inte klassificeras som personuppgifter.

— personalTachData (TRTP 02): Data som är tillgängliga i färdskrivaren och som klassificeras som personuppgifter.

— gnssData (TRTP 03): GNSS-data; dessa utgör alltid personuppgifter.

— standardEventData (TRTP 04): Data om registrerade händelser som inte klassificeras som personuppgifter.

— personalEventData (TRTP 05): Data om registrerade händelser som klassificeras som personuppgifter.

— standardFaultData (TRTP 06): Data om registrerade fel som inte klassificeras som personuppgifter.

— manufacturerData (TRTP 07): Data som gjorts tillgängliga av tillverkaren.

▼B

Se bilaga 3 till detta tillägg för mer information om innehållet i respektive datatyp.

Se tillägg 12 för mer information om format och innehåll avseende GNSS-data.

Se bilaga I B och bilaga I C för mer information om datakoder för händelser och fel.

ResquestAccepted (SID 09)

Detta meddelande sänds från fordonsenhetens gränssnitt om ett meddelande *RequestData* från ITS-enheten har accepterats. Meddelandet innehåller en parameter för överföringssvar (TREP) på 1 byte (som är samma som byte för TRTP i det tillhörande meddelandet *RequestData*) och samtliga data av den begärda typen.

DataUnavailable (SID 0A)

Detta meddelande sänds från fordonsenhetens gränssnitt om begärda data av någon anledning inte kan sändas till en ITS-enhet som finns på vita listan. Meddelandet innehåller en parameter för överföringssvar (TREP) på 1 byte (som är samma som byte för TRTP för begärda data) och en felkod på 1 byte som specificeras i tabell 3. Följande koder finns tillgängliga:

— Inga data tillgängliga (10): Fordonsenhetens gränssnitt kan av ospecificerade orsaker inte komma åt data i fordonsenheten.

— Personuppgifter delas inte (11): ITS-enheten försöker hämta personuppgifter som inte får delas.

NegativeAnswer (SID 0B)

Dessa meddelanden sänds från fordonsenhetens gränssnitt om en begäran inte kan slutföras av någon annan orsak än att data inte är tillgängliga. Dessa meddelanden är normalt en följd av en begäran med olämpligt format (längd, SID, ITSID, …), men är inte begränsade till just detta. TRTP i datafältet innehåller SID för begäran. Datafältet innehåller en kod som anger orsaken till det negativa svaret. Följande koder finns tillgängliga:

— Allmänt avvisande (kod: 10)

— Operation kan inte utföras av en orsak som varken förtecknas nedan eller i avsnittet om meddelandet *DataUnavailable*.

— Tjänsten stöds ej (kod: 11)

— SID i begäran kan inte tolkas.

— Underfunktion stöds ej (kod: 12)

— TRTP i begäran kan inte tolkas. Den kan exempelvis saknas eller ligga utanför de accepterade värdena.

— Fel meddelandelängd (kod: 13)

— Det mottagna meddelandets längd är felaktig (byte för LEN stämmer inte med meddelandets verkliga längd).

— Fel omständigheter eller sekvensfel för begäran (kod: 22)

— Den begärda tjänsten är inte aktiv eller sekvensen av meddelanden om begäran är felaktig.

— Begäran utanför tillåtet intervall (kod: 33)

▼B

— Posten med parameter för begäran (datafält) är inte giltig.

— Svar dröjer (kod: 78)

— Begärd åtgärd kan inte fullgöras i tid och fordonsenheten är inte beredd att godta en annan begäran.

— *ITSID* stämmer inte (kod: FB)

— *ITSID* för SRC stämmer inte med den tillhörande anordningen efter jämförelse med informationen från Bluetooth.

— *ITSID* saknas (kod: FC)

— *ITSID* för SRC tillhör inte någon anordning.

På raderna 1–72 (**FormatMessageModule**) i ASN.1-koden i bilaga 3 specificeras formatet för meddelandena enligt beskrivning i tabell 3. Mer information om samtycke till meddelandenas innehåll finns nedan.

4.5. **Förarens samtycke**

Alla tillgängliga data klassificeras som ”standard” (dvs. ej personuppgifter, *non-personal*) eller som ”personuppgifter” (*personal*). Personuppgifter får endast vara åtkomliga om föraren ger sitt samtycke och accepterar att hans/hennes personuppgifter som finns i färdskrivaren får lämna fordonets datanät och överföras till tredjepartstillämpningar.

Förarens samtycke ges när ett visst förarkort (*driver card*) eller verkstadskort som är okänt för fordonsenheten (*vehicle unit*) sätts in för första gången och kortinnehavaren uppmanas att ge sitt samtycke till att personuppgifter som finns i färdskrivaren tillhandahålls via det frivilliga ITS-gränssnittet. (Se även avsnitt 3.6.2 i bilaga I C.)

Status för samtycke (aktivt eller ej aktivt) registreras i färdskrivarens minne.

I händelse av flera förare får endast personuppgifter om de förare som givit sitt samtycke delas med ITS-gränssnittet. Om exempelvis två förare finns i fordonet och bara den första föraren accepterat att dela sina personuppgifter får personuppgifterna för den andra föraren inte delas.

4.6. **Hämtning av standarddata**

I figur 3 i bilaga 2 visas sekvensdiagram för en giltig begäran om åtkomst till standarddata som sänds från ITS-enheten. ITS-enheten finns på vita listan och begär inte några personuppgifter, och därför krävs ingen ytterligare verifiering. Diagrammen utgår från att rätt procedur, såsom visas i figur 2 i bilaga 2, redan har följts. De kan ses som en motsvarighet till den grå rutan *REQUEST TREATMENT* i figur 2.

Bland tillgängliga data ska följande anses som standarddata:

— standardTachData (TRTP 01)

— StandardEventData (TRTP 04)

— standardFaultData (TRTP 06)

4.7. **Hämtning av personuppgifter**

I figur 4 i bilaga 2 visas ett sekvensdiagram för behandling av en begäran om personuppgifter. Som redan nämnts får fordonsenhetens gränssnitt endast sända personuppgifter om föraren har gett sitt uttryckliga samtycke (se även avsnitt 4.5). I andra ska begäran avvisas automatiskt.

▼B

Bland tillgängliga data ska följande anses som personuppgifter:

— personalTachData (TRTP 02)

— gnssData (TRTP 03)

— personalEventData (TRTP 05)

— manufacturerData (TRTP 07)

4.8. **Hämtning av data om händelser och fel**

ITS-enheter ska kunna begära händelsedata enligt förteckningen med samtliga oväntade händelser. Dessa data anses vara standarddata eller personuppgifter – se bilaga 3. Innehållet avseende respektive händelse stämmer med den dokumentation som tillhandahålls i bilaga 1 till detta tillägg.

▼B

BILAGA 1

FÖRTECKNING ÖVER TILLGÄNGLIGA DATA GENOM ITS-GRÄNSSNITTET

Data	Källa	►C2 Dataklassificering (personuppgift/ej personuppgift) ◄
VehicleIdentificationNumber	Fordonsenhet	**Ej personuppgift**
CalibrationDate	Fordonsenhet	**Ej personuppgift**
TachographVehicleSpeed speed instant t	Fordonsenhet	Personuppgift
Driver1WorkingState Selector driver	Fordonsenhet	Personuppgift
Driver2WorkingState	Fordonsenhet	Personuppgift
DriveRecognize Speed Threshold detected	Fordonsenhet	**Ej personuppgift**
Driver1TimeRelatedStates Weekly day time	Förarkort	Personuppgift
Driver2TimeRelatedStates	Förarkort	Personuppgift
DriverCardDriver1	Fordonsenhet	**Ej personuppgift**
DriverCardDriver2	Fordonsenhet	**Ej personuppgift**
OverSpeed	Fordonsenhet	Personuppgift
TimeDate	Fordonsenhet	**Ej personuppgift**
HighResolutionTotalVehicleDistance	Fordonsenhet	**Ej personuppgift**
ServiceComponentIdentification	Fordonsenhet	**Ej personuppgift**
ServiceDelayCalendarTimeBased	Fordonsenhet	**Ej personuppgift**
Driver1Identification	Förarkort	Personuppgift
Driver2Identification	Förarkort	Personuppgift
NextCalibrationDate	Fordonsenhet	**Ej personuppgift**
Driver1ContinuousDrivingTime	Förarkort	Personuppgift
Driver2ContinuousDrivingTime	Förarkort	Personuppgift
Driver1CumulativeBreakTime	Förarkort	Personuppgift
Driver2CumulativeBreakTime	Förarkort	Personuppgift
Driver1CurrentDurationOfSelectedActivity	Förarkort	Personuppgift
Driver2CurrentDurationOfSelectedActivity	Förarkort	Personuppgift
SpeedAuthorised	Fordonsenhet	**Ej personuppgift**
TachographCardSlot1	Förarkort	**Ej personuppgift**
TachographCardSlot2	Förarkort	**Ej personuppgift**
Driver1Name	Förarkort	Personuppgift
Driver2Name	Förarkort	Personuppgift

▼B

Data	Källa	►C2 Dataklassificering (personuppgift/ej personuppgift) ◄
OutOfScopeCondition	Fordonsenhet	**Ej personuppgift**
ModeOfOperation	Fordonsenhet	**Ej personuppgift**
Driver1CumulatedDrivingTimePreviousAndCurrentWeek	Förarkort	Personuppgift
Driver2CumulatedDrivingTimePreviousAndCurrentWeek	Förarkort	Personuppgift
EngineSpeed	Fordonsenhet	Personuppgift
RegisteringMemberState	Fordonsenhet	**Ej personuppgift**
VehicleRegistrationNumber	Fordonsenhet	**Ej personuppgift**
Driver1EndOfLastDailyRestPeriod	Förarkort	Personuppgift
Driver2EndOfLastDailyRestPeriod	Förarkort	Personuppgift
Driver1EndOfLastWeeklyRestPeriod	Förarkort	Personuppgift
Driver2EndOfLastWeeklyRestPeriod	Förarkort	Personuppgift
Driver1EndOfSecondLastWeeklyRestPeriod	Förarkort	Personuppgift
Driver2EndOfSecondLastWeeklyRestPeriod	Förarkort	Personuppgift
Driver1CurrentDailyDrivingTime	Förarkort	Personuppgift
Driver2CurrentDailyDrivingTime	Förarkort	Personuppgift
Driver1CurrentWeeklyDrivingTime	Förarkort	Personuppgift
Driver2CurrentWeeklyDrivingTime	Förarkort	Personuppgift
Driver1TimeLeftUntilNewDailyRestPeriod	Förarkort	Personuppgift
Driver2TimeLeftUntilNewDailyRestPeriod	Förarkort	Personuppgift
Driver1CardExpiryDate	Förarkort	Personuppgift
Driver2CardExpiryDate	Förarkort	Personuppgift
Driver1CardNextMandatoryDownloadDate	Förarkort	Personuppgift
Driver2CardNextMandatoryDownloadDate	Förarkort	Personuppgift
TachographNextMandatoryDownloadDate	Fordonsenhet	**Ej personuppgift**
Driver1TimeLeftUntilNewWeeklyRestPeriod	Förarkort	Personuppgift
Driver2TimeLeftUntilNewWeeklyRestPeriod	Förarkort	Personuppgift
Driver1NumberOfTimes9hDailyDrivingTimesExceeded	Förarkort	Personuppgift
Driver2NumberOfTimes9hDailyDrivingTimesExceeced	Förarkort	Personuppgift

▼B

Data	Källa	►C2 Dataklassificering (personuppgift/ej personuppgift) ◄
Driver1CumulativeUninterruptedRestTime	Förarkort	Personuppgift
Driver2CumulativeUninterruptedRestTime	Förarkort	Personuppgift
Driver1MinimumDailyRest	Förarkort	Personuppgift
Driver2MinimumDailyRest	Förarkort	Personuppgift
Driver1MinimumWeeklyRest	Förarkort	Personuppgift
Driver2MinimumWeeklyRest	Förarkort	Personuppgift
Driver1MaximumDailyPeriod	Förarkort	Personuppgift
Driver2MaximumDailyPeriod	Förarkort	Personuppgift
Driver1MaximumDailyDrivingTime	Förarkort	Personuppgift
Driver2MaximumDailyDrivingTime	Förarkort	Personuppgift
Driver1NumberOfUsedReducedDailyRestPeriods	Förarkort	Personuppgift
Driver2NumberOfUsedReducedDailyRestPeriods	Förarkort	Personuppgift
Driver1RemainingCurrentDrivingTime	Förarkort	Personuppgift
Driver2RemainingCurrentDrivingTime	Förarkort	Personuppgift
GNSS position	Fordonsenhet	Personuppgift

2) KONTINUERLIGA GNSS-DATA, TILLGÄNGLIGA EFTER FÖRARENS SAMTYCKE

Se tillägg 12 om GNSS.

3) DATA OM HÄNDELSER, TILLGÄNGLIGA UTAN FÖRARENS SAMTYCKE

Händelse	Lagringsregler	Data som ska registreras per händelse
Insättning av ett ogiltigt kort	— De senaste tio händelserna	— Datum och tidpunkt för händelsen — Korttyp, kortnummer, utfärdande medlemsstat och generation för det kort som orsakat händelsen — Antal liknande händelser samma dag
Kortkonflikt	— De senaste tio händelserna	— Datum och tidpunkt för händelsens början — Datum och tidpunkt för händelsens slut — Korttyp, kortnummer, utfärdande medlemsstat och generation för de två kort som orsakat konflikten
Senaste kortsessionen ej korrekt avslutad	— De senaste tio händelserna	— Datum och tidpunkt för insättning av kort — Korttyp, kortnummer, utfärdande medlemsstat och generation — Data om senaste session enligt avläsning från kortet — Datum och tidpunkt för insättning av kort — Fordonets registreringsnummer (VRN), registrerande medlemsstat och fordonsenhetens generation

▼B

Händelse	Lagringsregler	Data som ska registreras per händelse
Avbrott i strömtillförseln.(2)	— Den långvarigaste händelsen för vart och ett av de senaste tio dygn där händelsen inträffat — De fem långvarigaste händelserna under de senaste 365 dygnen	— 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
Fel i kommunikation med kommunikationsanordning för fjärravläsning	— Den långvarigaste händelsen för vart och ett av de senaste tio dygn där händelsen inträffat — De fem långvarigaste händelserna under de senaste 365 dygnen	— 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
Positionsinformation från GNSS-mottagare saknas	— Den långvarigaste händelsen för vart och ett av de senaste tio dygn där händelsen inträffat — De fem långvarigaste händelserna under de senaste 365 dygnen	— 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
Fel i rörelsedata	— Den långvarigaste händelsen för vart och ett av de senaste tio dygn där händelsen inträffat — De fem långvarigaste händelserna under de senaste 365 dygnen	— 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
Konflikt i fordonets rörelsedata	— Den långvarigaste händelsen för vart och ett av de senaste tio dygn där händelsen inträffat — De fem långvarigaste händelserna under de senaste 365 dygnen	— 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
Försök till säkerhetsöverträdelse	De tio senaste händelserna per händelsetyp	— Datum och tidpunkt för händelsens början — Datum och tidpunkt för händelsens slut (om det är relevant) — Korttyp, kortnummer, utfärdande medlemsstat och generation för ett eventuellt kort som var insatt vid händelsens början och/eller slut — Händelsetyp

▼B

Händelse	Lagringsregler	Data som ska registreras per händelse
Tidskonflikt	— Den långvarigaste händelsen för vart och ett av de senaste tio dygn där händelsen inträffat — De fem långvarigaste händelserna under de senaste 365 dygnen	— Datum och tidpunkt enligt färdskrivaren — Aktuellt UTC-datum och aktuell UTC-tid — Korttyp, kortnummer, utfärdande medlemsstat och generation för ett eventuellt kort som var insatt vid händelsens början och/eller slut — Antal liknande händelser samma dag

4) DATA OM HÄNDELSER, TILLGÄNGLIGA MED FÖRARENS SAMTYCKE

Händelse	Lagringsregler	Data som ska registreras per händelse
Körning utan korrekt kort	— Den långvarigaste händelsen för vart och ett av de senaste tio dygn där händelsen inträffat — De fem långvarigaste händelserna under de senaste 365 dygnen	— 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
Insättning av kort under körning	— Den senaste händelsen för vart och ett av de senaste tio dygn där händelsen inträffat	— Datum och tidpunkt för händelsen — Korttyp, kortnummer, utfärdande medlemsstat och generation — Antal liknande händelser samma dag
Hastighetsöverträdelse (1)	— Den mest allvarliga händelsen för vart och ett av de senaste tio dygn där händelsen inträffat (dvs. den med högsta medelhastighet) — De fem mest allvarliga händelserna under de senaste 365 dygnen — Den första händelsen som inträffat efter den senaste kalibreringen	— Datum och tidpunkt för händelsens början — Datum och tidpunkt för händelsens slut — Högsta hastighet som uppmätts under händelsen — Aritmetisk medelhastighet som uppmätts under händelsen — Korttyp, kortnummer, utfärdande medlemsstat och generation för förarkortet (i förekommande fall) — Antal liknande händelser samma dag

5) DATA OM FEL, TILLGÄNGLIGA UTAN FÖRARENS SAMTYCKE

Fel	Lagringsregler	Data som ska registreras per fel
Kortfel	— De tio senaste förarkortsfelen	— Datum och tidpunkt för felets början — Datum och tidpunkt för felets slut — Korttyp, kortnummer, utfärdande medlemsstat och generation
Färdskrivarfel	— De tio senaste felen för varje typ av fel — Det första felet efter den senaste kalibreringen	— Datum och tidpunkt för felets början — Datum och tidpunkt för felets slut — Typ av fel — Korttyp, kortnummer, utfärdande medlemsstat och generation för ett eventuellt kort som var insatt vid felets början och/eller slut

▼B

Detta fel ska utlösas vid något av följande fel om kalibreringsläget inte är inställt:

— Internt fel i fordonsenheten.

— Skrivarfel.

— Bildskärmsfel.

— Överföringsfel.

— Sensorfel.

— Fel i GNSS-mottagare eller extern GNSS-anordning.

— Fel i kommunikationsanordning för fjärravläsning.

6) TILLVERKARSPECIFIKA HÄNDELSER OCH FEL, UTAN FÖRARENS SAMTYCKE

Händelse eller fel	Lagringsregler	Data som ska registreras per händelse
Definieras av tillverkaren	Definieras av tillverkaren	Definieras av tillverkaren

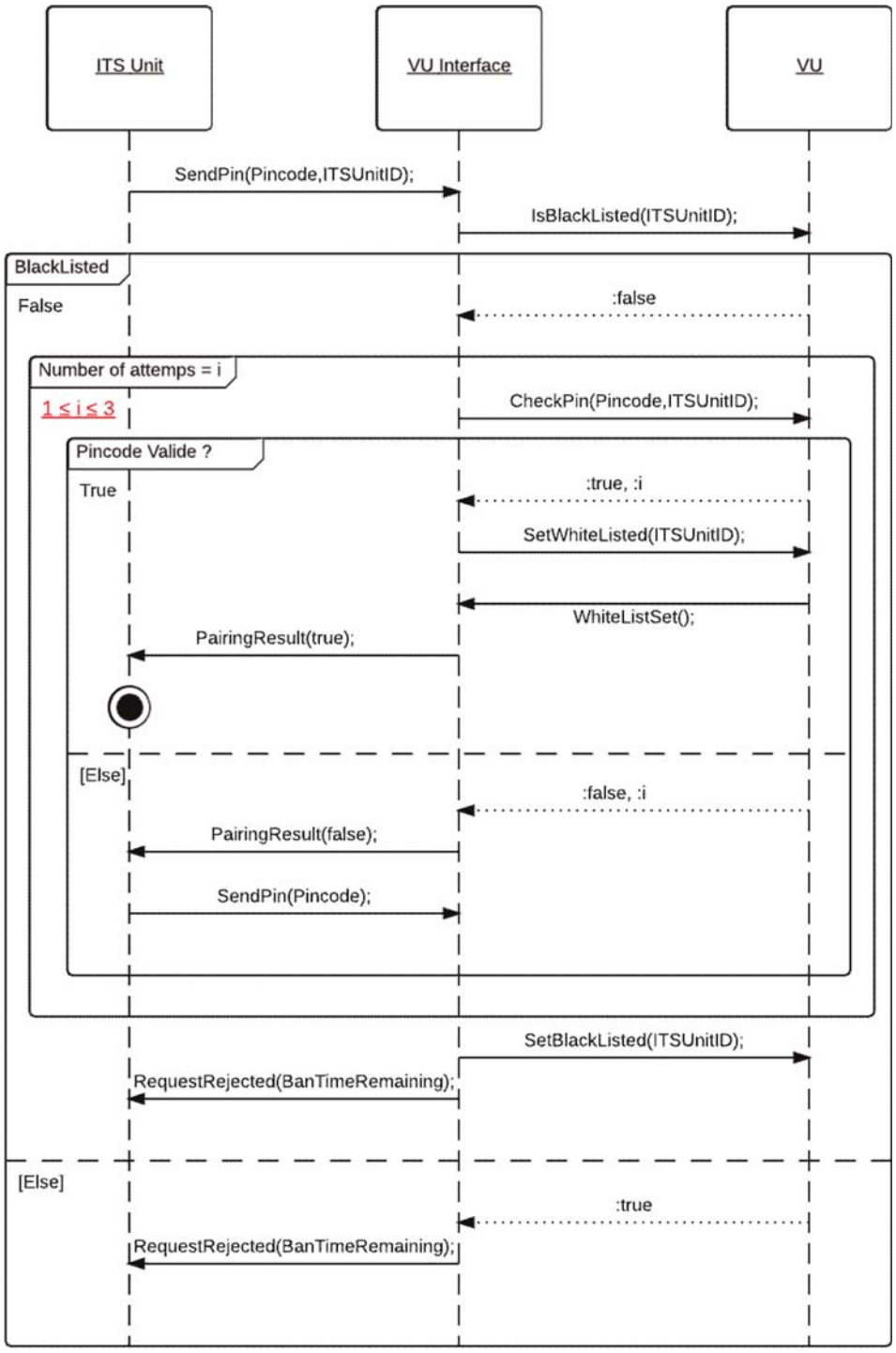
▼B

BILAGA 2

SEKVENSDIAGRAM FÖR MEDDELANDEUTBYTEN MED ITS-ENHETEN

Figur 1

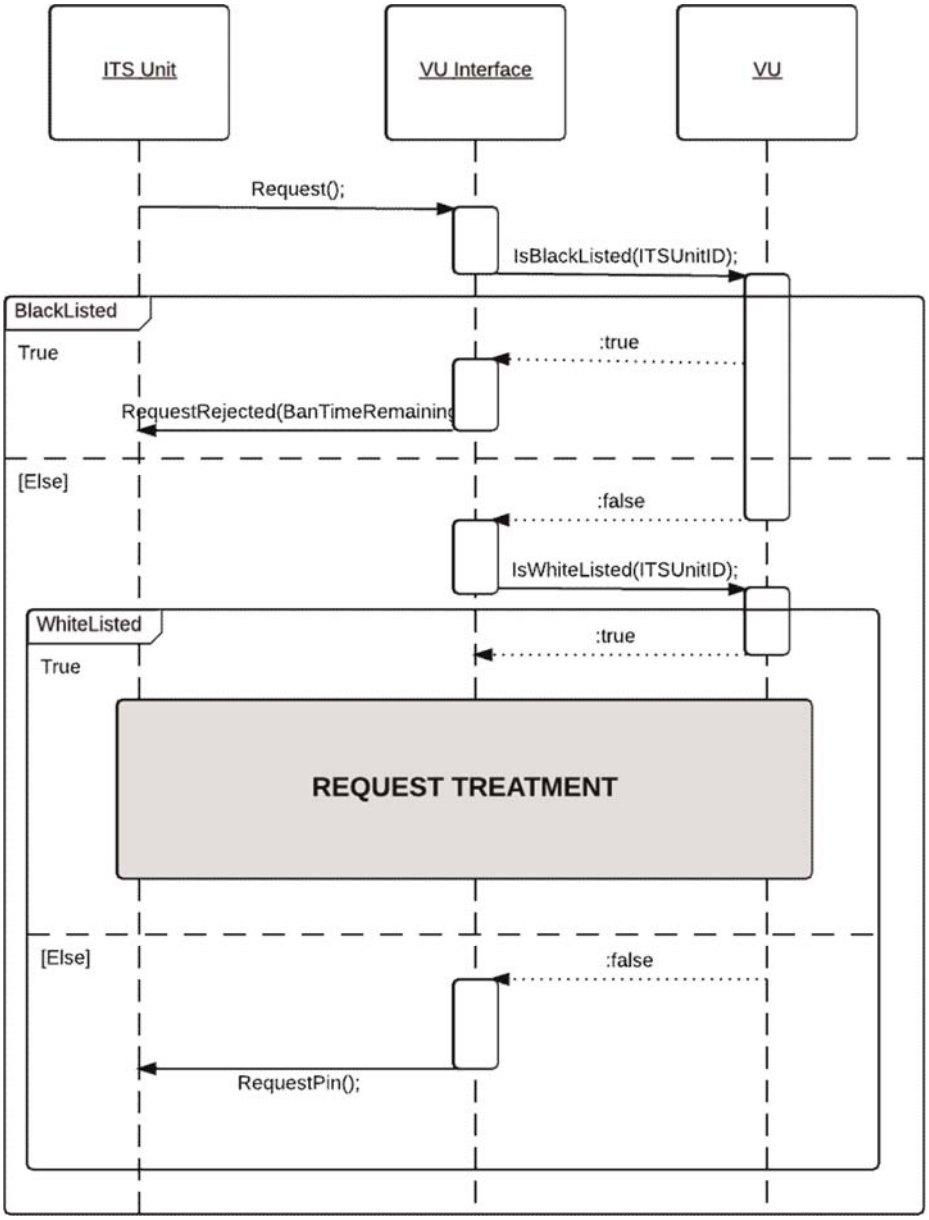
Sekvensdiagram för försök till PIN-validering



▼B

Figur 2

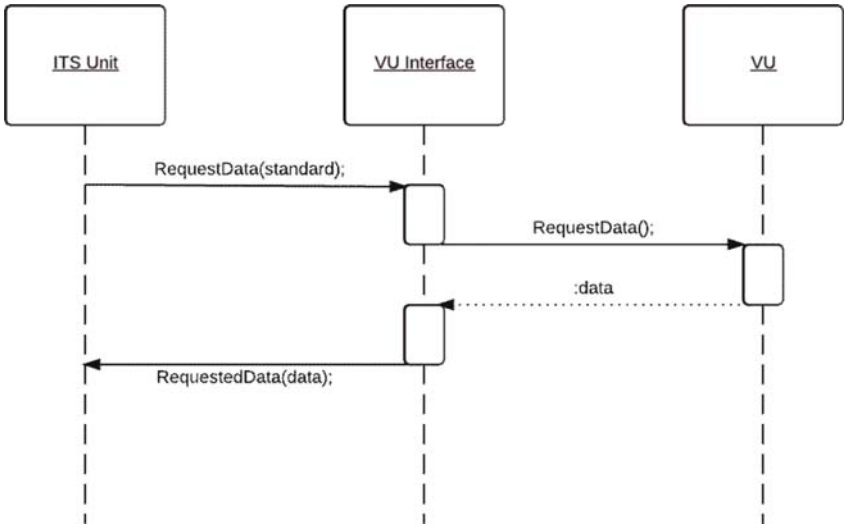
Sekvensdiagram för verifiering av ITS-enhetens auktorisation



▼B

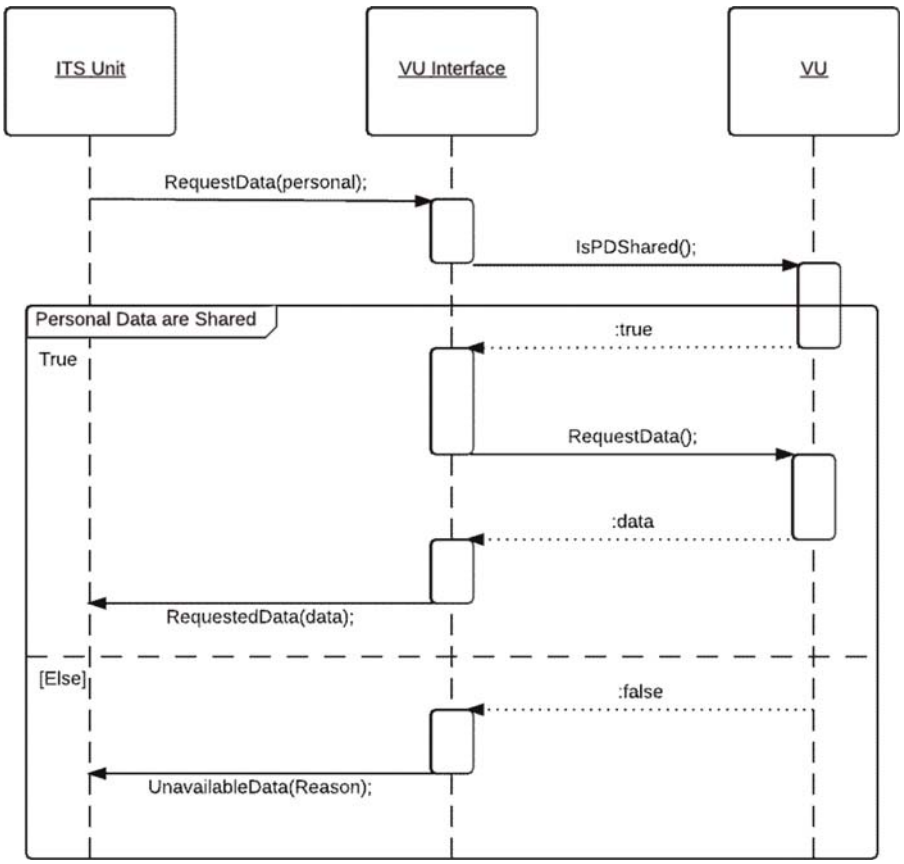
Figur 3

Sekvensdiagram för behandling av en begäran om data som inte klassificeras som personuppgifter (efter åtkomst genom rätt PIN-kod)



Figur 4

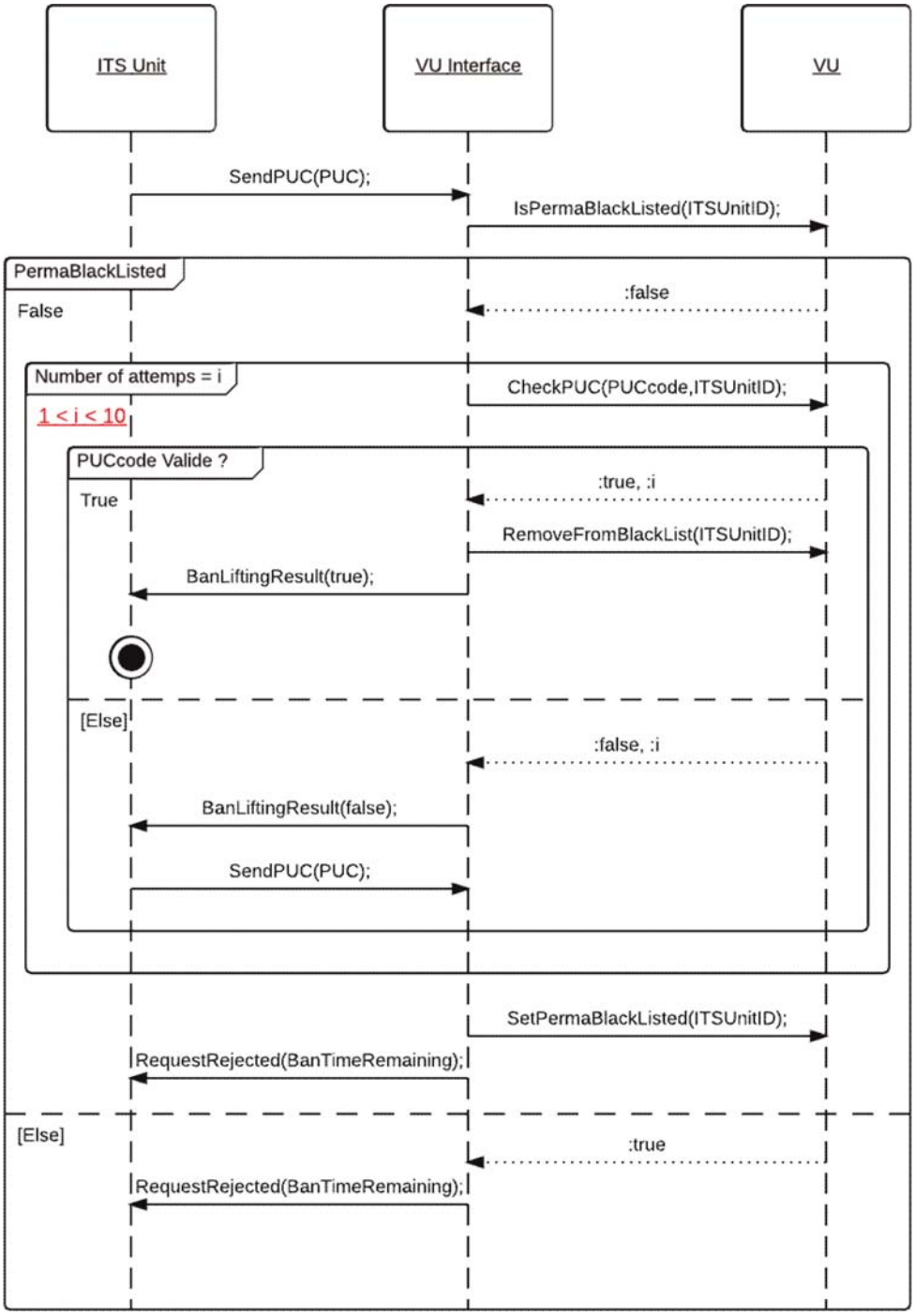
Sekvensdiagram för behandling av en begäran om data som klassificeras som personuppgifter (efter åtkomst genom rätt PIN-kod)



▼B

Figur 5

Sekvensdiagram för försök till PUC-validering



▼B

BILAGA 3

ASN.1-SPECIFIKATIONER

```
FormatMessageModule DEFINITIONS AUTOMATIC TAGS ::= BEGIN
EXPORTS ;
IMPORTS SendPIN, SendPUC, PairingResult, RequestPIN, RequestRejected,
        BanLiftingResult FROM PINPUCDataFieldsModule
        RequestAccepted,RequestData, DataUnavailable FROM
        RequestDataFieldsModule
        SendITSID, NegativeAnswer FROM OtherDataFieldsModule;

      CompleteMessage ::=SEQUENCE{
            header Header,
            data DataField,
            checksum Checksum
      }

      ----------------
      --HEADER TYPES--
      ----------------


      Header::=SEQUENCE{
            tgt IDList,
            src IDList,
            len BIT STRING (1..255)
      }

      vuID BIT STRING ::= 'EE'H
      IDList ::=CHOICE{
            vu BIT STRING (vuID),
            itsUnits SEQUENCE OF BIT STRING,
                  --Default hex Value:A0, redefined after first message exchange--
                  --Each ID will be linked to the Bluetooth ID of the device--
            ...
      }

      --------------------
      --DATAFIELDS TYPES--
      --------------------
      DataField ::=SEQUENCE{
            sid BIT STRING,
            trtp BIT STRING,
            subMBytes SubMessageBytes,
            dataField Content,
            ...
      }

      SubMessageBytes ::= SEQUENCE{
            currentSubM BIT STRING,
            totalSubM BIT STRING
      }

      Content ::= CHOICE{
            requestPIN RequestPIN,
            sendITSID SendITSID,
            sendPin SendPIN,
```

▼B

```
55                pairRslt PairingResult,
56                sendPUC SendPUC,
57                banlift BanLiftingResult,
58                requestRejected RequestRejected,
59                requestData RequestData,
60                requestOK RequestAccepted,
61                dataUnavailable DataUnavailable,
62                negAns NegativeAnswer
63          }
64
65          ------------------
66          --CHECKSUM TYPES--
67          ------------------
68
69          Checksum ::= SEQUENCE{
70                --SHA2 checksum
71          }
72    END
73
```

▼B

```
PINPUCDataFieldsModule DEFINITIONS AUTOMATIC TAGS ::= BEGIN
EXPORTS SendPIN, SendPUC, PairingResult, RequestPIN, RequestRejected,
BanLiftingResult;
IMPORTS ;

      ----------
      ---Utils--
      ----------

      PUC ::= SEQUENCE (SIZE(8)) OF
      INTEGER (SIZE(0..9))

      PIN ::=      SEQUENCE (SIZE(4)) OF
            INTEGER (SIZE(0..9))

      -------------------------
      --Messages From ITS Unit--
      -------------------------

      SendPIN {PIN:pin} ::= SEQUENCE {
            sid BIT STRING ('03'H),
            pin PIN (pin)
      }

      SendPUC {PUC:puc} ::= SEQUENCE {
            sid BIT STRING ('05'H),
            puc PUC (puc)
      }
      --------------------
      --Messages From VU--
      --------------------

      PairingResult ::= SEQUENCE{
            sid BIT STRING ('04'H),
            result BOOLEAN
      }

      RequestPIN {MType:receivedRequest}::= SEQUENCE{
            sid BIT STRING ('01'H)
      }

      RequestRejected ::= SEQUENCE{
            sid BIT STRING ('07'H),
            banTimeRemaining GeneralizedTime, --PermaBan == 1k years-- }

      BanLiftingResult ::= SEQUENCE{
            sid BIT STRING ('06'H),
            result BOOLEAN
      }
END
```

▼B

```
RequestDataFields DEFINITIONS AUTOMATIC TAGS ::= BEGIN
	EXPORTS RequestAccepted,RequestData, DataUnavailable ;
	IMPORTS StandardEvent, PersonalEvent, StandardFault FROM EventsModule;

	------------------
	---From ITS Unit--
	------------------
	RequestData ::= SEQUENCE{
		sid BIT STRING ('08'H),
		requestedData DataTypeCode,
		...
	}

	-----------
	--From VU--
	-----------
	RequestAccepted ::=SEQUENCE{
		sid BIT STRING ('09'H),
		trtp DataTypeCode,
		dataSheet CHOICE{
			standardData StandardTachDataContent,
			personalData PersonalTachDataContent,
			gnss GNSSDataContent,
			standardEvent StandardEventContent,
			personalEvent PersonalEventContent,
			standardFault StandardFaultContent,
			manufacturerdata ManufacturerDataContent,
			...
		}
	}

	DataTypeCode ::=CHOICE{
		standardTachData BIT STRING ('01'H),
		personalTachData BIT STRING ('02'H),
		gnssData BIT STRING ('03'H),
		standardEventData BIT STRING ('04'H),
		personalEventData BIT STRING ('05'H),
		standardFaultData BIT STRING ('06'H),
		manufacturerData BIT STRING ('07'H),
		...
	}

	DataUnavailable ::=SEQUENCE{
		sid BIT STRING ('0A'H),
		trtp DataTypeCode,
		reason UnavailableDataCodes
	}

	UnavailableDataCodes ::= CHOICE{
		noDataAvailable BIT STRING ('10'H),
		personalDataNotShared BIT STRING ('11'H),
		...
	}
	---------------------------
	--Complete Tachograph Data--
	---------------------------
	--The format of the data was taken from the ISO16844-7 norm, more information
available in this ISO document—

```

▼B

```
Time ::= SEQUENCE{
       seconds INTEGER (0..59.75), --increment: 0.25s--
       minutes INTEGER (0..59), --increment: 1min--
       hours INTEGER (0..23), --increment: 1h--
       day INTEGER (0.25.. 31.75), --increment: 0.25d--
       month INTEGER (1..12), --increment: 1month--
       year INTEGER (1985..2235), --increment: 1year--
       locMinOffset INTEGER (-59..59), --increment: 1min--
       locHouroffset INTEGER (-23..23)--increment: 1h--
}

Date ::= SEQUENCE{
       month INTEGER (1..12), --increment: 1month--
       day INTEGER (0.25.. 31.75), --increment: 0.25d--
       year INTEGER (1985..2235) --increment: 1year--
}

DriverName ::=SEQUENCE{
       codePageSurname UTF8String, --See ISO/IEC 8859--
       surname UTF8String,
       codePageFirstname UTF8String, --See ISO/IEC 8859--
       firstname UTF8String,
}

-------------------
--Message Content--
-------------------

StandardTachDataContent ::= SEQUENCE{
       trtp DataTypeCode (DataTypeCode.&standardTachData),
       personal BOOLEAN (FALSE),
       data StandardTachyDataSheet,
}

PersonalTachDataContent ::= SEQUENCE{
       trtp DataTypeCode (DataTypeCode.&personalTachData),
       personal BOOLEAN (TRUE),
       data PersonalTachyDataSheet
}

GNSSDataContent ::= SEQUENCE{
       trtp DataTypeCode (DataTypeCode.&gnssData),
       personal BOOLEAN (TRUE),
       data GNSSDataSheet
}

StandardEventContent ::= SEQUENCE{
       trtp DataTypeCode (DataTypeCode.&standardEventData),
       personal BOOLEAN (FALSE),
       data StandardEventDataSheet
}

PersonalEventContent ::= SEQUENCE{
       trtp DataTypeCode (DataTypeCode.&personalEventData),
       personal BOOLEAN (TRUE),
       data PersonalEventDataSheet
}

StandardFaultContent ::= SEQUENCE{
```

▼B

```
243                trtp DataTypeCode (DataTypeCode.&standardFaultData),
244                personal BOOLEAN (FALSE),
245                data StandardFault
246          }
247
248          ManufacturerDataContent ::= SEQUENCE{
249                trtp DataTypeCode (DataTypeCode.&manufacturerData),
250                personal BOOLEAN (TRUE),
251                ...
252          }
253
254          ---------------
255          --DATA SHEETS--
256          ---------------
257
258          --Data sheet format follows ISO 16844-7.--
259          StandardTachyDataSheet ::= SEQUENCE{
260                vin UTF8String (SIZE(17)),
261                calibrationDate Date,
262                driveRecognize INTEGER (2 UNION 12),
263                driverCardDriver1 INTEGER (2 UNION 12),
264                driverCardDriver2 INTEGER (2 UNION 12),
265                timeDate Time,
266                highResolutionTotalVehicleDistance INTEGER (0..21055406), --increment:
267    5m--
268                serviceComponentIdentification INTEGER (0..255),
269                serviceDelayCalendarTimeBased INTEGER (-125..125), --increment: 1week-
270    -
271                nextCalibrationDate Date,
272                speedAuthorised INTEGER (0..250.996), --increment 1/256km/h--
273                tachographCardSlot1 INTEGER (0..4...), --Maximum 250--
274                tachographCardSlot2 INTEGER (0..4...), --Maximum 250--
275                outOfScopeCondition INTEGER(2 UNION 12),
276                modeOfOperation INTEGER (0..4...), --Maximum 250--
277                registeringMemberState UTF8String,
278          vehicleRegistrationNumber SEQUENCE {
279                      codePageVRN INTEGER (0..255),
280                      vrn OCTET STRING (SIZE(13)),
281                },
282                tachographNextMandatoryDownloadDate Date,
283                ...
284          }
285
286          PersonalTachyDataSheet ::= SEQUENCE{
287                tachographVehicleSpeed INTEGER (0..250.996), --increment 1/256km/h--
288                driver1WorkingState INTEGER (2 UNION 12 UNION 102 UNION 112 UNION 1002
289    UNION 1012...),
290                driver2WorkingState INTEGER (2 UNION 12 UNION 102 UNION 112 UNION 1002
291    UNION 1012...),
292
293                driver1TimeRelatedStates INTEGER(2 UNION 12 UNION 102 UNION 112 UNION
294    1002 UNION
295                                                 1012 UNION 1102 UNION 1112 UNION
296    10002 UNION 10012 UNION
297                                                 10102 UNION 10112 UNION 11002 UNION
298    11012...),
299                driver2TimeRelatedStates INTEGER(2 UNION 12 UNION 102 UNION 112 UNION
300    1002 UNION
```

▼B

```
                                                    1012 UNION 1102 UNION 1112 UNION
10002 UNION 10012 UNION
                                                    10102 UNION 10112 UNION 11002 UNION
11012...),

                overSpeed INTEGER (2 UNION 12),
                driver1Identification INTEGER (SIZE(19)), --TODO NEED FURTHER SPECS
FROM TACHO REGULATION--
                driver2Identification INTEGER (SIZE(19)), --TODO NEED FURTHER SPECS
FROM TACHO REGULATION--
                driver1ContinuousDrivingTime INTEGER (0.. 64255), --increment: 1min--
                driver2ContinuousDrivingTime INTEGER (0.. 64255), --increment: 1min--
                driver1CurrentDurationOfSelectedActivity INTEGER (0.. 64255), --
increment: 1min--
                driver2CurrentDurationOfSelectedActivity INTEGER (0.. 64255), --
increment: 1min--
                driver1Name DriverName,
                driver2Name DriverName,
                driver1CumulatedDrivingTimePreviousAndCurrentWeek INTEGER (0.. 64255),
--increment: 1min--
                driver2CumulatedDrivingTimePreviousAndCurrentWeek INTEGER (0.. 64255),
--increment: 1min--
                engineSpeed INTEGER(0..8031.875), --increment: 0,125r/min--
                driver1EndOfLastDailyRestPeriod Time,
                driver2EndOfLastDailyRestPeriod Time,
                driver1EndOfLastWeeklyRestPeriod Time,
                driver2EndOfLastWeeklyRestPeriod Time,
                driver1EndOfSecondLastWeeklyRestPeriod Time,
                driver2EndOfSecondLastWeeklyRestPeriod Time,
                driver1CurrentDailyDrivingTime INTEGER (0.. 64255), --increment: 1min-
-
                driver2CurrentDailyDrivingTime INTEGER (0.. 64255), --increment: 1min-
-
                driver1CurrentWeeklyDrivingTime INTEGER (0.. 64255), --increment:
1min--
                driver2CurrentWeeklyDrivingTime INTEGER (0.. 64255), --increment:
1min--
                driver1TimeLeftUntilNewDailyRestPeriod INTEGER (0.. 64255), --
increment: 1min--
                driver2TimeLeftUntilNewDailyRestPeriod INTEGER (0.. 64255), --
increment: 1min--
                driver1CardExpiryDate Date,
                driver2CardExpiryDate Date,
                driver1CardNextMandatoryDownloadDate Date,
                driver2CardNextMandatoryDownloadDate Date,
                driver1TimeLeftUntilNewWeeklyRestPeriod INTEGER (0.. 64255), --
increment: 1min--
                driver2TimeLeftUntilNewWeeklyRestPeriod INTEGER (0.. 64255), --
increment: 1min--
                driver1NumberOfTimes9hDailyDrivingTimesExceeded INTEGER (0..13),
                driver2NumberOfTimes9hDailyDrivingTimesExceeced INTEGER (0..13),
                driver1CumulativeUninterruptedRestTime INTEGER (0.. 64255), --
increment: 1min--
                driver2CumulativeUninterruptedRestTime INTEGER (0.. 64255), --
increment: 1min--
                driver1MinimumDailyRest INTEGER (0.. 64255), --increment: 1min--
                driver2MinimumDailyRest INTEGER (0.. 64255), --increment: 1min--
                driver1MinimumWeeklyRest INTEGER (0.. 64255), --increment: 1min--
                driver2MinimumWeeklyRest INTEGER (0.. 64255), --increment: 1min--
```

▼B

```
360                driver1MaximumDailyPeriod INTEGER (0..250), --increment: 1h--
361                driver2MaximumDailyPeriod INTEGER (0..250), --increment: 1h--
362                driver1MaximumDailyDrivingTime INTEGER (910 UNION 1010),
363                driver2MaximumDailyDrivingTime INTEGER (910 UNION 1010),
364                driver1NumberOfUsedReducedDailyRestPeriods INTEGER (0..13),
365                driver2NumberOfUsedReducedDailyRestPeriods INTEGER (0..13),
366                driver1RemainingCurrentDrivingTime INTEGER (0.. 64255), --increment:
367    1min--
368                driver2RemainingCurrentDrivingTime INTEGER (0.. 64255), --increment:
369    1min--
370                ...
371          }
372
373          GNSSDataSheet ::=  SEQUENCE {
374          gnssPosition GeoCoordinates
375                --See Appendix 1 for definition of GeoCoordinates--
376          }
377
378          StandardEventDataSheet ::= SEQUENCE{
379                events SEQUENCE OF StandardEvent
380          }
381
382          PersonalEventDataSheet ::= SEQUENCE{
383                events SEQUENCE OF PersonalEvent
384          }
385    END
386
387    EventsModule DEFINITIONS AUTOMATIC TAGS ::= BEGIN
388          EXPORTS ALL;
389          IMPORTS NationAlpha FROM Appendix1; --See Appendix 1 for more information
390    about NationAlpha--
391
392                SecurityBreachEvent ::=SEQUENCE{
393                      --See Annex 1B for more information--
394                }
395
396                RecordingEquipmentFaultType ::= SEQUENCE{
397                      --See Annex 1B for more information--
398                }
399
400                StandardEvent::= CHOICE{
401                      insertionInvalidCard InsertionOfANonValidCard,
402                      cardConflict CardConflict,
403                      timeOverlap TimeOverlap,
404                      previousSessionNotClosed LastCardSessionNotCorrectlyClosed,
405                      overSpeeding OverSpeeding,
406                      powerSupplyInterruption PowerSupplyInterruption,
407                      comErrorWithRemoteFacility
408    CommunicationErrorWithTheRemoteCommunicationFacility,
409                      absenceGNSSPosition
410    AbsenceOfPositionInformationFromGNSSReceiver,
411                      positionDataError PositionDataError,
412                      motionDataError MotionDataError,
413                      vehicleMotionConflict VehicleMotionConflict,
414                      securityBreachAttempt SecurityBreachAttempt,
415                      timeConflict TimeConflict,
416                      ...
417                }
418
```

▼B

```
PersonalEvent ::= CHOICE{
      lackOfAppropriateCard DrivingWithoutAnAppropriateCard,
      cardInsertionWhileDriving CardInsertionWhileDriving,
      overSpeeding OverSpeeding,
      ...
}

StandardFault ::= CHOICE{
      cardFault CardFault,
      recordingEquipementFault RecordingEquipmentFault,
...
}

---------------
--EVENTS LIST--
---------------

InsertionOfANonValidCard::=SEQUENCE{
      beginDate GeneralizedTime,
      endDate GeneralizedTime,
      carsdType SEQUENCE OF UTF8String,
      cardsNumber SEQUENCE OF INTEGER,
      issuingMemberState SEQUENCE OF NationAlpha,
      cardsGeneration SEQUENCE OF INTEGER
}

CardConflict ::= SEQUENCE{
      beginDate GeneralizedTime,
      endDate GeneralizedTime,
      carsdType SEQUENCE OF UTF8String,
      cardsNumber SEQUENCE OF INTEGER,
      issuingMemberState SEQUENCE OF NationAlpha,
      cardsGeneration SEQUENCE OF INTEGER
}

TimeOverlap ::=SEQUENCE{
      beginDate GeneralizedTime,
      endDate GeneralizedTime,
      carsdType SEQUENCE OF UTF8String,
      cardsNumber SEQUENCE OF INTEGER,
      issuingMemberState SEQUENCE OF NationAlpha,
      cardsGeneration SEQUENCE OF INTEGER,
      numberSimilarEvent INTEGER
}

DrivingWithoutAnAppropriateCard ::= SEQUENCE{
      beginDate GeneralizedTime,
      endDate GeneralizedTime,
      carsdType SEQUENCE OF UTF8String,
      cardsNumber SEQUENCE OF INTEGER,
      issuingMemberState SEQUENCE OF NationAlpha,
      cardsGeneration SEQUENCE OF INTEGER,
      numberOfSimilarEvent INTEGER
}

CardInsertionWhileDriving ::= SEQUENCE{
      date GeneralizedTime,
      carsdType SEQUENCE OF UTF8String,
      cardsNumber SEQUENCE OF INTEGER,
```

▼B

```
                issuingMemberState SEQUENCE OF NationAlpha,
                numberOfSimilarEvents INTEGER
        }

        LastCardSessionNotCorrectlyClosed ::=SEQUENCE{
                beginDate GeneralizedTime,
                endDate GeneralizedTime,
                carsdType SEQUENCE OF UTF8String,
                cardsNumber SEQUENCE OF INTEGER,
                issuingMemberState SEQUENCE OF NationAlpha,
                cardsGeneration SEQUENCE OF INTEGER,
                oldSession SEQUENCE{
                        beginDate GeneralizedTime,
                        endDate GeneralizedTime,
                        vrn UTF8String,
                        issuingMemberState NationAlpha,
                        cardsGeneration INTEGER,
                }
        }

        OverSpeeding ::=SEQUENCE{
                beginDate GeneralizedTime,
                endDate GeneralizedTime,
                maximumSpeed INTEGER,
                averageSpeed INTEGER,
                cardType UTF8String,
                cardNumber INTEGER,
                issuingMemberState NationAlpha,
                cardGeneration INTEGER,
                numberOfSimilarEvents INTEGER
        }

        PowerSupplyInterruption ::=SEQUENCE{
                beginDate GeneralizedTime,
                endDate GeneralizedTime,
                carsdType SEQUENCE OF UTF8String,
                cardsNumber SEQUENCE OF INTEGER,
                issuingMemberState SEQUENCE OF NationAlpha,
                cardsGeneration SEQUENCE OF INTEGER,
                numberOfSimilarEvent INTEGER
        }

        CommunicationErrorWithTheRemoteCommunicationFacility ::=SEQUENCE{
                beginDate GeneralizedTime,
                endDate GeneralizedTime,
                carsdType SEQUENCE OF UTF8String,
                cardsNumber SEQUENCE OF INTEGER,
                issuingMemberState SEQUENCE OF NationAlpha,
                cardsGeneration SEQUENCE OF INTEGER,
                numberOfSimilarEvent INTEGER
        }

        AbsenceOfPositionInformationFromGNSSReceiver ::= SEQUENCE{
                beginDate GeneralizedTime,
                endDate GeneralizedTime,
                carsdType SEQUENCE OF UTF8String,
                cardsNumber SEQUENCE OF INTEGER,
                issuingMemberState SEQUENCE OF NationAlpha,
                cardsGeneration SEQUENCE OF INTEGER,
```

▼B

```
537                     numberOfSimilarEvent INTEGER
538             }
539
540             PositionDataError ::= SEQUENCE{
541                     beginDate GeneralizedTime,
542                     endDate GeneralizedTime,
543                     carsdType SEQUENCE OF UTF8String,
544                     cardsNumber SEQUENCE OF INTEGER,
545                     issuingMemberState SEQUENCE OF NationAlpha,
546                     cardsGeneration SEQUENCE OF INTEGER,
547                     numberOfSimilarEvent INTEGER
548             }
549
550             MotionDataError ::= SEQUENCE{
551                     beginDate GeneralizedTime,
552                     endDate GeneralizedTime,
553                     carsdType SEQUENCE OF UTF8String,
554                     cardsNumber SEQUENCE OF INTEGER,
555                     issuingMemberState SEQUENCE OF NationAlpha,
556                     cardsGeneration SEQUENCE OF INTEGER,
557                     numberOfSimilarEvent INTEGER
558             }
559
560             VehicleMotionConflict ::= SEQUENCE{
561                     beginDate GeneralizedTime,
562                     endDate GeneralizedTime,
563                     carsdType SEQUENCE OF UTF8String,
564                     cardsNumber SEQUENCE OF INTEGER,
565                     issuingMemberState SEQUENCE OF NationAlpha,
566                     cardsGeneration SEQUENCE OF INTEGER,
567                     numberOfSimilarEvent INTEGER
568             }
569
570             SecurityBreachAttempt ::= SEQUENCE{
571                     beginDate GeneralizedTime,
572                     endDate GeneralizedTime OPTIONAL,
573                     carsdType SEQUENCE OF UTF8String,
574                     cardsNumber SEQUENCE OF INTEGER,
575                     issuingMemberState SEQUENCE OF NationAlpha,
576                     numberOfSimilarEvent INTEGER,
577                     typeOfEvent SecurityBreachEvent
578             }
579
580
581             TimeConflict ::= SEQUENCE{
582                     beginDate GeneralizedTime,
583                     endDate GeneralizedTime,
584                     carsdType SEQUENCE OF UTF8String,
585                     cardsNumber SEQUENCE OF INTEGER,
586                     issuingMemberState SEQUENCE OF NationAlpha,
587                     cardsGeneration SEQUENCE OF INTEGER,
588                     numberOfSimilarEvent INTEGER
589             }
590
591             ---------------
592             --FAULTS LIST--
593             ---------------
594
595             CardFault ::= SEQUENCE{
```

▼B

```
596                     beginDate GeneralizedTime,
597                     endDate GeneralizedTime,
598                     carsdType SEQUENCE OF UTF8String,
599                     cardsNumber SEQUENCE OF INTEGER,
600                     issuingMemberState SEQUENCE OF NationAlpha,
601                     cardsGeneration SEQUENCE OF INTEGER,
602             }
603
604             RecordingEquipmentFault ::= SEQUENCE{
605                     beginDate GeneralizedTime,
606                     endDate GeneralizedTime,
607                     faultType RecordingEquipmentFaultType,
608                     carsdType SEQUENCE OF UTF8String,
609                     cardsNumber SEQUENCE OF INTEGER,
610                     issuingMemberState SEQUENCE OF NationAlpha,
611                     cardsGeneration SEQUENCE OF INTEGER,
612             }
613 END
```

▼B

Tillägg 14

FJÄRRKOMMUNIKATIONSFUNKTION

INNEHÅLLSFÖRTECKNING

1 INLEDNING

2 TILLÄMPNINGSOMRÅDE

3 FÖRKORTNINGAR, DEFINITIONER OCH BETECKNINGAR

4 DRIFTSCENARIER

4.1 Översikt

4.1.1 Nödvändiga förutsättningar för dataöverföring via gränssnitt för 5,8 GHz DSRC

4.1.2 Avläsarprofil 1a: via handriktad fjärravläsare eller fjärravläsare som är tillfälligt uppsatt och riktad vid vägkanten

4.1.3 Avläsarprofil 1b: via fjärravläsare som är monterad i och riktad från fordon

4.2 Säkerhet/integritet

5 FJÄRRKOMMUNIKATION – UTFORMNING OCH PROTOKOLL

5.1 Utformning

5.2 Arbetsgång

5.2.1 Arbetsmoment

5.2.2 Tolkning av data som mottagits via DSRC-kommunikation

5.3 Fysiska gränssnittsparametrar för DSRC och fjärrkommunikation

5.3.1 Begränsningar avseende placering

5.3.2 Ned- och upplänkningsparametrar

5.3.3 Antennutformning

5.4 Krav på DSRC-protokoll för RTM

5.4.1 Översikt

5.4.2 Kommandon

5.4.3 Kommandosekvens vid avläsning

5.4.4 Datastrukturer

5.4.5 Element i RtmData, operationer som utförs samt definitioner

5.4.6 Mekanism för dataöverföring

5.4.7 Detaljbeskrivning av DSRC-transaktion

5.4.8 Beskrivning av provning med DSRC-transaktion

5.5 Stöd för direktiv (EU) 2015/719

5.5.1 Översikt

5.5.2 Kommandon

▼B

5.5.3 Kommandosekvens vid avläsning

5.5.4 Datastrukturer

5.5.5 ASN.1-modul för OWS-transaktion via DSRC

5.5.6 Element i OwsData, operationer som utförs samt definitioner

5.5.7 Mekanismer för dataöverföring

5.6 Dataöverföring mellan fordonsenhetens DSRC-modul och fordonsenheten

5.6.1 Fysisk anslutning och gränssnitt

5.6.2 Tillämpningsprotokoll

5.7 Felhantering

5.7.1 Registrering och kommunikation av data i fordonsenhetens DSRC-modul

5.7.2 Fel i trådlös kommunikation

6 PROVNING VID DRIFTSÄTTNING OCH PERIODISK BESIKTNING AV FJÄRRKOMMUNIKATIONSFUNKTIONEN

6.1 Allmänt

6.2 ECHO

6.3 Prov för att validera skyddat datainnehåll

1 INLEDNING

I detta tillägg anges den utformning och de procedurer som ska följas för att säkerställa fjärrkommunikationsfunktionen (nedan kallad *kommunikationen*) såsom krävs i artikel 9 i förordning (EU) nr 165/2014 (nedan kallad *förordningen*).

DSC_1 I förordning (EU) nr 165/2014 fastställs att färdskrivaren ska vara utrustad med en fjärrkommunikationsfunktion som ska göra det möjligt för de behöriga kontrollmyndigheternas representanter (även kallade *kontrolltjänstemän*) att läsa färdskrivarinformation från passerande fordon med hjälp av utrustning för fjärravläsning (nedan kallad *fjärravläsare* eller *REDCR*, *Remote Early Detection Communication Reader*), eller mer specifikt sådan utrustning för trådlös anslutning via gränssnitt för 5,8 GHz DSRC (*Dedicated Short Range Communication*) enligt CEN.

Det är viktigt att inse att denna funktion är avsedd endast som ett inledande filter så att fordon kan väljas ut för närmare besiktning, och att den inte ersätter det formella besiktningsförfarande som fastställs i bestämmelserna i förordning (EU) nr 165/2014. Se skäl 9 i ingressen till den förordningen, som säger att kommunikation på distans mellan färdskrivare och kontrollmyndigheter vid kontroll ute på vägarna underlättar riktade vägkontroller.

DSC_2 *Data* ska utväxlas genom *kommunikationen* i form av en trådlös förbindelse som utnyttjar 5,8 GHz DSRC trådlös kommunikation som överensstämmer med detta tillägg och som provas mot lämpliga parametrar i EN 300 674-1, {*Electromagnetic compatibility and Radio spectrum Matters (ERM); Road*

▼B

Transport and Traffic Telematics (RTTT); Dedicated Short Range Communication (DSRC) transmission equipment (500 kbit/s/250 kbit/s) operating in the 5,8 GHz Industrial, Scientific and Medical (ISM) band; Part 1: General characteristics and test methods for Road Side Units (RSU) and On -Board Units (OBU)}.

DSC_3 *Kommunikationen* ska upprättas med kommunikationsutrustningen endast när detta begärs från den behöriga kontrollmyndighetens utrustning med hjälp av medel för radiokommunikation (*fjärravläsare*) som uppfyller relevanta krav.

DSC_4 *Data* ska skyddas för att säkerställa integritet.

DSC_5 Tillgång till *data* som kommuniceras ska begränsas till sådana behöriga kontrollmyndigheter med tillstånd att kontrollera överträdelser som avses i förordning (EG) nr 561/2006 och förordning (EU) nr 165/2014, och till verkstäder i den utsträckning som krävs för att kontrollera att färdskrivaren fungerar korrekt.

DSC_6 *Data* som utväxlas genom *kommunikationen* ska begränsas till de data som krävs för riktade vägkontroller av fordon med potentiellt manipulerade eller missbrukade färdskrivare.

DSC_7 Integritet och säkerhet för *data* ska uppnås genom att dessa skyddas inom fordonsenheten och genom att endast skyddade nyttolastdata och säkerhetsrelaterade data (se avsnitt 5.4.4) sänds via det trådlösa fjärrkommunikationsmediet i form av 5,8 GHz DSRC, vilket innebär att endast personer med tillstånd från de behöriga kontrollmyndigheterna har möjlighet att tolka de data som sänds genom *kommunikationen* och kontrollera deras autenticitet. Se tillägg 11 om gemensamma säkerhetsmekanismer.

DSC_8 *Data* ska innehålla en tidsstämpel som visar tidpunkten för senaste uppdatering.

DSC_9 Innehållet i säkerhetsdata ska endast vara känt och kontrolleras av de behöriga kontrollmyndigheterna, och av de parter till vilka de behöriga kontrollmyndigheterna delar med sig av innehållet, och innehållet faller utanför ramarna för den *kommunikation* som beskrivs i detta tillägg, förutom att *kommunikationen* ska tillhandahålla överföring av ett paket med säkerhetsdata tillsammans med varje paket med nyttolastdata.

DSC_10 Samma arkitektur och utrustning ska kunna användas för att skaffa tillgång till andra datakoncept (t.ex. ombordsystem för vägning) som utnyttjar den arkitektur som beskrivs här.

DSC_11 Förtydligande: I enlighet med bestämmelserna i artikel 7 i förordning (EU) nr 165/2014 får data som rör förarens identitet inte kommuniceras genom *kommunikationen*.

2 TILLÄMPNINGSOMRÅDE

I detta tillägg beskrivs hur de behöriga kontrollmyndigheternas representanter (även kallade *kontrolltjänstemän*) utnyttjar en specificerad trådlös kommunikation i form av 5,8 GHz DSRC för att på distans erhålla

▼B

data från ett visst fordon, som visar om fordonet är inblandat i en potentiell överträdelse av förordning (EU) nr 165/2014 och om man bör överväga att stoppa fordonet för vidare undersökning.

I förordning (EU) nr 165/2014 krävs att insamlade data ska begränsas till sådana data som visar en potentiell överträdelse eller är relevanta för detta, såsom definieras i artikel 9 i den förordningen.

I denna situation är den tid som är tillgänglig för kommunikation begränsad eftersom *kommunikationen* är riktad och utformad för kort avstånd. Samma kommunikationsmedel som används för fjärrövervakning av färdskrivare (RTM, *Remote Tachograph Monitoring*) kan dessutom utnyttjas av de behöriga kontrollmyndigheterna för andra tillämpningar (t.ex. högsta tillåtna vikter och största tillåtna dimensioner för tunga lastfordon såsom definieras i direktiv (EU) 2015/719). De behöriga kontrollmyndigheterna får själva besluta om sådant utnyttjande ska vara separerat eller sekventiellt i förhållande till övervakningen av färdskrivare.

I detta tillägg specificeras följande:

— Den utrustning och de procedurer och protokoll som ska användas i *kommunikationen*.

— De standarder och förordningar vars krav radioutrustningen ska uppfylla.

— Överlämningen av *data* till den utrustning som används i *kommunikationen*.

— Procedurer för förfrågan och överföring, samt i vilken ordning de olika operationerna sker.

— *Data* som ska överföras.

— Möjlig tolkning av de *data* som överförs genom *kommunikationen*.

— Bestämmelser om skyddade data som rör *kommunikationen*.

— De behöriga kontrollmyndigheternas tillgång till *data*.

— Möjligheten för *fjärravläsaren för tidig upptäckt* att begära olika datakoncept för *Freight and Fleet*.

Förtydligande: I detta tillägg specificeras inte följande:

— Drift och hantering i samband med insamling av *data* i fordonsenheten (denna ska bestämmas genom produktens utformning om inget annat anges i förordning (EU) nr 165/2014).

— Överlämningsform för insamlade data gentemot de behöriga kontrollmyndigheternas representant och kriterier som ska användas av den behöriga kontrollmyndigheten för att bestämma vilka fordon som ska stoppas (dessa ska bestämmas genom produktens utformning om inget annat anges i förordning (EU) nr 165/2014 eller i den behöriga kontrollmyndighetens policybeslut). Förtydligande: *Kommunikationen* innebär endast att *data* görs tillgängliga för de behöriga kontrollmyndigheterna så att de kan fatta väl underbyggda beslut.

— Bestämmelser om datasäkerhet (t.ex. kryptering) som rör innehållet i *data* (dessa specificeras i tillägg 11 om gemensamma säkerhetsmekanismer).

▼B

— Uppgifter om andra datakoncept än RTM som kan erhållas med hjälp av samma arkitektur och utrustning.

— Uppgifter om funktion och samverkan mellan fordonsenheten och fordonsenhetens DSRC-modul, samt funktion inom fordonsenhetens DSRC-modul (utöver tillhandahållande av *data* när detta begärs från en fjärravläsare för tidig upptäckt).

3 FÖRKORTNINGAR, DEFINITIONER OCH BETECKNINGAR

Följande förkortningar och definitioner som är särskilda för detta tillägg används i detta tillägg:

antenn	elektrisk anordning som omvandlar elektrisk energi till radiovågor och omvänt, och som används tillsammans med en radiosändare eller radiomottagare. I drift avger en radiosändare en elektrisk ström som svänger med radiofrekvens till antennens spetsar, och antennen utstrålar energin från den elektriska strömmen i form av elektromagnetiska vågor (radiovågor). Vid mottagningen fångar en antenn en del av den elektromagnetiska vågens energi för att generera en svag spänning vid sina spetsar, och spänningen förstärks sedan i en mottagare.
kommunikation	utväxling av information/data mellan en fjärravläsares DSRC-modul (även kallad *DSRC-REDCR* nedan) och en fordonsenhets DSRC-modul (även kallad *DSRC-VU* nedan) i enlighet med avsnitt 5 i en master-slave-konfiguration för att erhålla data.
data	skyddade data i definierat format (se avsnitt 5.4.4) som begärs av DSRC-REDCR och lämnas till DSRC-REDCR av DSRC-VU via en 5,8 GHz DSRC-länk såsom definieras i avsnitt 5 nedan.
förordning (EU) nr 165/2014	förordning (EU) nr 165/2014 av den 4 februari 2014 om färdskrivare vid vägtransporter, om upphävande av rådets förordning (EEG) nr 3821/85 om färdskrivare vid vägtransporter

▼B

	och om ändring av Europaparlamentets och rådets förordning (EG) nr 561/2006 om harmonisering av viss sociallagstiftning på vägtransportområdet.
AID	*Application Identifier* (tillämpningsidentifierare)
BLE	*Bluetooth Low Energy*
BST	*Beacon Service Table* (tabell med fjärravläsarens tjänster)
CIWD	*Card Insertion While Driving* (insättning av kort under körning)
CRC	*Cyclic Redundancy Check* (cyklisk redundanskontroll)
DSC (n)	Identifierare för ett specifikt krav i detta tillägg
DSRC	*Dedicated Short Range Communication* (radiokommunikation över korta avstånd)
DSRC-REDCR	*DSRC – Remote Early Detection Communication Reader* (DSRC-modul för fjärravläsare)
DSRC-VU	*DSRC – Vehicle Unit* (DSRC-modul för fordonsenhet). Denna ingår i den anordning för fjärravläst tidig upptäckt som definieras i bilaga 1C.
DWVC	*Driving Without Valid Card* (körning utan giltigt kort)
EID	*Element Identifier* (elementidentifierare)
LLC	*Logical Link Control* (länkprotokoll)
LPDU	*LLC Protocol Data Unit* (dataenhet enligt länkprotokoll)
OWS	*Onboard Weighing System* (ombordsystem för vägning)
PDU	*Protocol Data Unit* (dataenhet enligt protokoll)
REDCR	*Remote Early Detection Communication Reader* (fjärravläsare för tidig upptäckt). (Samma som den ”fjärravläsare för tidig upptäckt” som definieras i bilaga 1C.)
RTM	*Remote Tachograph Monitoring* (fjärrövervakning av färdskrivare)
SM-REDCR	*Security Module-Remote Early Detection Communication Reader* (säkerhetsmodul i fjärravläsare)
TARV	*Telematics Applications for Regulated Vehicles* (standard i serien ISO 15638)

▼B

VU	*Vehicle Unit* (fordonsenhet)
VUPM	*Vehicle Unit Payload Memory* (fordonsenhetens minne för nyttolastdata)
VUSM	*Vehicle Unit Security Module* (säkerhetsmodul i fordonsenhet)
VST	*Vehicle Service Table* (tabell med fordonets tjänster)
WIM	*Weigh In Motion* (vägning i rörelse)
WOB	*Weigh On Board* (vägning ombord)

Den specifikation som definieras i detta tillägg hänvisar till och är beroende av hela eller delar av följande förordningar och standarder. I respektive avsnitt i detta tillägg anges de relevanta standarderna eller de relevanta avsnitten i standarderna. I händelse av motstridiga uppgifter ska avsnitten i detta tillägg ha företräde. I händelse av motstridiga uppgifter och frånvaro av en tydligt fastställd specifikation i detta tillägg ska drift inom ERC 70-03 (och provning mot lämpliga parametrar i EN 300 674-1) ha företräde, följt i fallande ordning av EN 12795, EN 12253, EN 12834 och EN 13372, 6.2, 6.3, 6.4 och 7.1.

I detta tillägg hänvisas till följande förordningar och standarder:

[1] Europaparlamentets och rådets förordning (EU) nr 165/2014 av den 4 februari 2014 om färdskrivare vid vägtransporter, om upphävande av rådets förordning (EEG) nr 3821/85 om färdskrivare vid vägtransporter och om ändring av Europaparlamentets och rådets förordning (EG) nr 561/2006 om harmonisering av viss sociallagstiftning på vägtransportområdet.

[2] Europaparlamentets och rådets förordning (EG) nr 561/2006 av den 15 mars 2006 om harmonisering av viss sociallagstiftning på vägtransportområdet och om ändring av rådets förordningar (EEG) nr 3821/85 och (EG) nr 2135/98 samt om upphävande av rådets förordning (EEG) nr 3820/85.

[3] ERC 70-03 CEPT: ECC Recommendation 70-03: Relating to the Use of Short Range Devices (SRD)

[4] ISO 15638 Intelligent transport systems — Framework for cooperative telematics applications for regulated commercial freight vehicles (TARV).

[5] EN 300 674-1 Electromagnetic compatibility and Radio spectrum Matters (ERM); Road Transport and Traffic Telematics (RTTT); Dedicated Short Range Communication (DSRC) transmission equipment (500 kbit/s/250 kbit/s) operating in the 5,8 GHz Industrial, Scientific and Medical (ISM) band; Part 1: General characteristics and test methods for Road Side Units (RSU) and On-Board Units (OBU).

[6] EN 12253 Road transport and traffic telematics – Dedicated short-range communication – Physical layer using microwave at 5.8 GHz.

▼B

[7] EN 12795 Road transport and traffic telematics – Dedicated short-range communication – Data link layer: medium access and logical link control.

[8] EN 12834 Road transport and traffic telematics – Dedicated short-range communication – Application layer.

[9] EN 13372 Road transport and traffic telematics – Dedicated short-range communication – Profiles for RTTT applications

[10] ISO 14906 Electronic fee collection — Application interface definition for dedicated short- range communication

4 DRIFTSCENARIER

4.1 **Översikt**

I förordning (EU) nr 165/2014 anges specifika och kontrollerade scenarier där *kommunikationen* ska användas.

Dessa scenarier är följande:

”Communication Profile 1: Roadside inspection using a short range wireless communication Remote Early Detection Communication Reader instigating a physical roadside inspection (master-:-slave)

Reader Profile 1a: via a hand aimed or temporary roadside mounted and aimed Remote Early Detection Communication

Reader Profile 1b: via a vehicle mounted and directed Remote Early Detection Communication Reader”.

4.1.1 *Nödvändiga förutsättningar för dataöverföring via gränssnitt för 5,8 GHz DSRC*

ANMÄRKNING: Se figur 14.3 nedan för att förstå det sammanhang som ger de nödvändiga förutsättningarna.

4.1.1.1 Data som lagras i fordonsenhet

DSC_12 Fordonsenheten ska ansvara för att uppdatera data var 60:e sekund och för att underhålla de data som lagras i fordonsenheten, utan någon inblandning av funktionen för DSRC-kommunikation. Detta uppnås genom fordonsenhetens interna funktioner, såsom anges i förordning (EU) nr 165/2014 och i bilaga 1C, avsnitt 3.19 om fjärrkommunikation för riktade vägkontroller, och specificeras inte i detta tillägg.

4.1.1.2 Data som tillhandahålls fordonsenhetens DSRC-modul

DSC_13 Fordonsenheten ska ansvara för att färdskrivardata för DSRC-kommunikation (*data*) uppdateras så snart som de data som lagras i fordonsenheten uppdateras, med det intervall som bestäms i avsnitt 4.1.1.1 (DSC_12), utan någon inblandning av funktionen för DSRC-kommunikation.

DSC_14 Data från fordonsenheten ska användas som grund för att skapa och uppdatera *data*. Medlen för att åstadkomma detta specificeras i bilaga I C, avsnitt 3.19 om fjärrkommunikation för riktade vägkontroller. Om denna specifikation saknas bestäms medlen genom produktens utformning, och de specificeras inte i detta tillägg. När det gäller utformning av anslutningen mellan fordonsenhetens DSRC-modul och fordonsenheten, se avsnitt 5.6.

▼B

4.1.1.3 Datainnehåll

DSC_15 Innehåll och format för *data* ska vara sådant att det efter dekryptering är strukturerat och tillgängliggjort i den form och det format som specificeras i avsnitt 5.4.4 om datastrukturer i detta tillägg.

4.1.1.4 Dataöverlämning

DSC_16 *Data* som regelbundet uppdaterats i enlighet med procedurerna i avsnitt 4.1.1.1 ska skyddas innan de överlämnas till fordonsenhetens DSRC-modul (*DSRC-VU*) och överlämnas som ett skyddat datakoncept för tillfällig lagring som nuvarande version av *data* i fordonsenhetens DSRC-modul. Data överförs från fordonsenhetens säkerhetsmodul (*VUSM*) till DSRC-funktionen i form av fordonsenhetens minne för nyttolastdata (*VUPM*). *VUSM* och *VUPM* är funktioner och inte nödvändigtvis fysiska enheter. Den fysiska lösningen för att uppfylla dessa funktioner ska bestämmas genom produktens utformning om inget annat anges i förordning (EU) nr 165/2014.

4.1.1.5 Säkerhetsdata

DSC_17 Säkerhetsdata (*securityData)*, inklusive de data som krävs för att *fjärravläsaren* ska kunna dekryptera *data*, ska tillhandahållas såsom definieras i tillägg 11 om gemensamma säkerhetsmekanismer och överlämnas som ett datakoncept för tillfällig lagring i fordonsenhetens DSRC-modul som nuvarande version av *securityData* och i den form som definieras i avsnitt 5.4.4 i detta tillägg.

4.1.1.6 VUPM-data tillgängliga för överföring via DSRC-gränssnitt

DSC_18 Det datakoncept som alltid ska vara tillgängligt i DSRC-funktionen i form av fordonsenhetens minne för nyttolastdata (*VUPM*) för omedelbar överföring efter begäran från *fjärravläsaren* definieras i avsnitt 5.4.4 som en fullständigt specificerad ASN.1-modul.

Kommunikationsprofil 1 – allmän översikt

Denna profil omfattar det användningsfall där de behöriga kontrollmyndigheternas representant använder en *fjärravläsare för tidig upptäckt* (gränssnitt för 5,8 GHz DSRC som fungerar inom ERC 70-03 och som provats mot lämpliga parametrar från EN 300 674-1, såsom beskrivs i avsnitt 5) för att på distans identifiera ett fordon som är inblandat i en potentiell överträdelse av förordning (EU) nr 165/2014. När fordonet väl har identifierats bestämmer den representant från de behöriga kontrollmyndigheterna som kontrollerar avläsningen om fordonet bör stoppas.

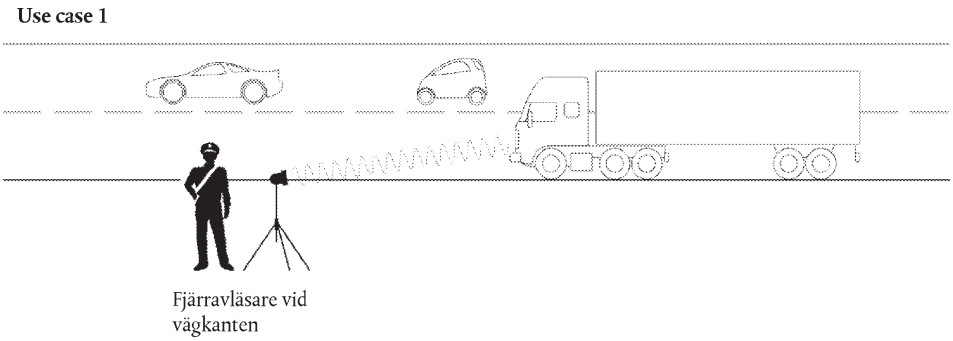
4.1.2 *Avläsarprofil 1a: via handriktad fjärravläsare eller fjärravläsare som är tillfälligt uppsatt och riktad vid vägkanten*

I detta användningsfall finns de behöriga kontrollmyndigheternas representant vid vägkanten och riktar en handhållen fjärravläsare, eller en fjärravläsare som är monterad på ett stativ eller flyttbar på annat sätt, från vägkanten mot mitten av fordonets vindruta. Avläsningen görs med hjälp av gränssnitt för 5,8 GHz DSRC som fungerar inom ERC 70-03 och som provats mot lämpliga parametrar i EN 300 674-1 såsom beskrivs i avsnitt 5. Se figur 14.1 (användningsfall 1).

▼B

Figur 14.1

Avläsning från vägkanten med 5,8 GHz DSRC

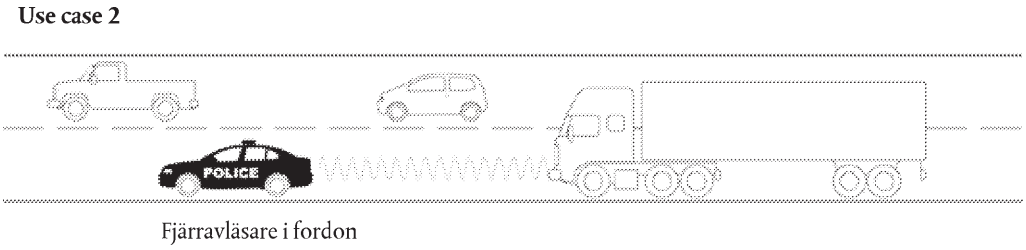


4.1.3 *Avläsarprofil 1b: via fjärravläsare som är monterad i och riktad från fordon*

I detta användningsfall finns de behöriga kontrollmyndigheternas representant i ett fordon i rörelse. Antingen riktar representanten en handhållen, flyttbar fjärravläsare från sitt fordon mot vindrutans mitt på det fordon som ska kontrolleras eller så är fjärravläsaren monterad i eller på fordonet så att den är riktad mot vindrutans mitt på det fordon som ska kontrolleras när representantens fordon är i en speciell position i förhållande till det fordon som ska kontrolleras (t.ex. direkt framför i trafiken). Avläsningen görs med hjälp av gränssnitt för 5,8 GHz DSRC som fungerar inom ERC 70-03 och som provats mot lämpliga parametrar i EN 300 674-1 såsom beskrivs i avsnitt 5. Se figur 14.2 (användningsfall 2).

Figur 14.2

Fordonsbaserad avläsning med 5.8 GHz DSRC



4.2 **Säkerhet/integritet**

För att göra det möjligt att verifiera autenticitet och integritet hos data som överförs genom fjärrkommunikation kontrolleras och dekrypteras skyddade data i enlighet med tillägg 11 om gemensamma säkerhetsmekanismer.

5 FJÄRRKOMMUNIKATION – UTFORMNING OCH PROTOKOLL

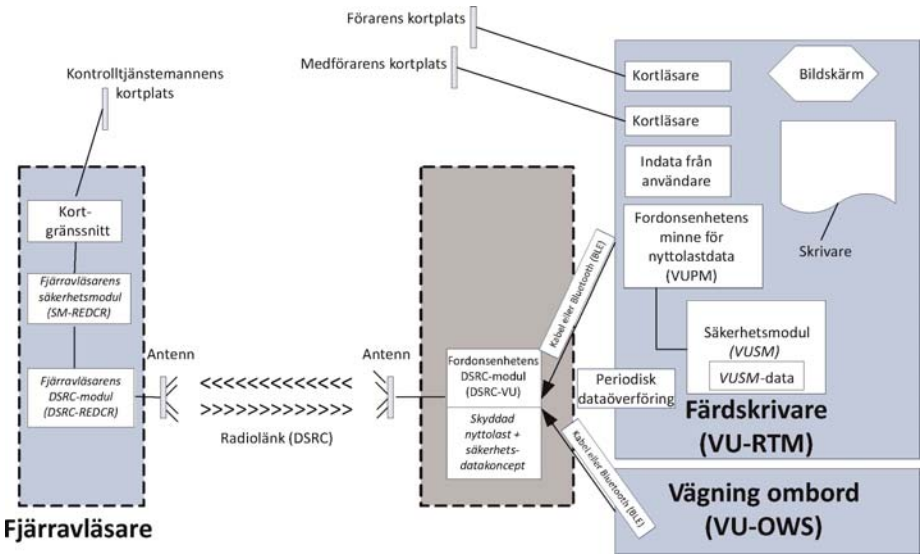
5.1 **Utformning**

Utformningen av fjärrkommunikationsfunktionen i en smart färdskrivare visas i figur 14.3.

▼B

Figur 14.3

Utformning av fjärrkommunikationsfunktion



DSC_19 Följande funktioner finns i fordonsenheten:

— *Säkerhetsmodul* (VUSM). Denna funktion i fordonsenheten ansvarar för att skydda de *data* som ska överföras från *fordonsenhetens DSRC-modul* (DSRC-VU) via fjärrkommunikation till de behöriga kontrollmyndigheternas representant.

— Skyddade data lagras i säkerhetsmodulens minne. Med de intervall som fastställs i avsnitt 4.1.1.1 (DSC_12) krypterar fordonsenheten datakonceptet för RTM (som omfattar nyttolastdata och säkerhetsdata med värden som fastställs nedan i detta tillägg) och kompletterar de data som finns i minnet i fordonsenhetens DSRC-modul. Säkerhetsmodulens funktion definieras i tillägg 11 om gemensamma säkerhetsmekanismer och faller utanför tillämpningsområdet för det här tillägget, förutom att den ska tillhandahålla uppdateringar till *fordonsenhetens minne för nyttolastdata* (VUPM) så snart som data i säkerhetsmodulen ändras.

— Kommunikationen mellan fordonsenheten och fordonsenhetens DSRC-modul kan ske via kabel eller BLE (*Bluetooth Low Energy*), och fordonsenhetens DSRC-modul kan fysiskt vara integrerad med antennen i fordonets vindruta eller vara placerad i fordonsenheten eller någonstans däremellan.

— Fordonsenhetens DSRC-modul ska alltid ha tillgång till en tillförlitlig strömkälla. Strömtillförseln kan lösas genom valfri utformning.

— Fordonsenhetens DSRC-modul ska ha ett permanent minne för att upprätthålla data i fordonsenhetens DSRC-modul även när fordonets tändning är avstängd.

— Om kommunikationen mellan fordonsenheten och fordonsenhetens DSRC-modul sker via BLE och strömkällan är ett ej uppladdningsbart batteri ska strömkällan för fordonsenhetens DSRC-modul bytas ut vid varje periodisk besiktning

▼B

och tillverkaren av utrustningen till fordonsenhetens DSRC-modul ska ansvara för att strömtillförseln är tillräcklig från en periodisk besiktning till nästa, så att en fjärravläsare har normal tillgång till data utan fel eller avbrott under hela perioden.

— *Fordonsenhetens minne för nyttolast* i form av RTM-data (VUPM). Denna funktion i fordonsenheten ansvarar för att tillhandahålla och uppdatera *data*. Datainnehållet (datatypen *TachographPayload*) definieras i avsnitt 5.4.4/5.4.5 nedan och uppdateras med det intervall som fastställs i avsnitt 4.1.1.1 (DSC_12).

— *Fordonsenhetens DSRC-modul* (DSRC-VU). Detta är den funktion som ingår i eller är ansluten till antennen, som kommunicerar med fordonsenheten via kabel eller trådlös (BLE) anslutning och som lagrar aktuella data (VUPM-data) och hanterar svaret på en begäran om avläsning med 5,8 GHz DSRC som medium. Bortkoppling av DSRC-funktionen eller störning under normal fordonsdrift ska tolkas som en överträdelse av förordning (EU) nr 165/2014.

— *Fjärravläsarens säkerhetsmodul* (SM-REDCR) är den funktion som används till att dekryptera och integritetskontrollera de data som kommer från fordonsenheten. Medlen för att åstadkomma detta fastställs i tillägg 11 om gemensamma säkerhetsmekanismer och definieras inte i det här tillägget.

— *Fjärravläsarens DSRC-modul* (DSRC-REDCR) omfattar en 5,8 GHz transceiver och tillhörande fast programvara och programvara som sköter *kommunikationen* med *fordonsenhetens DSRC-modul* i enlighet med detta tillägg.

— *Fjärravläsarens DSRC-modul* skickar en begäran till *fordonsenhetens DSRC-modul* i det fordon som ska kontrolleras och erhåller *data* (aktuella VUPM-data i det fordon som ska kontrolleras) via DSRC-länk och DSRC-processer och lagrar mottagna data i sin säkerhetsmodul.

— Antennen till fordonsenhetens DSRC-modul ska placeras på en plats där den ger en optimal DSRC-kommunikation mellan fordonet och antennen vid vägkanten (normalt i eller i närheten av centrum av fordonets vindruta …). För lätta fordon är det lämpligt med en motsvarande installation på vindrutans övre del.

— Det får inte finnas några metallföremål som kan störa kommunikationen (t.ex. namnskyltar, dekaler, antireflexfolie (för toning), solskydd, vindrutetorkare i viloläge) framför eller i närheten av antennen.

— Antennen ska monteras så att dess siktlinje är i stort sett parallell med vägbanan.

▼B

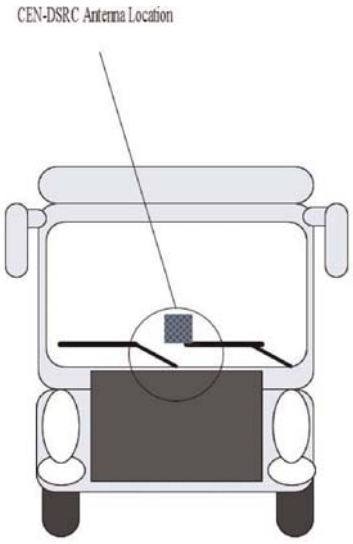
DSC_20 Antennen och kommunikationen ska fungera inom ERC 70-03, provade mot lämpliga parametrar i EN 300 674-1 såsom beskrivs i avsnitt 5. Antennen och kommunikationen kan utnyttja teknik, t.ex. filter för kommunikation med 5,8 GHz DSRC enligt CEN, för att minska radiostörningar såsom beskrivs i ECC-rapport 228.

DSC_21 DSRC-antennen ska vara ansluten till fordonsenhetens DSRC-modul, antingen direkt i modulen, monterad på eller i närheten av vindrutan, eller via en särskilt avsedd kabel som är utformad på ett sätt som försvårar lagstridig bortkoppling. Bortkoppling av antennen eller störning av dess funktion ska vara en överträdelse av förordning (EU) nr 165/2014. Avsiktlig maskning eller annan negativ påverkan på antennens driftsprestanda ska tolkas som en överträdelse av förordning (EU) nr 165/2014.

DSC_22 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 såsom fastställs i DSC_19 och visas i figur 14.4 (den ovala linjen), och så att den effektivt stöder de användningsfall som beskriv i avsnitt 4.1.2 och 4.1.3.

Figur 14.4

Exempel på placering av antenn för 5,8 GHz DSRC i vindrutan på reglerade fordon



Formfaktorn hos fjärravläsaren och dess antenn kan variera beroende på omständigheterna (läsaren stativmonterad, handhållen, fordonsmonterad osv.) och det tillvägagångssätt som används av de behöriga kontrollmyndigheternas representant.

En visnings- och/eller meddelandefunktion används för att presentera resultaten från fjärrkommunikationsfunktionen för de behöriga kontrollmyndigheternas representant. Visningen kan ske på en bildskärm, som en utskrift eller en audiosignal, eller som en kombination av sådana meddelanden. Formen för en sådan visning och/eller ett sådant meddelande beror på de krav som ställs av de behöriga kontrollmyndigheternas representanter och specificeras inte i detta tillägg.

▼B

DSC_23 Fjärravläsarens utformning och formfaktor ska vara en kommersiell fråga, inom ramarna for ERC 70-03 och de specifikationer för utformning och prestanda som anges i avsnitt 5.3.2 i detta tillägg, för att därigenom ge marknaden maximal flexibilitet att utforma och tillhandahålla utrustning som klarar de särskilda avläsningsscenarierna hos en viss behörig kontrollmyndighet.

DSC_24 Utformning och formfaktor för fordonsenhetens DSRC-modul och dess placering inuti eller utanför fordonsenheten ska vara en kommersiell fråga, inom ramarna for ERC 70-03 och de specifikationer för utformning och prestanda som anges i detta tillägg (avsnitt 5.3.2) och i det här avsnittet (5.1).

DSC_25 Fordonsenhetens DSRC-modul ska dock kunna godta datakonceptvärden från annan intelligent fordonsutrustning genom öppna branschstandarder för anslutningar och protokoll (t.ex. från ombordsystem för vägning) så länge sådana datakoncept identifieras genom unika och kända tillämpningsidentifierare, och instruktioner för att hantera sådana protokoll ska göras tillgängliga av Europeiska kommissionen och vara tillgängliga utan kostnad för tillverkare av relevant utrustning.

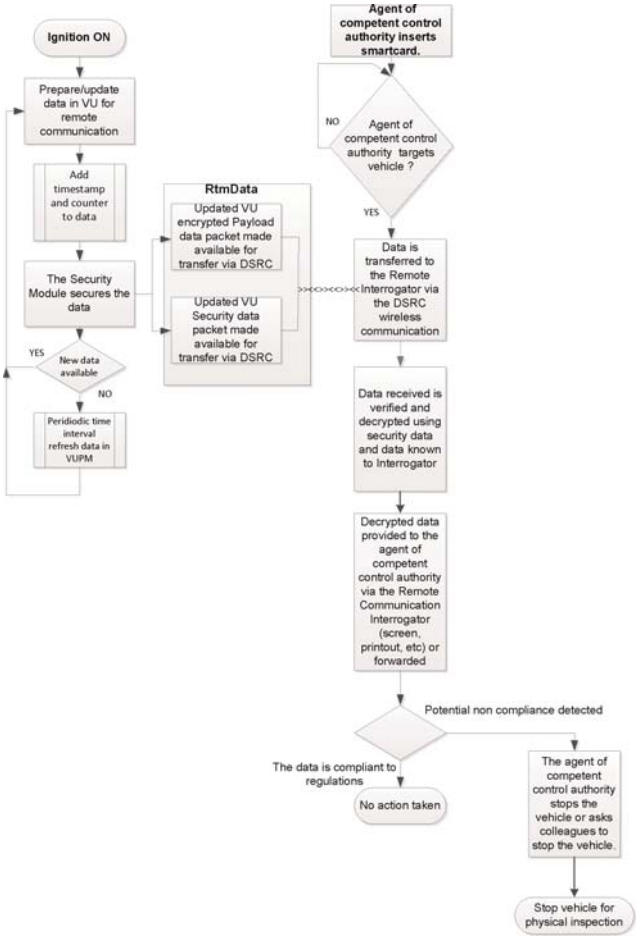
5.2 **Arbetsgång**

5.2.1 *Arbetsmoment*

Arbetsgången och de ingående arbetsmomenten visas i figur 14.5.

Figur 14.5

Arbetsgång för fjärrkommunikationsfunktion



▼B

De olika stegen beskrivs nedan:

a. Så snart fordonet är i drift (tändning påslagen, *Ignition ON*) förses fordonsenheten med data från färdskrivaren. Fordonsenheten förbereder *data* för fjärrkommunikationsfunktionen (krypterade) och uppdaterar *fordonsenhetens minne för nyttolastdata* (VUPM) och minnet i *fordonsenhetens DSRC-modul* (DSRC-VU) såsom anges i avsnitten 4.1.1.1–4.1.1.2. Insamlade *data* ska formateras såsom fastställs i avsnitt 5.4.4–5.4.5 nedan.

b. Vid varje uppdatering av *data* ska tidsstämpeln i säkerhetsdatakonceptet uppdateras.

c. *Fordonsenhetens säkerhetsmodul* (VUSM) skyddar data i enlighet med de förfaranden som fastställs i tillägg 11.

d. Vid varje uppdatering av *data* (se avsnitt 4.1.1.1–4.1.1.2) ska dessa *data* överföras till *fordonsenhetens DSRC-modul* där de ersätter eventuella tidigare data, för att uppdaterade innevarande *data* alltid ska finnas tillgängliga om en avläsning begärs från en *fjärravläsare* (REDCR). *Data* från fordonsenheten till *fordonsenhetens DSRC-modul* ska kunna identifieras genom filnamnet *RTMData* eller genom en tillämpningsidentifierare och attributidentifierare.

e. Om de behöriga kontrollmyndigheternas representant vill kontrollera ett fordon och samla in *data* från detta fordon ska representanten först sätta in sitt smartkort i *fjärravläsaren* för att aktivera *kommunikationen* och tillåta att *fjärravläsarens säkerhetsmodul* (SM-REDCR) kontrollerar kortets autenticitet och dekrypterar dess data.

f. De behöriga kontrollmyndigheternas representant riktar sedan *fjärravläsaren* mot ett fordon och begär data via fjärrkommunikation. *Fjärravläsaren* öppnar en gränssnittssession för 5,8 GHz DSRC med *fordonsenhetens DSRC-modul* i det fordon som ska kontrolleras och begär *data*. *Data* överförs till *fjärravläsaren* via det trådlösa kommunikationssystem som ett DSR-attribut med hjälp av tillämpningstjänsten GET såsom definieras i avsnitt 5.4. Attributet innehåller krypterade värden som nyttolastdata och säkerhetsdata för DSRC.

g. Data analyseras av utrustningen i *fjärravläsaren* och lämnas till de behöriga kontrollmyndigheternas representant.

h. De behöriga kontrollmyndigheternas representant använder mottagna data som stöd för att besluta om fordonet ska stoppas för en detaljerad besiktning, eller om en annan representant ska ombes göra detta.

5.2.2 *Tolkning av data som mottagits via DSRC-kommunikation*

DSC_26 Data som tas emot via gränssnittet för 5,8 GHz ska motsvara den innebörd och det format som definieras i avsnitten 5.4.4 och 5.4.5 nedan och endast denna innebörd och detta format, och de ska tolkas inom de ramar som definieras där. I enlighet med bestämmelserna i förordning (EU) nr 165/2014 får

▼B

data endast användas för att lämna relevant information till en behörig kontrollmyndighet, som hjälp för att avgöra vilket fordon som bör stoppas för en fysisk besiktning, och dessa data ska därefter förstöras i enlighet med artikel 9 i förordning (EU) nr 165/2014.

5.3 **Fysiska gränssnittsparametrar för DSRC och fjärrkommunikation**

5.3.1 *Begränsningar avseende placering*

DSC_27 Fjärravläsning av fordon med gränssnitt för 5,8 GHz DSRC bör inte användas inom 200 meter från en portal för 5,8 GHz DSRC som är i drift.

5.3.2 *Ned- och upplänkningsparametrar*

DSC_28 Den utrustning som används för fjärrövervakning av färdskrivare ska överensstämma med och fungera inom ERC 70-03 och de parametrar som definieras i tabellerna 14.1 och 14.2 nedan.

DSC_29 För att säkerställa kompatibilitet med driftsparametrar för andra standardiserade 5.8 GHz DSRC-system ska utrustningen som används för fjärrövervakning av färdskrivare dessutom överensstämma med parametrar från EN 12253 och EN 13372.

Närmare bestämt:

Tabell 14.1

Nedlänkningsparametrar

Parameternummer (*Item No.*)	Parameter	Värde(n)	Anmärkning
D1	Bärfrekvenser för nedlänkning	Det finns fyra alternativ som kan användas av en fjärravläsare: 5,7975 GHz 5,8025 GHz 5,8075 GHz 5,8125 GHz	Inom ERC 70-03. Bärfrekvenser får väljas av den som utformar systemet för vägkontroller och behöver inte vara kända för fordonsenhetens DSRC-modul. (Överensstämmer med EN 12253, EN 13372).
D1a (*)	Tolerans för bär-frekvenser	Inom ± 5 ppm.	(Överensstämmer med EN 12253.)
D2 (*)	Sändarens spektrummask för RSU (fjärravläsare)	Inom ERC 70-03. Fjärravläsaren ska överensstämma med klass B,C enligt definition i EN 12253. Inga andra särskilda krav i detta tillägg.	Parameter som används för att kontrollera interferens mellan fjärravläsare som finns nära varandra (enligt definition i EN 12253 och EN 13372).
D3	Minsta frekvensområde för OBU (fordonsenhetens DSRC-modul)	5,795–5,815 GHz	(Överensstämmer med EN 12253.)
D4 (*)	Maximal effekttäthet (EIRP)	Inom ERC 70-03 (utan licens) och inom nationell lagstiftning. Maximum +33 dBm.	(Överensstämmer med EN 12253.)

▼B

Parameternummer (*Item No.*)	Parameter	Värde(n)	Anmärkning
D4a	Vinkelbaserad EIRP-mask	I enlighet med deklarerad och offentliggjord specifikation från fjärravläsarens konstruktör.	(Överensstämmer med EN 12253.)
D5	Polarisering	Vänster, cirkulär	(Överensstämmer med EN 12253.)
D5a	Korspolarisering	XPD: I siktlinjen: RSU (fjärravläsare): t ≥ 15 dB OBU (fordonsenhetens DSRC-modul): r ≥ 10 dB Vid området med – 3 dB: RSU (fjärravläsare): t ≥ 10 dB OBU (fordonsenhetens DSRC-modul): r ≥ 6 dB	(Överensstämmer med EN 12253.)
D6 (*)	Modulering	Amplitudmodulering, två nivåer.	(Överensstämmer med EN 12253.)
D6a (*)	Moduleringsindex	0,5 ... 0,9	(Överensstämmer med EN 12253.)
D6b	Ögonmönster	≥ 90 % (tid) / ≥ 85 % (amplitud)	
D7 (*)	Datakodning	FM0 En ”1”-bit har övergångar endast i början och slutet av bitintervallet. En ”0”-bit har jämfört med ”1”-biten ytterligare en övergång i mitten av bitintervallet.	(Överensstämmer med EN 12253.)
D8 (*)	Bithastighet	500 kbit/s	(Överensstämmer med EN 12253.)
D8a	Bitklockans tolerans	Bättre än ± 100 ppm.	(Överensstämmer med EN 12253.)
D9 (*)	Nivå för bitfel (BER, *Bit Error Rate*) i kommunikation	$\leq 10^{-6}$ när inkommande effekt (*incident power*) vid OBU (fordonsenhetens DSRC-modul) är i det intervall som ges av [D11a–D11b].	(Överensstämmer med EN 12253.)
D10	Utlösare för väckning (*wake-up trigger*) för OBU (fordonsenhetens DSRC-modul).	OBU (fordonsenhetens DSRC-modul) ska väckas vid mottagande av varje ram med minst 11 oktetter (inklusive ingress (*preamble*)).	Inget särskilt väckningsmönster krävs. Fordonsenhetens DSRC-modul får väckas vid mottagande av en ram med färre än 11 oktetter. (Överensstämmer med EN 12253.)
D10a	Maximal starttid	≤ 5 ms	(Överensstämmer med EN 12253.)
D11	Kommunikationszon	Rumslig region (*spatial region*) inom vilken nivån för bitfel (BER, i enlighet med D9a) uppnås.	(Överensstämmer med EN 12253.)
D11a (*)	Effektgräns för kommunikation (övre)	– 24 dBm	(Överensstämmer med EN 12253.)

▼B

Parameternummer (*Item No.*)	Parameter	Värde(n)	Anmärkning
D11b (*)	Effektgräns för kommunikation (nedre)	Inkommande effekt: – 43 dBm (siktlinje) – 41 dBm (mellan – 45° och +45°, motsvarande det plan som är parallellt med vägbanan när fordonsenhetens DSRC-modul senare installeras i fordonet (azimut)).	(Överensstämmer med EN 12253.) Utökat krav för horisontella vinklar upp till ±45°, till följd av de användningsfall som definieras i detta tillägg.
D12 (*)	Nivå för frånkopplingseffekt för fordonsenhetens DSRC-modul	– 60 dBm	(Överensstämmer med EN 12253.)
D13	Ingress (*preamble*)	Ingress är obligatorisk.	(Överensstämmer med EN 12253.)
D13a	Ingressens längd och mönster	16 bitar ±1 bit i form av FM0-kodade ”1”-bitar.	(Överensstämmer med EN 12253.)
D13b	Ingressens vågform	En alternerande sekvens av låg nivå och hög nivå med en pulsvaraktighet på 2 µs. Toleransen ges av D8a.	(Överensstämmer med EN 12253.)
D13c	Slutbitar (*trailing bits*)	RSU (fjärravläsaren) tillåts överföra maximalt 8 bitar efter slutflaggan. En OBU (fordonsenhetens DSRC-modul) måste inte ta hänsyn till dessa ytterligare bitar.	(Överensstämmer med EN 12253.)

(*) Nedlänkningsparametrar som är föremål för överensstämmelseprovning i enlighet med relevanta parameterprov i EN 300 674-1.

Tabell 14.2

Upplänkningsparametrar

Parameternummer (*Item No.*)	Parameter	Värde(n)	Anmärkning
U1 (*)	Underbärfrekvenser (*subcarrier frequencies*)	En OBU (fordonsenhetens DSRC-modul) ska stödja 1,5 MHz och 2,0 MHz. En RSU (fjärravläsare) ska stödja 1,5 MHz eller 2,0 MHz eller båda. U1-0: 1,5 MHz U1-1: 2,0 MHz	Val av underbärfrekvens (1,5 MHz eller 2,0 MHz) beror på vilken profil som väljs i EN 13372.
U1a (*)	Tolerans för underbärfrekvenser	Inom ± 0,1 %.	(Överensstämmer med EN 12253.)
U1b	Användning av sidoband	Samma data på båda sidor.	(Överensstämmer med EN 12253.)
U2 (*)	Sändarens spektrummask för OBU (fordonsenhetens DSRC-modul)	I enlighet med EN12253. 1) Bandeffekt ut (*out band power*): se ETSI EN 300674-1.	(Överensstämmer med EN 12253.)

▼B

Parameternummer (*Item No.*)	Parameter	Värde(n)	Anmärkning
		2) Bandeffekt in (*in band power*): [U4a] dBm vid 500 kHz. 3) Emission i alla andra upplänks-kanaler: U2(3)-1 = – 35 dBm vid 500 kHz.	
U4a (*)	Maximal effekttäthet, enkelt sidband (*maximum single side band E.I.R.P.*) (siktlinje)	Två alternativ: U4a-0: – 14 dBm U4a-1: – 21 dBm	Enligt deklarerad och offentliggjord specifikation från utrustningens konstruktör.
U4b (*)	Maximal effekttäthet, enkelt sidband (*maximum single side band E.I.R.P.*) (35°)	Två alternativ: — Ej tillämpligt — – 17 dBm	Enligt deklarerad och offentliggjord specifikation från utrustningens konstruktör.
U5	Polarisering	Vänster, cirkulär	(Överensstämmer med EN 12253.)
U5a	Korspolarisering	XPD: I siktlinjen: RSU (fjärravläsare): r ≥ 15 dB OBU (fordonsenhetens DSRC-modul): t ≥ 10 dB Vid – 3 dB: RSU (fjärravläsare): r ≥ 10 dB OBU (fordonsenhetens DSRC-modul): t ≥ 6 dB	(Överensstämmer med EN 12253.)
U6	Modulering av underbärvåg	2-PSK Kodade data, synkroniserade med underbärvåg: övergångar för kodade data sammanfaller med övergångar för underbärvåg.	(Överensstämmer med EN 12253.)
U6b	Pulsförhållande	Pulsförhållande: 50 % ± α, α ≤ 5 %	(Överensstämmer med EN 12253.)
U6c	Modulering av bärvåg	Multiplikation av modulerad underbärvåg och bärvåg.	(Överensstämmer med EN 12253.)
U7 (*)	Datakodning	NRZI (ingen övergång i början av ”1”-bit, övergång i början av ”0”-bit, ingen övergång inom bit).	(Överensstämmer med EN 12253.)
U8 (*)	Bithastighet	250 kbit/s	(Överensstämmer med EN 12253.)
U8a	Tolerans för bitklocka	Inom ± 1 000 ppm.	(Överensstämmer med EN 12253.)
U9	Nivå för bitfel (BER, *Bit Error Rate*) i kommunikation	$\leq 10^{-6}$	(Överensstämmer med EN 12253.)

▼B

Parameternummer (*Item No.*)	Parameter	Värde(n)	Anmärkning
U11	Kommunikationszon	Den rumsliga region (*spatial region*) inom vilken fordonsenhetens DSRC-modul finns så att dess överföringar tas emot av fjärravläsaren med nivå för bitfel som är lägre än den som ges av U9a.	(Överensstämmer med EN 12253.)
U12a (*)	Omvandlingsvinst (*conversion gain*) (lägre gräns)	1 dB för varje sidband. Vinkelintervall: Cirkulärt och symmetriskt mellan siktlinje och ±35° och	
		mellan – 45° och + 45°, motsvarande det plan som är parallellt med vägbanan när fordonsenhetens DSRC-modul senare installeras i fordonet (azimut).	Större än det angivna värdeintervallet för horisontella vinklar upp till ± 45°, till följd av de användningsfall som definieras i detta tillägg.
U12b (*)	Omvandlingsvinst (*conversion gain*) (övre gräns)	10 dB för varje sidband.	Mindre än det angivna värdeintervallet för varje sidband inom en cirkulär kon runt siktlinjen med ± 45° öppningsvinkel.
U13	Ingress (*preamble*)	Ingress är obligatorisk.	(Överensstämmer med EN 12253.)
U13a	Ingress (*preamble*) längd och mönster	32–36 μs, modulerad endast med underbärvåg, därefter 8 bitar i form av NRZI-kodade ”0”-bitar.	(Överensstämmer med EN 12253.)
U13b	Slutbitar (*trailing bits*)	Fordonsenhetens DSRC-modul tillåts överföra maximalt 8 bitar efter slutflaggan. En RSU (fjärravläsare) måste inte ta hänsyn till dessa ytterligare bitar.	(Överensstämmer med EN 12253.)

(*) Upplänkningsparametrar som är föremål för överensstämmelseprovning i enlighet med relevanta parameterprov i EN 300 674-1.

5.3.3 *Antennutformning*

5.3.3.1 Fjärravläsarens antenn

DSC_30 *Fjärravläsarens* antenn ska utformas på grundval av kommersiella faktorer och fungera inom de gränser som definieras i avsnitt 5.3.2 och som är anpassade för att optimera avläsningsprestanda för *fjärravläsarens DSRC-modul* utifrån dess syfte och de avläsningsförhållanden som *fjärravläsaren* är utformad för.

5.3.3.2 Fordonsenhetens antenn

DSC_31 Antennen till *DSRC-VU* ska utformas på grundval av kommersiella faktorer och fungera inom de gränser som definieras i avsnitt 5.3.2 och som är anpassade för att optimera avläsningsprestanda för *fjärravläsarens DSRC-modul* utifrån dess syfte och de avläsningsförhållanden som *fjärravläsaren* är utformad för.

▼B

DSC_32 Fordonsenhetens antenn ska monteras på eller i närheten av vindrutan såsom anges i avsnitt 5.1 ovan.

DSC_33 I provningsmiljö i en verkstad (se avsnitt 6.3) ska antennen till en fordonsenhets DSRC-modul, monterad i enlighet med avsnitt 5.1 ovan, klara att ansluta till en standardiserad provningskommunikation och att tillhandahålla en RTM-transaktion såsom definieras i detta tillägg över ett avstånd av mellan 2 och 10 meter under mer än 99 % av tiden, räknad som ett medelvärde av 1 000 avläsningar.

5.4 **Krav på DSRC-protokoll för RTM**

5.4.1 *Översikt*

DSC_34 Transaktionsprotokollet för överföring av *data* via gränssnittslänken för 5,8 GHz DSRC ska överensstämma med följande steg. I detta avsnitt beskrivs ett transaktionsflöde under ideala förhållanden utan omsändningar eller kommunikationsavbrott.

ANMÄRKNING: Syftet med initieringsfasen (steg 1) är att upprätta kommunikationen mellan *fjärravläsaren* och DSRC-modulerna i de fordonsenheter som rör sig in i transaktionszonen för 5,8 GHz DSRC (*master-slave*) men ännu inte upprättat kommunikation med *fjärravläsaren*, och att väcka tillämpningsprocesserna.

— **Steg 1** Initiering. *Fjärravläsaren* (även kallad *interrogator*) sänder en ram med en BST (*Beacon Service Table*) som inbegriper tillämpningsidentifierare (AID) för de tjänster som den stöder. För RTM-tillämpningen gäller endast tjänsten med AID = 2 (*Freight&Fleet*). *Fordonsenhetens DSRC-modul* (DSRC-VU) utvärderar mottagen BST och ska svara (se nedan) med en lista över de tillämpningar som stöds inom domänen *Freight&Fleet*, eller inte svara alls om ingen tillämpning stöds. Om *fjärravläsaren* inte erbjuder AID = 2 ska fordonsenhetens DSRC-modul inte besvara fjärravläsaren.

— **Steg 2** *Fordonsenhetens DSRC-modul* sänder en ram med en begäran om tilldelning av ett privat fönster.

— **Steg 3** *Fjärravläsaren* sänder en ram med en tilldelning av ett privat fönster.

— **Steg 4** *Fordonsenhetens DSRC-modul* använder det tilldelade privata fönstret för att sända en ram med sin VST (*Vehicle Service Table*). Denna VST inbegriper en lista med alla olika tillämpningsinstanser som *fordonsenhetens DSRC-modul* stöder inom ramen för AID = 2. De olika instanserna ska identifieras med hjälp av unikt genererade EID (*Element Identifier*), var och en med ett parametervärde i form av en tillämpningsmarkering (*Application Context Mark*) som anger den tillämpning och den standard som stöds.

— **Steg 5** *Fjärravläsaren* analyserar sedan erbjuden VST och antingen avslutar anslutningen (RELEASE) eftersom VST inte har något av intresse att erbjuda (dvs. mottagen VST kommer från en fordonsenhet vars DSRC-modul inte stöder RTM-transaktioner) eller startar en instans av tillämpningen (*app instantiation*) (om mottagen VST är lämplig för detta).

▼B

— **Steg 6** För att åstadkomma detta ska fjärravläsaren sända en ram med ett kommando för att hämta RTM-data och identifiera tillämpningsinstansen för RTM genom att ange den identifierare som angavs av fordonsenhetens DSRC-modul i VST, och tilldela ett privat fönster.

— **Steg 7** *Fordonsenhetens DSRC-modul* använder det just tilldelade privata fönstret för att sända en ram med den adresserade identifierare som motsvarar tillämpnings-instansen för RTM i VST, följd av attributet *RtmData* (nyttolastelement och säkerhetselement).

— **Steg 8** Om flera tjänster begärs ändras värdet ”n” till referensnumret för nästa tjänst och processen upprepas.

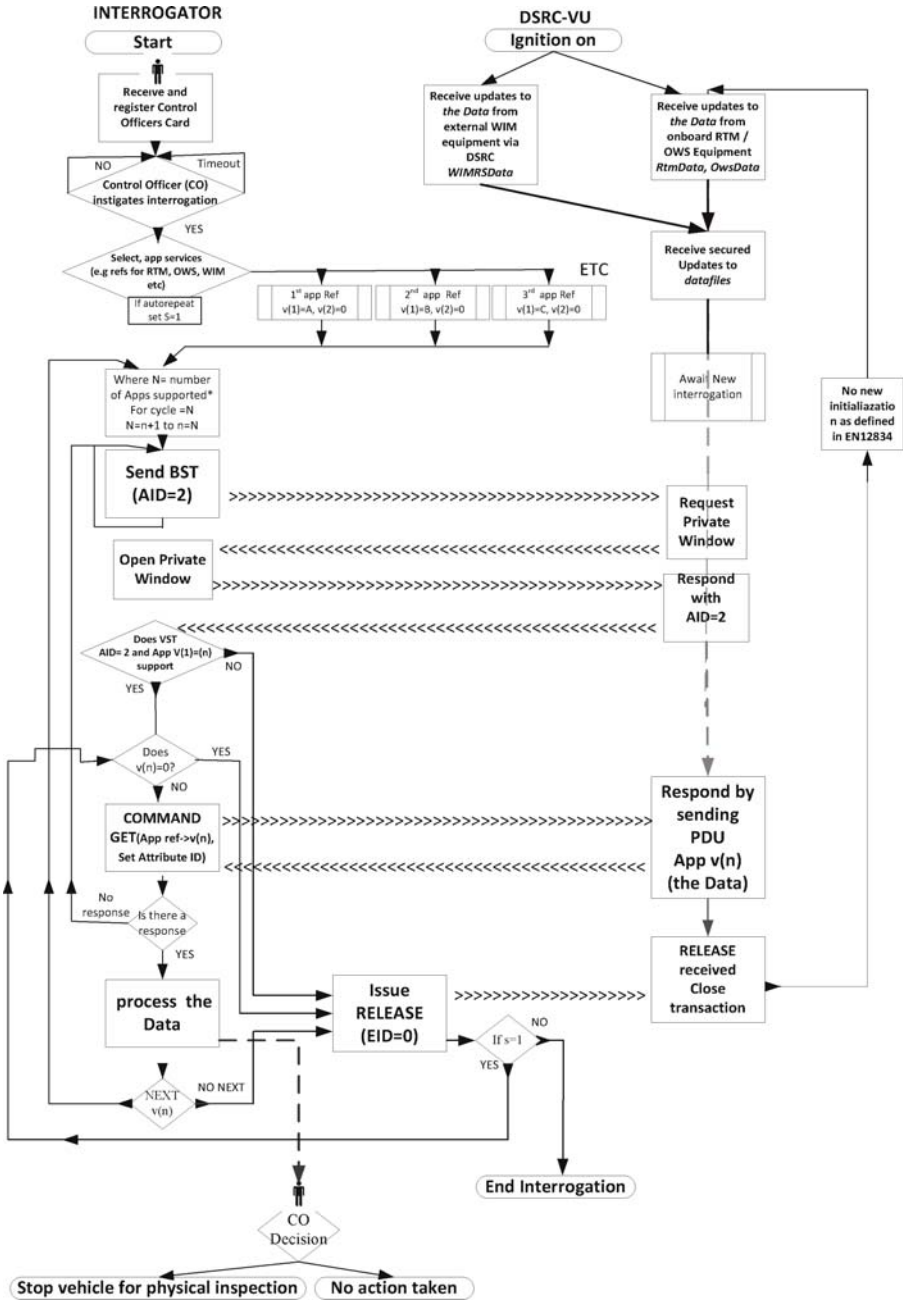
— **Steg 9** *Fjärravläsaren* antingen bekräftar att data tagits emot genom att sända en ram med ett RELEASE-kommando till *fordonsenhetens DSRC-modul* för att avsluta sessionen eller går tillbaka till steg 6 (om den misslyckades med att validera en lyckad mottagning av LDPU).

Se figur 14.6 som en illustration av transaktionsprotokollet.

▼B

Figur 14.6

Processflöde för RTM via 5,8 GHz DSRC



5.4.2 *Kommandon*

DSC_35 Följande kommandon är de enda funktioner som används i en transaktionsfas för RTM-data.

— **INITIALISATION.request**: Ett kommando som sänds ut i alla riktningar från fjärravläsaren och som anger vilka tillämpningar fjärravläsaren stöder.

— **INITIALISATION.response**: Ett svar från fordonsenhetens DSRC-modul (DSRC-VU) som bekräftar anslutningen och innehåller en lista med de tillämpningsinstanser som stöds, deras egenskaper och information om hur de ska adresseras (EID).

▼B

— **GET.request**: Ett kommando som sänds från fjärravläsaren till fordonsenhetens DSRC-modul och som anger tillämpningsinstansen som ska adresseras med hjälp av en definierat EID, såsom den tas emot i VST, och ger instruktioner till fordonsenhetens DSRC-modul att sända de utvalda attributen som data. Syftet med kommandot GET är att fjärravläsaren ska få data från fordonsenhetens DSRC-modul.

— **GET.response**: Ett svar från fordonsenhetens DSRC-modul som innehåller de data som fjärravläsaren begärt.

— **ACTION.request ECHO**: Ett kommando som ger instruktioner till fordonsenhetens DSRC-modul att sända tillbaka data från fordonsenhetens DSRC-modul till fjärravläsaren. Syftet med kommandot ECHO är att ge verkstäder eller anläggningar för typgodkännandeprov möjlighet att prova om DSRC-länken fungerar, utan att behöva ha tillgång till säkerhetsuppgifter.

— **ACTION**.response ECHO: Ett svar från fordonsenhetens DSRC-modul på kommandot ECHO.

— **EVENT_REPORT.request** RELEASE: Ett kommando som ger instruktioner till fordonsenhetens DSRC-modul att transaktionen avslutas. Syftet med kommandot RELEASE är att avsluta sessionen med fordonsenhetens DSRC-modul. Efter att ha mottagit RELEASE ska fordonsenhetens DSRC-modul inte svara på några ytterligare avläsningar inom den aktuella anslutningen. Notera att enligt EN 12834 kommer en fordonsenhets DSRC-modul inte att godta två förbindelser med samma avläsare, såvida inte avläsaren varit utanför kommunikationszonen under 255 sekunder eller avläsarens identifierare (*beacon ID*) ändrats.

5.4.3 *Kommandosekvens vid avläsning*

DSC_36 En transaktion beskrivs så här i form av en sekvens av kommandon och svar:

Sekvens	Sändare		Mottagare	Beskrivning	Operation
1	REDCR	>	DSRC-VU	Initiering av kommunikations-länk – begäran	REDCR sänder ut BST i alla riktningar
2	*DSRC-VU*	>	*REDCR*	*Initiering av kommunikations-länk – svar*	*Om BST stöder AID=2 så begär DSRC-VU ett privat fönster*
3	REDCR	>	DSRC-VU	Beviljar ett privat fönster	Sänder ram med tilldelning av privat fönster
4	*DSRC-VU*	>	*REDCR*	*Sänder VST*	*Sänder ram som omfattar VST*
5	REDCR	>	DSRC-VU	Sänder GET.request för data i attribut till specifik EID	
6	*DSRC-VU*	>	*REDCR*	*Sänder GET.response med begärt attribut för specifik EID*	*Sänder attribut (RTMData, OWSData, ...) med data för specifik EID*

▼B

Sekvens	Sändare		Mottagare	Beskrivning	Operation
7	REDCR	>	DSRC-VU	Sänder GET.request för data som hör till annat attribut (om detta är lämpligt)	
8	*DSRC-VU*	>	*REDCR*	*Sänder GET.response med begärt attribut*	*Sänder attribut med data för specifik EID*
9	REDCR	>	DSRC-VU	Kvitterar lyckat mottagande av data	Sänder RELEASE-kommando som stänger transaktionen
10	*DSRC-VU*			*Stänger transaktionen*	

I avsnitten 5.4.7 och 5.4.8 finns ett exempel på en transaktionssekvens och innehållet i de utväxlade ramarna.

5.4.4 *Datastrukturer*

DSC_37 Den semantiska strukturen hos de *data* som passerar genom gränssnittet för 5,8 GHz DSRC ska vara förenlig med den som beskrivs i detta tillägg. Strukturen för dessa data specificeras i det här avsnittet.

DSC_38 Nyttolasten (RTM-data) består av en konkatenering av följande:

1. Data i form av EncryptedTachographPayload, som är krypterade från den nyttolast (TachographPayload) som finns definierad i ASN.1 i avsnitt 5.4.5. Krypteringsmetoden beskrivs i tillägg 11.

2. DSRCSecurityData, specificeras i tillägg 11.

DSC_39 RTM-data adresseras som RTM Attribute=1 och överförs i RTM-container =10.

DSC_40 Markeringen för RTM Context (*RTM Context Mark*) ska ange den del av en standard i serien av TARV-standarder som stöds (RTM motsvarar del 9).

ASN.1-modulen för DSRC-data inom RTM-tillämpningen definieras på följande sätt:

▼B

```
TarvRtm {iso(1) standard(0) 15638 part9(9) version1(1)}
DEFINITIONS AUTOMATIC TAGS
::= BEGIN
IMPORTS
-- Imports data attributes and elements from EFC which are used for RTM
LPN
FROM EfcDsrcApplication {iso(1) standard(0) 14906 application(0) version5(5)}

-- Imports function parameters from the EFC Application Interface Definition
SetMMIRq
FROM EfcDsrcApplication {iso(1) standard(0) 14906 application(0) version5(5)}

-- Imports the L7 DSRCData module data from the EFC Application Interface Definition
Action-Request, Action-Response, ActionType, ApplicationList, AttributeIdList, AttributeList,
Attributes,
BeaconID, BST, Dsrc-EID, DSRCApplicationEntityID, Event-Report-Request, Event-Report- Response,
EventType, Get-Request, Get-Response, Initialisation-Request, Initialisation-Response,
ObeConfiguration, Profile, ReturnStatus, Time, T-APDUs, VST
FROM EfcDsrcGeneric {iso(1) standard(0) 14906 generic(1) version5(5)};


-- Definitions of the RTM functions:
RTM-InitialiseComm-Request ::= BST
RTM-InitialiseComm-Response::= VST
RTM-DataRetrieval-Request::= Get-Request (WITH COMPONENTS {fill (SIZE(1)), eid, accessCredentials ABSENT,iid
ABSENT,  attrIdList})
RTM-DataRetrieval-Response::= Get-Response {RtmContainer} (WITH COMPONENTS {..., eid, iid ABSENT})
RTM-TerminateComm::= Event-Report-Request {RtmContainer}(WITH COMPONENTS {mode (FALSE), eid (0),
eventType (0)})

RTM-TestComm-Request::= Action-Request {RtmContainer} (WITH COMPONENTS {..., eid (0), actionType
(15), accessCredentials ABSENT, iid ABSENT})

RTM-TestComm-Response::= Action-Response {RtmContainer} (WITH COMPONENTS {..., fill (SIZE(1)), eid
(0), iid ABSENT})

-- Definitions of the RTM attributes:
RtmData ::= SEQUENCE {
      encryptedTachographPayload OCTET STRING (SIZE(67)) (CONSTRAINED BY { -- calculated encrypting
TachographPayload as per Appendix 11 --}),
      DSRCSecurityData OCTET STRING
      }
TachographPayload ::= SEQUENCE {
            tp15638VehicleRegistrationPlate LPN -- Vehicle Registration Plate as per EN 15509.
            tp15638SpeedingEvent            BOOLEAN,  -- 1= Irregularities in speed (see Annex 1C)
            tp15638DrivingWithoutValidCard  BOOLEAN,     -- 1= Invalid card usage (see Annex 1C)
            tp15638DriverCard               BOOLEAN,-- 0= Indicates a valid driver card  (see Annex 1C)
            tp15638CardInsertion            BOOLEAN, -- 1= Card insertion while driving (see Annex 1C)
            tp15638MotionDataError          BOOLEAN, -- 1= Motion data error (see Annex 1C)
            tp15638VehicleMotionConflict    BOOLEAN, -- 1= Motion conflict (see Annex 1C)
            tp156382ndDriverCard            BOOLEAN, -- 1= Second driver card inserted (see Annex 1C)
            tp15638CurrentActivityDriving   BOOLEAN, -- 1= other activity selected;
                                                      -- 0= driving selected
            tp15638LastSessionClosed        BOOLEAN, -- 1= improperly, 0= properly, closed
            tp15638PowerSupplyInterruption  INTEGER (0..127), -- Supply interrupts in the last 10 days
            tp15638SensorFault              INTEGER (0..255),-- eventFaultType as per data dictionary
-- All subsequent time related types as defined in Annex 1C.
            tp15638TimeAdjustment           INTEGER(0..4294967295), -- Time of the last time adjustment
            tp15638LatestBreachAttempt      INTEGER(0..4294967295), -- Time of last breach attempt
            tp15638LastCalibrationData      INTEGER(0..4294967295), -- Time of last calibration data
            tp15638PrevCalibrationData      INTEGER(0..4294967295), -- Time of previous calibration data
            tp15638DateTachoConnected       INTEGER(0..4294967295), -- Date tachograph connected
            tp15638CurrentSpeed             INTEGER (0..255), -- Last current recorded speed
            tp15638Timestamp                INTEGER(0..4294967295) -- Timestamp of current record[2]
            }
Rtm-ContextMark ::= SEQUENCE {
  standardIdentifier    StandardIdentifier, -- identifier of the TARV part and its version

  RtmCommProfile          INTEGER {
                                C1 (1),
                                C2 (2)
                                } (0..255) DEFAULT 1
  }
RtmTransferAck ::= INTEGER {
                Ok (1),
                NoK (2)
                } SIZE (1..255)
```

▼B

```
StandardIdentifier ::= OBJECT IDENTIFIER
RtmContainer ::= CHOICE {
        integer                     [0]    INTEGER,
        bitstring                   [1]    BIT STRING,
        octetstring                 [2]    OCTET STRING (SIZE (0..127, ...)),
        universalString             [3]    UniversalString,
        beaconId                    [4]    BeaconID,
        t-apdu                      [5]    T-APDUs,
        dsrcApplicationEntityId     [6]    DSRCApplicationEntityID,
        dsrc-Ase-Id                 [7]    Dsrc-EID,
        attrIdList                  [8]    AttributeIdList,
        attrList                    [9]    AttributeList{RtmContainer},
        rtmData                     [10]   RtmData,
        rtmContextmark              [11]   Rtm-ContextMark,
        reserved12                  [12]   NULL,
        reserved13                  [13]   NULL,
        reserved14                  [14]   NULL,
        time                        [15]   Time,
-- values from 16 to 255 reserved for ISO/CEN usage
        }}

END
```

5.4.5 *Element i RtmData, operationer som utförs samt definitioner*

DSC_41 De datavärden som beräknas av fordonsenheten och sedan används för att uppdatera skyddade data i fordonsenhetens DSRC-modul ska beräknas enligt de regler som definieras i tabell 14.3.

Tabell 14.3

Element i RtmData, operationer som utförs samt definitioner

(1) RTM-data-element	(2) Operation som utförs av fordonsenheten		(3) ASN.1-definition av data
RTM1 **Fordonets registreringsskylt (*Vehicle Registration Plate*)**	Fordonsenheten ska sätta värdet för *tp15638VehicleRegistrationPlate* (dataelementet RTM1) till det värde som registrerats för datatypen *VehicleRegistrationIdentification* såsom den definieras i tillägg 1 om *VehicleRegistrationIdentification*.	Vehicle Registration Plate uttryckt som en teckensträng.	`tp15638VehicleRegstrationPlate LPN, --fordonets registeringsnummer (Vehicle Registration Plate) med format enligt ISO 14906, med den begränsning som specificeras i EN 15509, nämligen en SEQUENCE som omfattar landskod, följd av en alfabets-indikator, följd av skyltens nummer i sig, vilket alltid är 14 oktetter (utfyllda med nollor) så att längden av LPN enligt EN 15509 alltid är 17 oktetter, varav 14 motsvarar den egentliga registreringsskyltens nummer.`
RTM2 **Hastighetsöverträdelse (*Speeding Event*)**	Fordonsenheten ska generera ett booleskt värde för dataelement RTM2, tp15638SpeedingEvent. Värdet för tp15638SpeedingEvent ska beräknas av fordonsenheten utifrån antalet hastighetsöverträdelser som registrerats i fordonsenheten bland de senaste tio dagarnas händelser, enligt definition i bilaga 1C.	1 (TRUE): Anger oegentligheter i fråga om hastighet bland de senaste tio dagarnas händelser.	`tp15638speedingEvent BOOLEAN,`

▼B

(1) RTM-data-element	(2) Operation som utförs av fordonsenheten		(3) ASN.1-definition av data
	Om det finns minst en tp15638SpeedingEvent bland de senaste tio dagarnas händelser ska värdet för tp15638SpeedingEvent sättas till TRUE. I annat fall (”ELSE”): Om det inte finns någon sådan händelse bland de senaste tio dagarnas händelser ska tp15638SpeedingEvent sättas till FALSE.		
RTM3 **Körning utan giltigt kort (*Driving Without Valid Card*)**	Fordonsenheten ska generera ett booleskt värde för dataelement RTM3, tp15638DrivingWithoutValidCard. Fordonsenheten ska tilldela variabeln tp15638DrivingWithoutValidCard värdet TRUE om det i fordonsenhetens data finns registrerad minst en händelse av typen *Driving Without Valid Card* bland de senaste tio dagarnas händelser, enligt definition i bilaga 1C. I annat fall (”ELSE”): Om det inte finns någon sådan händelse bland de senaste tio dagarnas händelser ska variabeln tp15638DrivingWithoutValidCard sättas till FALSE.	1 (TRUE): Anger användning av ogiltigt kort.	`tp15638DrivingWithoutValidCard` `BOOLEAN,`
RTM4 **Giltigt förarkort (*Valid Driver Card*)**	Fordonsenheten ska generera ett booleskt värde för dataelement RTM4, tp15638DriverCard, baserat på de data som är lagrade i fordonsenheten och definierade i tillägg 1. Om inget giltigt förarkort finns ska fordonsenheten sätta variabeln till TRUE. I annat fall (”ELSE”): Om det inte finns något giltigt förarkort ska fordonsenheten sätta variabeln till FALSE.	0 (FALSE): Anger ett giltigt förarkort:	`tp15638DriverCard` `BOOLEAN,`
RTM5 **Insättning av kort under körning (*Card Insertion while Driving*)**	Fordonsenheten ska generera ett booleskt värde för dataelement RTM5. Fordonsenheten ska tilldela variabeln tp15638CardInsertion värdet TRUE om det i fordonsenhetens data finns registrerad minst en händelse av typen *Card Insertion while Driving* bland de senaste tio dagarnas händelser, enligt definition i bilaga 1C. I annat fall (”ELSE”): Om det inte finns någon sådan händelse bland de senaste tio dagarnas händelser ska variabeln tp15638CardInsertion sättas till FALSE.	1 (TRUE): Anger insättning av kort under körning bland de senaste tio dagarnas händelser.	`tp15638CardInsertion` `BOOLEAN,`
RTM6 **Fel i rörelsedata (*Motion Data Error*)**	Fordonsenheten ska generera ett booleskt värde för dataelement RTM6. Fordonsenheten ska tilldela variabeln tp15638MotionDataError värdet TRUE om det i fordonsenhetens data finns registrerad minst en händelse av typen *Motion Data Error* bland de senaste tio dagarnas händelser, enligt definition i bilaga 1C. I annat fall (”ELSE”): Om det inte finns någon sådan händelse bland de senaste tio dagarnas händelser ska variabeln tp15638MotionDataError sättas till FALSE.	1 (TRUE): Anger fel i rörelsedata bland de senaste tio dagarnas händelser.	`tp15638motionDataError` `BOOLEAN,`

▼B

(1) RTM-data-element	(2) Operation som utförs av fordonsenheten		(3) ASN.1-definition av data
RTM7 **Konflikt i fordonets rörelsedata (*Vehicle Motion Conflict*)**	Fordonsenheten ska generera ett booleskt värde för dataelement RTM7. Fordonsenheten ska tilldela variabeln tp15638vehicleMotionConflict värdet TRUE om det i fordonsenhetens data finns registrerad minst en händelse av typen *Vehicle Motion Conflict* bland de senaste tio dagarnas händelser (värde: '0A'H). I annat fall ("ELSE"): Om det inte finns någon sådan händelse bland de senaste tio dagarnas händelser ska variabeln tp15638vehicleMotionConflict sättas till FALSE.	1 (TRUE): Anger konflikt bland de senaste tio dagarnas händelser.	`tp15638vehicleMotionConflict` `BOOLEAN,`
RTM8 **Två förarkort (*2nd Driver Card*)**	Fordonsenheten ska generera ett booleskt värde för dataelement RTM8, baserat på föraraktivitetsdata (*Driver Activity Data*) i form av flera förare (CREW) och medförare (CO-DRIVER) – se bilaga 1C. Om två förarkort finns ska fordonsenheten sätta variabeln till TRUE. I annat fall ("ELSE"): Om det inte finns två förarkort ska fordonsenheten sätta variabeln till FALSE.	1 (TRUE): Anger att två förarkort är insatta.	`tp156382ndDriverCard BOOLEAN,`
RTM9 **Innevarande aktivitet (*Current Activity*)**	Fordonsenheten ska generera ett booleskt värde för dataelement RTM9. Om den innevarande aktiviteten inte registreras i fordonsenheten som körning (DRIVING) enligt definition i bilaga 1C ska fordonsenheten sätta variabeln till TRUE. I annat fall ("ELSE"): Om den innevarande aktiviteten registreras i fordonsenheten som körning (DRIVING) ska fordonsenheten sätta variabeln till FALSE.	1 (TRUE): Annan aktivitet vald. 0 (FALSE): Körning är vald som aktivitet.	`tp15638currentActivityDriving` `BOOLEAN`
RTM10 **Senaste avslutade session (*Last Session Closed*)**	Fordonsenheten ska generera ett booleskt värde för dataelement RTM10. Om den senaste kortsessionen inte avslutades på korrekt sätt enligt definition i bilaga Annex 1C ska fordonsenheten sätta variabeln till TRUE. I annat fall ("ELSE"): Om den senaste kortsessionen avslutades på korrekt sätt ska fordonsenheten sätta variabeln till FALSE.	1 (TRUE): Ej korrekt avslutning. 0 (FALSE): Korrekt avslutning.	`tp15638lastSessionClosed` `BOOLEAN`
RTM11 **Avbrott i strömtillförseln (*Power Supply Interruption*)**	Fordonsenheten ska generera ett heltals-värde för dataelement RTM11. Fordonsenheten ska tilldela variabeln tp15638PowerSupplyInterruption ett värde som är lika med det längsta avbrottet i strömtillförseln i enlighet med artikel 9 i förordning (EU) nr 165/2014 som registrerats som en händelse av typen *Power Supply Interruption* enligt definition i bilaga 1C.	— Antal avbrott av strömtillförseln bland de senaste tio dagarnas händelser.	`tp15638powerSupplyInterruption` `INTEGER (0..127),`

▼B

(1) RTM-data-element	(2) Operation som utförs av fordonsenheten		(3) ASN.1-definition av data
	I annat fall (”ELSE”): Om det inte finns någon sådan händelse av typen *Power Supply Interruption* bland de senaste tio dagarnas händelser ska heltalsvärdet sättas till 0.		
RTM12 **Sensorfel (*Sensor Fault*)**	Fordonsenheten ska generera ett heltalsvärde för dataelement RTM12. Fordonsenheten ska tilldela variabeln sensorFault något av följande värden: — 1 Om en händelse av typen sensorfel (‘35’H *Sensor fault*) har registrerats under de senaste tio dagarna. — 2 Om en händelse av typen fel i GNSS-mottagare (*GNSS receiver fault*, antingen intern eller extern med värdet ‘51’H respektive ‘52’H) har registrerats under de senaste tio dagarna. — 3 Om en händelse av typen externt fel i GNSS-kommunikation (‘53’H *External GNSS communication fault*) har registrerats bland de senaste tio dagarnas händelser. — 4 Om både sensorfel (*Sensor Fault*) och fel i GNSS-mottagare (*GNSS receiver fault*) har registrerats bland de senaste tio dagarnas händelser. — 5 Om både sensorfel (*Sensor Fault*) och externt fel i GNSS-kommunikation (*External GNSS communication fault*) har registrerats bland de senaste tio dagarnas händelser. — 6 Om både fel i GNSS-mottagare (*GNSS receiver fault*) och externt fel i GNSS-kommunikation (*External GNSS communication fault*) har registrerats bland de senaste tio dagarnas händelser. — 7 Om samtliga tre sensorfel har registrerats bland de senaste tio dagarnas händelser. I annat fall (”ELSE”): Värdet ska sättas till 0 om inga händelser har registrerats bland de senaste tio dagarnas händelser.	— En oktett för sensorfel i enlighet med datakatalog.	`tp15638SensorFault INTEGER (0..255),`
RTM13 **Tidsinställning (*Time Adjustment*)**	Fordonsenheten ska generera ett heltalsvärde (timeReal från tillägg 1) för dataelement RTM13, baserat på befintliga data om tidsinställning enligt definition i bilaga 1C. Fordonsenheten ska tilldela tidsvärdet för den senaste händelsen av typen tidsinställning (*Time Adjustment*). I annat fall (”ELSE”): Om ingen händelse av typen *Time Adjustment* enligt definition i bilaga 1C finns ska fordonsenheten sätta värdet 0.	Tidpunkt för senaste tidsinställning	`tp15638TimeAdjustment INTEGER(0..4294967295),`
RTM14 **Försök till säkerhetsöverträdelse (*Security Breach Attempt*)**	Fordonsenheten ska generera ett heltalsvärde (timeReal från tillägg 1) för dataelement RTM14, baserat på befintliga data om händelser av typen *Security Breach Attempt* enligt definition i bilaga 1C. Fordonsenheten ska sätta ett värde som är lika med tidpunkten för den senaste händelsen av typen *Security Breach Attempt* som registrerats av fordonsenheten.	Tidpunkt för senaste försök till säkerhetsöverträdelse — Standardvärde: 0x00FF	`tp15638LatestBreachAttempt INTEGER(0..4294967295),`

▼B

(1) RTM-data-element	(2) Operation som utförs av fordonsenheten		(3) ASN.1-definition av data
	I annat fall (”ELSE”): Om ingen händelse av typen *Security Breach Attempt* enligt definition i bilaga 1C finns ska fordonsenheten sätta värdet 0x00FF.		
RTM15 **Senaste kalibrering (*Last Calibration*)**	Fordonsenheten ska generera ett heltalsvärde (timeReal från tillägg 1) för dataelement RTM15, baserat på befintliga data om senaste kalibrering enligt definition i bilaga 1C. Fordonsenheten ska sätta ett värde som är lika med tidpunkten för de senaste två kalibreringarna (RTM15 respektive RTM16), vilka bestäms genom VuCalibrationData enligt definition i tillägg 1. Fordonsenheten ska sätta värdet för RTM15 till timeReal för senaste kalibreringspost.	Tidpunkt för senaste kalibreringsdata	`tp15638LastCalibrationData` `INTEGER(0..4294967295),`
RTM16 **Föregående kalibrering (*Previous Calibration*)**	Fordonsenheten ska generera ett heltalsvärde (timeReal från tillägg 1) för dataelement RTM16, baserat på den kalibreringspost som föregår posten för den senaste kalibreringen. I annat fall (”ELSE”): Om det inte finns någon föregående kalibrering ska fordonsenheten sätta värdet för RTM16 till 0.	Tidpunkt för föregående kalibrerings-data	`tp15638PrevCalibrationData` `INTEGER(0..4294967295),`
RTM17 **Anslutningsdatum för färdskrivare (*Date Tachograph Connected*)**	För dataelement RTM17 ska fordonsenheten generera ett heltalsvärde (timeReal från tillägg 1). Fordonsenheten ska sätta ett värde som är lika med tidpunkten för första installation av fordonsenheten. Fordonsenheten ska hämta dessa fata från VuCalibrationData (tillägg 1) i vuCalibrationRecords där CalibrationPurpose är lika med ‘03’H	Anslutningsdatum för färdskrivare	`tp15638DateTachoConnected` `INTEGER(0..4294967295),`
RTM18 **Nuvarande hastighet (*Current Speed*)**	Fordonsenheten ska generera ett heltals-värde för dataelement RTM18. Fordonsenheten ska sätta värdet för RTM16 till den senast registrerade hastigheten vid tidpunkten för senaste uppdatering av RtmData.	Senast registrerade nuvarande hastighet	`tp15638CurrentSpeed` `INTEGER (0..255),`
RTM19 **Tidsstämpel (*Timestamp*)**	För dataelement RTM19 ska fordonsenheten generera ett heltalsvärde (timeReal från tillägg 1). Fordonsenheten ska sätta värdet för RTM19 till tidpunkten för senaste uppdatering av RtmData.	Tidsstämpel för nuvarande post med datatyp TachographPayload	`tp15638Timestamp` `INTEGER(0..4294967295),`

5.4.6 *Mekanism för dataöverföring*

DSC_42 Nyttolastdata som tidigare definierats begärs av fjärravläsaren efter initieringsfasen, och sänds därmed från fordonsenhetens DSRC-modul i det tilldelade fönstret. Kommandot GET används av fjärravläsaren för att hämta data.

▼B

DSC_43 Data ska kodas med hjälp av PER (*Packed Encoding Rules*) för alla utväxlingar via DSRC.

5.4.7 *Detaljbeskrivning av DSRC-transaktion*

DSC_44 Initieringen utförs i enlighet med DSC_44–DSC_48) och tabellerna 14.4–14.9. I initieringsfasen inleder fjärravläsaren med att sända en ram som innehåller en BST (*Beacon Service Table*) i enlighet med EN 12834 och EN 13372, avsnitt 6.2, 6.3, 6,4 och 7.1, med de inställningar som anges i följande tabell 14.4.

Tabell 14.4

Initiering – raminställningar för BST

Fält	Inställningar
Länkidentifierare	Utsänd adress (*broadcast address*)
BeaconId	Enligt EN 12834
Tidpunkt	Enligt EN 12834
Profil	Ingen utökning, 0 eller 1 ska användas
MandApplications	Ingen utökning, EID finns inte, parameter finns inte, AID = 2 Freight&Fleet
NonMandApplications	Finns inte
ProfileList	Ingen utökning, antal profiler i lista = 0
Indikator för fragmentering (*fragmentation header*)	Ingen fragmentering
Inställningar för skikt 2 (layer 2 settings)	Kommando-PDU, UI-kommando (Command PDU, UI command)

Ett praktiskt exempel på de inställningar som anges i tabell 14.4, med bitkodning, finns i följande tabell 14.5.

Tabell 14.5

Initiering – exempel på innehåll i BST-ram

Oktett #	Attribut/fält	Bitar i oktett	Beskrivning
1	Flagga (FLAG)	0111 1110	Startflagga (start flag)
2	Utsänd identifierare (broadcast ID)	1111 1111	Utsänd adress (broadcast address)
3	Kontrollfält för MAC (MAC Control Field)	1010 0000	Kommando-PDU (Command PDU)
4	Kontrollfält för LLC (LLC Control field)	0000 0011	UI-kommando (UI command)

▼B

Oktett #	Attribut/fält	Bitar i oktett	Beskrivning
5	Indikator för fragmentering (fragmentation header)	1xxx x001	Ingen fragmentering
6	BST	1000	Initieringsbegäran (initialisation request)
	SEQUENCE {		
	OPTION indicator BeaconID SEQUENCE { ManufacturerId INTEGER (0..65535)	0	Ej obligatoriska tillämpningar (*NonMand applications*) finns inte
		xxx	Identifierare för tillverkare (*Manufacturer Identifier*)
7		xxxx xxxx	
8		xxxx x	
	IndividualID INTEGER (0..134217727)	xxx	27 bitars identifierare, tillgänglig för tillverkare
9		xxxx xxxx	
10		xxxx xxxx	
11	}	xxxx xxxx	
12	Time INTEGER (0..4294967295)	xxxx xxxx	32 bitars UNIX realtid
13		xxxx xxxx	
14		xxxx xxxx	
15		xxxx xxxx	
16	Profile INTEGER (0..127,…)	0000 0000	Ingen utökning. Exempelprofil 0
17	MandApplications SEQUENCE (SIZE(0..127,…)) OF {	0000 0001	Ingen utökning, antal obligatoriska tillämpningar (*mandApplications*) = 1
18	SEQUENCE {		
	OPTION indicator	0	EID finns inte
	OPTION indicator	0	Parameter finns inte
	AID DSRCApplicationEntityID } }	00 0010	Ingen utökning. AID = 2 (Freight&Fleet)

▼B

Oktett #	Attribut/fält	Bitar i oktett	Beskrivning
19	ProfileList SEQUENCE (0..127,…) OF Profile }	0000 0000	Ingen utökning, antal profiler i lista = 0
20	FCS	xxxx xxxx	Ramkontrollsekvens (frame check sequence)
21		xxxx xxxx	
22	Flagga (flag)	0111 1110	Slutflagga (end flag)

DSC_45 En fordonsenhets DSRC-modul kräver vid mottagandet av en BST ett tilldelat privat fönster, såsom anges i EN 12795 och EN 13372, avsnitt 7.1.1, utan några särskilda RTM-inställningar. I tabell 14.6 finns ett exempel på bitkodning.

Tabell 14.6

Initiering – innehåll i ram för begäran om tilldelning av privat fönster

Oktett #	Attribut/fält	Bitar i oktett	Beskrivning
1	Flagga (FLAG)	0111 1110	Startflagga (start flag)
2	Privat LID	xxxx xxxx	Länkadress för den specifika fordonsenhetens DSRC-modul
3		xxxx xxxx	
4		xxxx xxxx	
5		xxxx xxxx	
6	Kontrollfält för MAC (*MAC control field*)	0110 0000	Begäran om privat fönster (*private window request*)
7	FCS	xxxx xxxx	Ramkontrollsekvens (*frame check sequence*)
8		xxxx xxxx	
9	Flagga (flag)	0111 1110	Slutflagga (end flag)

DSC_46 Fjärravläsaren svarar sedan genom att tilldela ett privat fönster, såsom anges i EN 12795 och EN 13372, avsnitt 7.1.1, utan några särskilda RTM-inställningar.

I tabell 14.7 finns ett exempel på bitkodning.

Tabell 14.7

Initiering – innehåll i ram för tilldelning av privat fönster

Oktett #	Attribut/fält	Bitar i oktett	Beskrivning
1	Flagga (FLAG)	0111 1110	Startflagga (start flag)
2	Privat LID	xxxx xxxx	Länkadress för den specifika fordonsenhetens DSRC-modul
3		xxxx xxxx	

▼B

Oktett #	Attribut/fält	Bitar i oktett	Beskrivning
4		xxxx xxxx	
5		xxxx xxxx	
6	Kontrollfält för MAC (MAC control field)	0010 s000	Tilldelning av privat fönster (private window allocation)
7	FCS	xxxx xxxx	Ramkontrollsekvens (frame check sequence)
8		xxxx xxxx	
9	Flagga (flag)	0111 1110	Slutflagga (end flag)

DSC_47 Efter att ha tagit emot det tilldelade privata fönstret sänder fordonsenhetens DSRC-modul sin VST (*Vehicle Service Table*) såsom definieras i EN 12834 och EN 13372, avsnitt 6.2, 6.3, 6.4 och 7.1, med de inställningar som anges i tabell 14.8, med hjälp av det tilldelade överföringsfönstret.

Tabell 14.8

Initiering – raminställningar för VST

Fält	Inställningar
Privat LID	Enligt EN 12834
VST-parametrar	Fyllning (fill) = 0, därefter för varje tillämpning som stöds: EID finns, parameter finns, AID = 2, EID som genererats av OBU (fordonsenhetens DSRC-modul)
Parameter	Ingen utökning, innehåller markering för *RTM Context*
ObeConfiguration	Det frivilliga fältet ObeStatus kan finnas, men ska inte användas av fjärravläsaren.
Indikator för fragmentering (*fragmentation header*)	Ingen fragmentering
Inställningar för skikt 2 (layer 2 settings)	Kommando-PDU, UI-kommando (Command PDU, UI command)

DSC_48 Fordonsenhetens DSRC-modul ska stödja tillämpningen *Freight&Fleet*, som identifieras genom tillämpningsidentifierare (AID) ”2”. Det får finnas stöd för andra tillämpningsidentifierare, men dessa ska inte förekomma i denna VST eftersom BST endast kräver AID = 2. Fältet *Applications* innehåller en lista med tillämpningsinstanser som stöds i fordonsenhetens DSRC-modul. För varje tillämpningsinstans som stöds anges en referens till lämplig standard i form av en markering för Rtm Context som är uppbyggd av en OBJECT IDENTIFIER som står för den berörda standarden, dess del av standarden (9 för RTM) och eventuellt dess version samt en EID som genereras av fordonsenhetens DSRC-modul och som är kopplad till denna tillämpningsinstans.

Ett praktiskt exempel på de inställningar som anges i tabell 14.8, med bitkodning, finns i tabell 14.9.

▼B

Tabell 14.9

Initiering – exempel på innehåll i VST-ram

Oktett #	Attribut/fält	Bitar i oktett	Beskrivning
1	Flagga (FLAG)	0111 1110	Startflagga (start flag)
2	Privat LID	xxxx xxxx	Länkadress för den specifika fordonsenhetens DSRC-modul
3		xxxx xxxx	
4		xxxx xxxx	
5		xxxx xxxx	
6	Kontrollfält för MAC (MAC control field)	1100 0000	Kommando-PDU (Command PDU)
7	Kontrollfält för LLC (LLC Control field)	0000 0011	UI-kommando (UI command)
8	Indikator för fragmentering (fragmentation header)	1xxx x001	Ingen fragmentering
9	VST SEQUENCE {	1001	Initieringssvar
	Fyllning (*fill*) BIT STRING (SIZE(4))	0000	Används ej, sätts till 0
10	Profile INTEGER (0..127,...) Applications SEQUENCE OF {	0000 0000	Ingen utökning. Exempelprofil 0
11		0000 0001	Ingen utökning, 1 tillämpning
12	SEQUENCE {		
	OPTION indicator	1	EID finns
	OPTION indicator	1	Parameter finns
	AID DSRCApplicationEntityID	00 0010	Ingen utökning. AID = 2 (Freight&Fleet)
13	EID Dsrc-EID	xxxx xxxx	Definierad inom OBU (fordonsenhetens DSRC-modul), identifierar tillämpningsinstansen.
14	Parameter Container {	0000 0010	Ingen utökning, vald container = 02, oktettsträng
15		0000 1000	Ingen utökning, längd för markering för Rtm Context = 8

▼B

Oktett #	Attribut/fält	Bitar i oktett	Beskrivning
16	Rtm-ContextMark::= SEQUENCE { StandardIdentifier standardIdentifier	0000 0110	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. Notera att endast ett element i sekvensen visas (det frivilliga elementet RtmCommProfile är utelämnat).
17		0000 0110	
18		0010 1000	
19		1000 0000	
20		1111 1010	
21		0001 0110	
22		0000 1001	
23		0000 0001	
24	ObeConfiguration Sequence {		
	OPTION indicator	0	ObeStatus finns inte
	EquipmentClass INTEGER (0..32767)	xxx xxxx	
25		xxxx xxxx	
26	ManufacturerId INTEGER (0..65535)	xxxx xxxx	Identifierare för tillverkaren av fordonsenhetens DSRC-modul enligt beskrivning i register i ISO 14816.
27		xxxx xxxx	
28	FCS	xxxx xxxx	Ramkontrollsekvens (frame check sequence)
29		xxxx xxxx	
30	Flagga (flag)	0111 1110	Slutflagga (end flag)

DCS_49 Fjärravläsaren läser sedan dessa data genom att sända kommandot GET, i överensstämmelse med det GET-kommando som definieras i EN 13372, avsnitt 6.2, 6.3 och 6.4, och i EN 12834, och med de inställningar som anges i tabell 14.10.

Tabell 14.10

Överlämning – raminställningar för GET.request (begäran)

Fält	Inställningar
Anroparens identifierare (IID, Invoker Identifier)	Finns inte
Länkidentifierare (LID, Link Identifier)	Länkadress för den specifika fordonsenhetens DSRC-modul
Sammankedjning (chaining)	Nej
Elementidentifierare (EID, Element Identifier)	Enligt specifikation i VST. Ingen utökning.

▼B

Fält	Inställningar
Åtkomstuppgifter (access credentials)	Nej
AttributeIdList	Ingen utökning, 1 attribut, AttributeID = 1 (RtmData)
Fragmentering	Nej
Inställningar för skikt 2 (*layer 2 settings*)	Kommando-PDU, insamlat ACn-kommando (*Command PDU, Polled ACn command*)

I tabell 14.11 visas ett exempel på avläsning av RTM-data.

Tabell 14.11

Överlämning – exempel på ram för GET.request (begäran)

Oktett #	Attribut/fält	Bitar i oktett	Beskrivning
1	Flagga (FLAG)	0111 1110	Startflagga (start flag)
2	Privat LID	xxxx xxxx	Länkadress för den specifika fordonsenhetens DSRC-modul
3		xxxx xxxx	
4		xxxx xxxx	
5		xxxx xxxx	
6	Kontrollfält för MAC (MAC control field)	1010 s000	Kommando-PDU (Command PDU)
7	Kontrollfält för LLC (*LLC Control field*)	n111 0111	Insamlat ACn-kommando (*polled ACn command*), n bitar
8	Indikator för fragmentering (*fragmentation header*)	1xxx x001	Ingen fragmentering
9	Get.request SEQUENCE {	0110	Begäran om GET
	OPTION indicator	0	Åtkomstuppgifter saknas
	OPTION indicator	0	IID saknas
	OPTION indicator	1	AttributeIdList finns
	Fill BIT STRING(SIZE(1))	0	Satt till 0.
10	EID INTEGER (0..127)	xxxx xxxx	EID för instansen av RTM-tillämpningen, enligt specifikation i VST. Ingen utökning.
11	AttributeIdList SEQUENCE OF { AttributeId }}	0000 0001	Ingen utökning, antal attribut = 1
12		0000 0001	AttributeId=1, RtmData. Ingen utökning.
13	FCS	xxxx xxxx	Ramkontrollsekvens (frame check sequence)
14		xxxx xxxx	
15	Flagga (flag)	0111 1110	Slutflagga (end flag)

▼B

DSC_50 När fordonsenhetens DSRC-modul tar emot begäran om GET sänder den ett svar i form av GET samt de data som begärs, i överensstämmelse med det GET-svar som definieras i EN 13372, avsnitt 6.2, 6.3 och 6.4, och i EN 12834, och med de inställningar som anges i tabell 14.12.

Tabell 14.12

Överlämning – raminställningar för GET.response (svar)

Fält	Inställningar
Anroparens identifierare (IID, Invoker Identifier)	Finns inte
Länkidentifierare (LID, Link Identifier)	Enligt EN 12834
Sammankedjning (chaining)	Nej
Elementidentifierare (EID, Element Identifier)	Enligt specifikation i VST.
Åtkomstuppgifter (*access credentials*)	Nej
Fragmentering	Nej
Inställningar för skikt 2 (*layer 2 settings*)	PDU för svar, svar tillgängligt och kommando accepterat, ACn-kommando

I tabell 14.13 visas ett exempel på avläsning av RTM-data.

Tabell 14.13

Överlämning – exempel på raminnehåll (svar)

Oktett #	Attribut/fält	Bitar i oktett	Beskrivning
1	Flagga (FLAG)	0111 1110	Startflagga (start flag)
2	Privat LID	xxxx xxxx	Länkadress för den specifika fordonsenhetens DSRC-modul
3		xxxx xxxx	
4		xxxx xxxx	
5		xxxx xxxx	
6	Kontrollfält för MAC (*MAC control field*)	1101 0000	PDU för svar
7	Kontrollfält för LLC (*LLC Control field*)	n111 0111	Svar tillgängligt, ACn-kommando (n bitar)
8	Statusfält för LLC (LLC status field)	0000 0000	Svar tillgängligt och kommando accepterat
9	Indikator för fragmentering (fragmentation header)	1xxx x001	Ingen fragmentering
10	Get.response SEQUENCE {	0111	Hämta svar

▼B

Oktett #	Attribut/fält	Bitar i oktett	Beskrivning
	OPTION indicator	0	IID saknas
	OPTION indicator	1	Attributlista finns
	OPTION indicator	0	Returstatus saknas
	Fill BIT STRING(SIZE(1))	0	Används inte
11	EID INTEGER(0..127,…)	xxxx xxxx	Svar från RTM-tillämpningens instans. Ingen utökning.
12	AttributeList SEQUENCE OF {	0000 0001	Ingen utökning, antal attribut = 1
13	Attributes SEQUENCE { AttributeId	0000 0001	Ingen utökning, AttributeID = 1 (RtmData)
14	AttributeValue CONTAINER {	0000 1010	Ingen utökning, val av container = 10_{10}.
15		kkkk kkkk	RtmData
16		kkkk kkkk	
17		kkkk kkkk	
…		…	
n	}}}}	kkkk kkkk	
n+1	FCS	xxxx xxxx	Ramkontrollsekvens (frame check sequence)
n+2		xxxx xxxx	
n+3	Flagga (flag)	0111 1110	Slutflagga (end flag)

DSC_51 Fjärravläsaren stänger sedan anslutningen genom att sända kommandot EVENT_REPORT, RELEASE, i överensstämmelse med EN 13372. avsnitt 6.2, 6.3 och 6.4, och med EN 12834, avsnitt 7.3.8, och utan några särskilda RTM-inställningar. I tabell 14.14 visas ett exempel på bitkodning av kommandot RELEASE.

Tabell 14.14

Avslutning – Raminnehåll för EVENT_REPORT RELEASE

Oktett #	Attribut/fält	Bitar i oktett	Beskrivning
1	Flagga (FLAG)	0111 1110	Startflagga (start flag)
2	Privat LID	xxxx xxxx	Länkadress för den specifika fordonsenhetens DSRC-modul
3		xxxx xxxx	
4		xxxx xxxx	

▼B

Oktett #	Attribut/fält	Bitar i oktett	Beskrivning
5		xxxx xxxx	
6	Kontrollfält för MAC (*MAC control field*)	1000 s000	Ramen innehåller en LPDU för kommando
7	Kontrollfält för LLC (*LLC Control field*)	0000 0011	UI-kommando (*UI command*)
8	Indikator för fragmentering (fragmentation header)	1xxx x001	Ingen fragmentering
9	EVENT_REPORT.request SEQUENCE {	0010	EVENT_REPORT (Release)
	OPTION indicator	0	Åtkomstuppgifter saknas
	OPTION indicator	0	Händelseparameter (event parameter) saknas
	OPTION indicator	0	IID saknas
	Mode BOOLEAN	0	Inget svar förväntas
10	EID INTEGER (0..127,…)	0000 0000	Ingen utökning, EID = 0 (System)
11	EventType INTEGER (0..127,…) }	0000 0000	Händelsetyp 0 = Release
12	FCS	xxxx xxxx	Ramkontrollsekvens (frame check sequence)
13		xxxx xxxx	
14	Flagga (flag)	0111 1110	Slutflagga (end flag)

DSC_52 Fordonsenhetens DSRC-modul förväntas inte svara på RELEASE-kommandot. Kommunikationen är därmed stängd.

5.4.8 *Beskrivning av provning med DSRC-transaktion*

DSC_53 Fullständig provning som inbegriper att skydda data ska utföras såsom definieras i tillägg 11 om gemensamma säkerhetsmekanismer av personer med tillstånd och tillgång till säkerhetsförfaranden, med hjälp av det normala GET-kommando som definieras ovan.

DSC_54 Provning vid driftsättning och periodisk besiktning som kräver dekryptering och förståelse för det dekrypterade datainnehållet ska utföras såsom anges i tillägg 11 om gemensamma säkerhetsmekanismer och i tillägg 9 om provning som krävs för typgodkännande.

Den grundläggande DSRC-kommunikationen kan dock provas med kommandot ECHO. Sådana prov kan vara nödvändiga vid driftsättning eller periodisk besiktning eller annars om så krävs av den behöriga kontrollmyndigheten eller i förordning (EU) nr 165/2014 (se avsnitt 6 nedan).

▼B

DSC_55 För att utföra detta grundläggande kommunikationsprov ger fjärravläsaren kommandot ECHO under en session, dvs. efter det att en initieringsfas fullbordats med gott resultat. Provsekvensen liknar därmed den som gäller i en riktig avläsning:

— Steg 1: *Fjärravläsaren* sänder en BST (*Beacon Service Table*) som inbegriper tillämpningsidentifierare (AID) för de tjänster som den stöder. För RTM-tillämpningar gäller endast tjänsten med AID = 2.

Fordonsenhetens DSRC-modul utvärderar mottagen BST och svarar om den hittar en begäran om *Freight&Fleet* (AID = 2) i BST. Om *fjärravläsaren* inte erbjuder AID=2 ska fordonsenhetens DSRC-modul avsluta transaktionen med *fjärravläsaren*.

— Steg 2: *Fordonsenhetens DSRC-modul* sänder en begäran om tilldelning av ett privat fönster.

— Steg 3: Fjärravläsaren sänder en tilldelning av ett privat fönster.

— Steg 4: *Fordonsenhetens DSRC-modul* använder det tilldelade privata fönstret för att sända sin VST (*Vehicle Service Table*). Denna VST inbegriper en lista med alla olika tillämpningsinstanser som *fordonsenhetens DSRC-modul* stöder inom ramen för AID = 2. De olika instanserna ska identifieras med hjälp av unikt genererade EID (*Element Identifier*), var och en med ett parametervärde som anger den instans av tillämpningen som stöds.

— Steg 5: *Fjärravläsaren* analyserar sedan erbjuden VST och antingen avslutar anslutningen (RELEASE) eftersom VST inte har något av intresse att erbjuda (dvs. mottagen VST kommer från en fordonsenhet vars DSRC-modul inte klarar RTM) eller startar en instans av tillämpningen (*app instantiation*) (om mottagen VST är lämplig för detta).

— Steg 6: *Fjärravläsaren* ska ge ett kommando (ECHO) till den specifika *fordonsenhetens DSRC-modul* och tilldelar ett privat fönster.

— Steg 7: Fordonsenhetens *DSRC-modul* använder det just tilldelade privata fönstret för att sända en ram med ECHO som svar.

Följande tabeller ger ett praktiskt exempel på en session med utväxling av ECHO-kommandon.

DSC_56 Initieringen utförs i enlighet med avsnitt 5.4.7 (DSC_44–DSC_48) och tabellerna 14.4–14.9.

DSC_57 Fjärravläsaren sänder sedan kommandot ACTION, ECHO, i överensstämmelse med ISO 14906 och innehållande 100 dataoktetter, men utan några särskilda RTM-inställningar. I tabell 14.15 visas innehållet i den ram som sänds från fjärravläsaren.

▼B

Tabell 14.15

Exempel på ram för ACTION, ECHO (begäran)

Oktett #	Attribut/fält	Bitar i oktett	Beskrivning
1	Flagga (FLAG)	0111 1110	Startflagga (start flag)
2	Privat LID	xxxx xxxx	Länkadress för den specifika fordonsenhetens DSRC-modul
3		xxxx xxxx	
4		xxxx xxxx	
5		xxxx xxxx	
6	Kontrollfält för MAC (*MAC control field*)	1010 s000	Kommando-PDU (*Command PDU*)
7	Kontrollfält för LLC (*LLC Control field*)	n111 0111	Insamlat ACn-kommando (*polled ACn command*), n bitar
8	Indikator för fragmentering (fragmentation header)	1xxx x001	Ingen fragmentering
9	ACTION.request SEQUENCE {	0000	Begäran om åtgärd (action) (ECHO)
	OPTION indicator	0	Åtkomstuppgifter saknas
	OPTION indicator	1	Åtgärdsparameter (action parameter) finns
	OPTION indicator	0	IID saknas
	Mode BOOLEAN	1	Svar förväntas
10	EID INTEGER (0..127,…)	0000 0000	Ingen utökning, EID = 0 (System)
11	ActionType INTEGER (0..127,…)	0000 1111	Ingen utökning, begäran om åtgärdstyp (action type) ECHO
12	ActionParameter CONTAINER {	0000 0010	Ingen utökning, vald container = 2,
13		0110 0100	Ingen utökning. Strånglängd = 100 oktetter
14		xxxx xxxx	Data som ska återges (echo)
…		…	
113	}}	xxxx xxxx	
114	FCS	xxxx xxxx	Ramkontrollsekvens (frame check sequence)
115		xxxx xxxx	
116	Flagga (flag)	0111 1110	Slutflagga (end flag)

▼B

DSC_58 När fordonsenhetens DSRC-modul tar emot begäran om ECHO sänder den ett ECHO-svar på 100 dataoktetter genom att återspegla det mottagna kommandot, i enlighet med ISO 14906 och utan några särskilda RTM-inställningar. I tabell 14.16 visas ett exempel på kodning på bitnivå.

Tabell 14.16

Exempel på ram för ACTION, ECHO (svar)

Oktett #	Attribut/fält	Bitar i oktett	Beskrivning
1	Flagga (FLAG)	0111 1110	Startflagga (start flag)
2	Privat LID	xxxx xxxx	Den specifika fordonsenhetens länkadress
3		xxxx xxxx	
4		xxxx xxxx	
5		xxxx xxxx	
6	Kontrollfält för MAC (*MAC control field*)	1101 0000	PDU för svar
7	Kontrollfält för LLC (*LLC Control field*)	n111 0111	ACn-kommando (n bitar)
8	Statusfält för LLC (LLC status field)	0000 0000	Svar tillgängligt
9	Indikator för fragmentering (fragmentation header)	1xxx x001	Ingen fragmentering
10	ACTION.response SEQUENCE {	0001	Svar på ACTION (ECHO)
	OPTION indicator	0	IID saknas
	OPTION indicator	1	Svarsparameter (response parameter) finns
	OPTION indicator	0	Returstatus saknas
	Fill BIT STRING (SIZE (1))	0	Används inte
11	EID INTEGER (0..127)	0000 0000	Ingen utökning, EID = 0 (System)
12	ResponseParameter CONTAINER {	0000 0010	Ingen utökning, vald container = 2
13		0110 0100	Ingen utökning. Stränglängd = 100 oktetter
14		xxxx xxxx	Återgivna data (echo)
…		…	
113	}}	xxxx xxxx	
114	FCS	xxxx xxxx	Ramkontrollsekvens (frame check sequence)
115		xxxx xxxx	
116	Flagga (flag)	0111 1110	Slutflagga (end flag)

▼B

5.5 **Stöd för direktiv (EU) 2015/719**

5.5.1 *Översikt*

DSC_59 Till stöd för direktiv (EU) 2015/719 om ändring av rådets direktiv 96/53/EG om största tillåtna dimensioner i nationell och internationell trafik och högsta tillåtna vikter i internationell trafik för vissa vägfordon som framförs inom gemenskapen kommer transaktionsprotokollet för överföring av OWS-data via 5,8 GHz DSRC att vara samma som det som används för RTM-data (se avsnitt 5.4.1), med den enda skillnaden att objektidentifieraren som anger TARV-standard kommer att peka på standarden ISO 15638, del 20, som handlar om vägning ombord och ombordbaserade vägningssystem (WOB/OWS).

5.5.2 *Kommandon*

DSC_60 De kommandon som används för en OWS-transaktion kommer att vara samma som de som används för en RTM-transaktion.

5.5.3 *Kommandosekvens vid avläsning*

DSC_61 Kommandosekvensen vid avläsning av OWS-data kommer att vara samma som för RTM-data.

5.5.4 *Datastrukturer*

DSC_62 Nyttolastdata (OWS-data) består av en konkatering av följande:

1. Data i form av EncryptedOwsPayload, som är krypterade från den nyttolast (OwsPayload) som finns definierad i ASN.1 i avsnitt 5.5.5. Krypteringsmetoden ska vara samma som den som används för RtmData och som anges i tillägg 11.

2. DSRCSecurityData, beräknade med samma algoritmer som används för RtmData och som anges i tillägg 11.

▼B

5.5.5 *ASN.1-modul för OWS-transaktion via DSRC*

DSC_63 ASN.1-modulen för DSRC-data inom RTM-tillämpningen definieras på följande sätt:

```
TarvOws {iso(1) standard(0) 15638 part20(20)
version1(1)} DEFINITIONS AUTOMATIC TAGS
::= BEGIN
IMPORTS
-- Imports data attributes and elements from EFC which are used for OWS
LPN
FROM EfcDsrcApplication {iso(1) standard(0) 14906 application(0) version5(5)}

-- Imports function parameters from the EFC Application Interface Definition
SetMMIRq
FROM EfcDsrcApplication {iso(1) standard(0) 14906 application(0) version5(5)}

-- Imports the L7 DSRCData module data from the EFC Application Interface Definition
Action-Request, Action-Response, ActionType, ApplicationList, AttributeIdList, AttributeList,
Attributes,
BeaconID, BST, Dsrc-EID, DSRCApplicationEntityID, Event-Report-Request, Event-Report- Response,
EventType, Get-Request, Get-Response, Initialisation-Request, Initialisation-Response,
ObeConfiguration, Profile, ReturnStatus, Time, T-APDUs, VST
FROM EfcDsrcGeneric {iso(1) standard(0) 14906 generic(1) version5(5)};

-- Definitions of the OWS functions:
OWS-InitialiseComm-Request ::= BST
OWS-InitialiseComm-Response::= VST
OWS-DataRetrieval-Request::= Get-Request (WITH COMPONENTS {fill (SIZE(1)), eid, accessCredentials
ABSENT, iid ABSENT, attrIdList})
OWS-DataRetrieval-Response::= Get-Response {OwsContainer} (WITH COMPONENTS {..., eid, iid ABSENT})
OWS-TerminateComm::= Event-Report-Request {OwsContainer}(WITH COMPONENTS {mode (FALSE), eid (0),
eventType (0)})
OWS-TestComm-Request::= Action-Request {OwsContainer} (WITH COMPONENTS {..., eid (0), actionType
(15), accessCredentials ABSENT, iid ABSENT})
OWS-TestComm-Response::= Action-Response {OwsContainer} (WITH COMPONENTS {..., fill (SIZE(1)), eid
(0), iid ABSENT})

-- Definitions of the OWS attributes:
OwsData :: = SEQUENCE {
     encryptedOwsPayload OCTET STRING (SIZE(51)) (CONSTRAINED BY { -- calculated encrypting
OwsPayload as per Appendix 11 --}),
     DSRCSecurityData OCTET STRING
     }
OwsPayload :: = SEQUENCE {
           tp15638VehicleRegistrationPlate LPN -- Vehicle Registration Plate as per EN 15509.
           recordedWeight INTEGER (0..65535),           -- 0= Total measured weight of the  heavy
goods vehicle                                                          -- with 10 Kg
resolution.
           axlesConfiguration OCTET STRING SIZE (3),     -- 0= 20 bits allowed for the number
                                                                  -- of axles for 10 axles.
           axlesRecordedWeight OCTET STRING SIZE (20),   -- 0= Recorded Weight for each axle
                                                                  -- with 10 Kg resolution.
           tp15638Timestamp              INTEGER(0..4294967295)      -- Timestamp of current record
     }

Ows-ContextMark ::= SEQUENCE {
 standardIdentifier    StandardIdentifier, -- identifier of the TARV part and its version
     }

StandardIdentifier ::= OBJECT IDENTIFIER
 OwsContainer ::= CHOICE {
     integer                    [0]    INTEGER,
     bitstring                  [1]    BIT STRING,
     octetstring                [2]    OCTET STRING (SIZE (0..127, ...)),
     universalString            [3]    UniversalString,
     beaconId                   [4]    BeaconID,
     t-apdu                     [5]    T-APDUs,
     dsrcApplicationEntityId    [6]    DSRCApplicationEntityID,
     dsrc-Ase-Id                [7]    Dsrc-EID,
     attrIdList                 [8]    AttributeIdList,
     attrList                   [9]    AttributeList{RtmContainer},
     reserved10                 [10]   NULL,
     OwsContextmark             [11]   Ows-ContextMark,
     OwsData                    [12]   OwsData,
     reserved13                 [13]   NULL,
     reserved14                 [14]   NULL,
     time                       [15]   Time,
-- values from 16 to 255 reserved for ISO/CEN usage
     }}

END
```

▼B

5.5.6 *Element i OwsData, operationer som utförs samt definitioner*

Elementen i OwsData är definierade som ett stöd för direktiv (EU) 2015/719 om ändring av rådets direktiv 96/53/EG om största tillåtna dimensioner i nationell och internationell trafik och högsta tillåtna vikter i internationell trafik för vissa vägfordon som framförs inom gemenskapen. Deras innebörd är följande:

— *recordedWeight* står för det tunga godsfordonets uppmätta totalvikt, med en upplösning på 10 kg såsom definieras i EN ISO 14906. Exempelvis står värdet 2500 för en vikt på 25 ton.

— *axlesConfiguration* står för det tunga godsfordonets konfiguration i form av antal axlar. Konfigurationen definieras med en 20-bitars bitmask (utökad från EN ISO 14906).

En bitmask på 2 bitar representerar axeln i konfigurationen enligt följande format:

— Värdet 00B betyder att värdet är ”ej tillgängligt” eftersom fordonet saknar utrustning för att samla in data om vikten som belastar axeln.

— Värdet 01B betyder att axeln inte finns på det aktuella fordonet.

— Värdet 10B betyder att axeln finns och att vikten har beräknats och samlats in och nu finns i fältet *axlesRecordedWeight*.

— Värdet 11B är reserverat för framtida användning.

De sista fyra bitarna är reserverade för framtida användning (RFU, *Reserved for Future Use*).

Antal axlar										
Antal axlar på dragfordon			Antal axlar på släpvagn							
00/01/10/11	00/01/10/11	00/01/10/11	00/01/10/11	00/01/10/11	00/01/10/11	00/01/10/11	00/01/10/11	00/01/10/11	00/01/10/11	RFU (4 bitar)

— *axlesRecordedWeight* står för den vikt som registrerats för respektive axel, med en upplösning på 10 kg. Två oktetter används för varje axel. Exempelvis står värdet 150 för en vikt på 1 500 kg.

Övriga datatyper definieras i avsnitt 5.4.5.

5.5.7 *Mekanismer för dataöverföring*

DSC_64 Mekanismen för överföring av OWS-data mellan fjärravläsaren och fordonets DSRC-modul ska vara samma som för RTM-data (se avsnitt 5.4.6).

DSC_65 Dataöverföringen mellan den plattform där högsta tillåtna vikter finns samlade och fordonets DSRC-modul ska baseras på den fysiska förbindelsen och de gränssnitt och det protokoll som definieras i avsnitt 5.6.

5.6 **Dataöverföring mellan fordonsenhetens DSRC-modul och fordonsenheten**

5.6.1 *Fysisk anslutning och gränssnitt*

DSC_66 Anslutningen mellan *fordonsenheten* och *fordonsenhetens DSRC-modul* kan utgöras av antingen en fysisk kabel eller trådlös kommunikation över korta avstånd baserad på Bluetooth v4.0 BLE.

▼B

DSC_67 Oavsett val av fysisk anslutning och gränssnitt ska följande krav vara uppfyllda:

DSC_68 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 fordonsenhetens DSRC-modul följa en öppen standard. Fordonsenheten ska anslutas till dess DSRC-modul via antingen

i) en fast kabel på minst 2 meter och en godkänd hankontakt av typen Straight DIN 41612 H11 Connector med 11 stift från DSRC-modulen som passar med en liknande DIN/ISO-godkänd honkontakt från fordonsenheten,

ii) *Bluetooth Low Energy* (BLE), eller

iii) en standardanslutning enligt ISO 11898 eller SAE J1939.

DSC_69 b) Definitionen av gränssnitt och anslutning mellan fordonsenheten och fordonsenhetens DSRC-modul måste stödja kommandona i det tillämpningsprotokoll som definieras i avsnitt 5.6.2.

DSC_70 c) Fordonsenheten och fordonsenhetens DSRC-modul måste ha kapacitet för dataöverföring via anslutningen i praktisk drift när det gäller prestanda och strömtillförsel.

5.6.2 *Tillämpningsprotokoll*

DSC_71 Tillämpningsprotokollet för kommunikationen mellan fordonsenhetens kommunikationsanordning för fjärravläsning och fordonsenhetens DSRC-modul ansvarar för periodisk överföring av data för fjärravläsning från fordonsenheten till dess DSRC-modul.

DSC_72 Följande huvudsakliga kommandon hanteras:

1. Initiering av kommunikationslänk – begäran

2. Initiering av kommunikationslänk – svar

3. Sänd data med identifierare för RTM-tillämpningen och nyttolast i form av RTM-data

4. Kvittering av data

5. Avslutning av kommunikationslänk – begäran

6. Avslutning av kommunikationslänk – svar

DSC_73 I ASN1.0 kan de ovanstående kommandona definieras på följande sätt:

▼B

```
Remote Communication DT Protocol DEFINITIONS ::= BEGIN

     RCDT-Communication Link Initialization - Request ::= SEQUENCE {
          LinkIdentifier INTEGER
     }

     RCDT-Communication Link Initialization - Response::= SEQUENCE {
          LinkIdentifier INTEGER,
          answer         BOOLEAN
     }

          RCDT- Send Data ::=
          SEQUENCE { LinkIdentifier
          INTEGER, DataTransactionId
          INTEGER, RCDTData
          SignedTachographPayload
     }

          RCDT Data Acknowledgment ::
          SEQUENCE { LinkIdentifier
          INTEGER, DataTransactionId
          INTEGER,
          answer         BOOLEAN
     }

          RCDT-Communication Link Termination - Request ::= SEQUENCE {
          LinkIdentifier INTEGER
     }

          RCDT-Communication Link Termination - Response::= SEQUENCE {
          LinkIdentifier INTEGER,
          answer         BOOLEAN
     }

End
```

DSC_74 Beskrivning av kommandon och parametrar:

— `RCDT-Communication Link Initialization – Request` används för att initiera kommunikationslänken. Kommandot sänds från fordonsenheten till dess DSRC-modul. LinkIdentifier sätts av fordonsenheten och kommuniceras till dess DSRC-modul så att en specifik kommunikationslänk kan spåras.

(*Anm.:* Detta är för att stödja framtida länkar och andra tillämpningar/moduler, t.ex. för vägning ombord.)

— `RCDT-Communication Link Initialization – Response` används av fordonsenhetens DSRC-modul för att ge svar på begäran om att initiera kommunikationslänken. Kommandot sänds från fordonsenhetens DSRC-modul till fordonsenheten. Kommandot ger resultatet av initieringen i form av svaret ”= 1” (initiering utförd) eller ”= 0” (initiering misslyckad).

DSC_75 Initiering av kommunikationslänken får ske endast efter installation och kalibrering och efter det att motorn har startats/fordonsenheten har satts på.

▼B

— RCDT-Send Data används av fordonsenheten för att sända signerade data för fjärrkommunikation (*RCDTData*) till fordonsenhetens DSRC-modul. Data sänds var 60:e sekund. Parametern DataTransactionId identifierar den specifika dataöverföringen. LinkIdentifier används också för att säkerställa att den tillämpliga länken är korrekt.

— RCDT-Data Acknowledgment sänds av fordonsenhetens DSRC-modul för att ge återkoppling till fordonsenheten om mottagandet av data via det kommando RCDT-Send Data som identifieras med parametern DataTransactionId. Parametern i svaret är 1 (OK) eller 0 (fel). Om fordonsenheten tar emot fler än tre svar som är lika med 0 eller om fordonsenheten inte tar emot någon kvittering (RCDT Data Acknowledgment) för ett visst, tidigare sänt kommando RCDT-Send Data med ett visst DataTransactionId kommer fordonsenheten att generera och registrera en händelse.

— RCDT-Communication Link Termination request sänds av fordonsenheten till fordonsenhetens DSRC-modul för att avsluta en länk med en viss LinkIdentifier.

DSC_76 Vid omstart av fordonsenhetens DSRC-modul eller fordonsenheten ska samtliga befintliga kommunikationslänkar tas bort, eftersom det annars kan finnas ”hängande” länkar orsakade av en plötslig nedstängning av fordonsenheten.

— RCDT-Communication Link Termination – Response sänds av fordonsenhetens DSRC-modul till fordonsenheten för att bekräfta mottagandet av fordonsenhetens begäran om att avsluta länken med just denna LinkIdentifier.

5.7 **Felhantering**

5.7.1 *Registrering och kommunikation av data i fordonsenhetens DSRC-modul*

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 som EventFaultType med värdet ‘62’H (kommunikationsfel i kommunikationsanordning för fjärravläsning) tillsammans med en tidsstämpel.

DSC_78 Fordonsenheten ska upprätthålla en fil med ett unikt namn som enkelt kan identifieras av besiktningstjänstemän, i syfte att registrera interna kommunikationsfel i fordonsenheten.

DSC_79 Om fordonsenhetens minne för nyttolastdata (VUPM) försöker hämta data från säkerhetsmodulen (för att lämna dessa vidare till fordonsenhetens DSRC-modul) men misslyckas med detta, ska den registrera felet som EventFaultType med värdet ‘62’H (kommunikationsfel i kommunikationsanordning

▼B

för fjärravläsning) tillsammans med en tidsstämpel. Kommunikationsfelet upptäcks när meddelandet `RCDT Data Acknowledgment` inte tas emot för motsvarande meddelande `RCDT Send Data` (dvs. där de två meddelandena har samma DataTransactionId) `DataTransactionId` vid mer än tre på varandra följande tillfällen.

5.7.2 *Fel i trådlös kommunikation*

DSC_80 Hantering av kommunikationsfel ska ske i enlighet med det som föreskrivs i relaterade DSRC-standarder, nämligen EN 300 674-1, EN 12253, EN 12795, EN 12834 och lämpliga parametrar från EN 13372.

5.7.2.1 *Krypterings- och signaturfel*

DSC_81 Krypterings- och signaturfel ska hanteras såsom definieras i tillägg 11 om gemensamma säkerhetsmekanismer och förekommer inte i några felmeddelanden som hänger ihop med DSRC-överföringen av data.

5.7.2.2 *Registrering av fel*

DSRC är ett dynamiskt trådlöst kommunikationsmedium i en miljö med okända atmosfärs- och interferensförhållanden, särskilt med den kombination av flyttbar fjärravläsare och bil i rörelse som är aktuell för den här tillämpningen. Det är därför nödvändigt att säkerställa skillnaden mellan en ”misslyckad avläsning” och ett ”fel”. För transaktioner via ett trådlöst gränssnitt är det vanligt med misslyckade avläsningar och konsekvensen är vanligen att försöka igen, dvs. att återsända BST och försöka samma sekvens igen, vilket under de flesta omständigheter leder till att anslutningen och dataöverföringen lyckas, såvida inte fordonet som ska kontrolleras har förflyttat sig utom räckhåll under den tid som krävs för återsändning. (En lyckad avläsning kan ha omfattat flera försök och omförsök.)

En misslyckad avläsning kan bero på att antennerna inte parades på rätt sätt (”siktningsfel”), att en av antennerna är skärmad (detta kan vara avsiktligt, men också orsakas av ett annat fordons fysiska närvaro). Det kan också bero på radiointerferens, särskilt från Wi-Fi på cirka 5,8 GHz eller annan allmänt tillgänglig trådlös kommunikation, radarinterferens eller svåra atmosfäriska förhållanden (t.ex. under ett åskväder), eller helt enkelt att fordonet rör sig utanför DSRC-kommunikationens räckvidd. Enstaka misslyckade avläsningar kan, till följd av sin natur, inte registreras, helt enkelt därför att kommunikationen inte upprättades.

Om de behöriga kontrollmyndigheternas representant riktar fjärravläsaren mot ett fordon och försöker avläsa dess fordonsenhets DSRC-modul utan att någon lyckad dataöverföring uppstår kan detta misslyckande dock bero på avsiktlig manipulering, och representanten behöver därför ett medel för att logga misslyckandet och förvarna kollegor längre fram om den eventuella överträdelsen. Kollegorna kan sedan stoppa fordonet och utföra en fysisk besiktning. Eftersom ingen lyckad kommunikation har ägt rum kan dock inte fordonsenhetens DSRC-modul ge några data om misslyckandet. Sådan rapportering ska därför ingå som en funktion i utformningen av fjärravläsarens utrustning.

”Misslyckad avläsning” är tekniskt sett något annat än ett ”fel”. I detta sammanhang är ett fel samma sak som mottagande av ett felaktigt värde.

▼B

Data som överförs till *fordonsenhetens DSRC-modul* är redan skyddade när de lämnas och måste därför kontrolleras av den som tillhandahållit dessa data (se avsnitt 5.4).

Data som därefter överförs genom gränssnittet (luften) kontrolleras genom cyklisk redundanskontroll (CRC) på kommunikationsnivån. Data som valideras genom CRC är korrekta. Data som inte valideras genom CRC återsänds. Sannolikheten att data skulle kunna passera genom en CRC på fel sätt är statistiskt så liten att den kan lämnas utan avseende.

Om data inte valideras genom CRC och det inte finns tid att återsända och ta emot korrekta data blir resultatet inte ett fel, utan en instansiering av en särskild typ av misslyckad avläsning.

De enda meningsfulla ”misslyckade” data som kan registreras är antalet lyckade initieringar av transaktioner som förekommer men inte leder till en lyckad dataöverföring till fjärravläsaren.

DSC_82 *Fjärravläsaren* ska därför registrera, med tidsstämpel, antalet tillfällen där initieringsfasen lyckas för en DSRC-avläsning, men transaktionen avslutas innan korrekta *data* hämtats av fjärravläsaren. Dessa data ska vara tillgängliga för de behöriga kontrollmyndigheternas representant och lagras i fjärravläsarens minne. De medel som används för att åstadkomma detta ska bestämmas genom produktens utformning eller genom en specifikation från en behörig kontrollmyndighet.

De enda meningsfulla data om ”fel” som kan registreras är antalet tillfällen där fjärravläsaren misslyckas med att dekryptera de *data* som tas emot. Det bör dock noteras att detta enbart berör effektiviteten för fjärravläsarens programvara. Data kan vara tekniskt dekrypterade utan att ha någon semantisk mening.

DSC_83 *Fjärravläsaren* ska därför registrera, med tidsstämpel, antalet tillfällen den försökt men misslyckats med att dekryptera data som tagits emot via DSRC-gränssnittet.

6 PROVNING VID DRIFTSÄTTNING OCH PERIODISK BESIKTNING AV FJÄRRKOMMUNIKATIONSFUNKTIONEN

6.1 **Allmänt**

DSC_84 Två typer av prov kan förutses för fjärrkommunikationsfunktionen:

1) Ett ECHO-prov för att validera den trådlösa kommunikationskanalen mellan fjärravläsarens DSRC-modul och fordonsenhetens DSRC-modul.

2) Ett säkerhetsprov från början till slut för att säkerställa att ett verkstadskort kan komma åt krypterat och signerat datainnehåll som skapas i fordonsenheten och överförs via den trådlösa kommunikationskanalen.

6.2 **ECHO**

Detta avsnitt innehåller bestämmelser som är framtagna särskilt för att endast prova att kommunikationskanalen mellan fjärravläsarens DSRC-modul och fordonsenhetens DSRC-modul är funktionellt aktiv.

▼B

Syftet med kommandot ECHO är att ge verkstäder eller anläggningar för typgodkännandeprov möjlighet att prova om DSRC-länken fungerar, utan att behöva ha tillgång till säkerhetsuppgifter. Provarens utrustning behöver därför endast kunna initiera en DSRC-kommunikation (sända en BST med AID = 2) och sedan sända ECHO-kommandot och, under antagandet att DSRC fungerar, ta emot ECHO-svaret. Se avsnitt 5.4.8 för mer information. Under antagandet att detta svar tas emot korrekt kan den korrekta funktionen hos DSRC-länken mellan fjärravläsarens DSRC-modul och fordonsenhetens DSRC-modul valideras.

6.3 **Prov för att validera skyddat datainnehåll**

DSC_85 Detta prov utförs för att validera ett skyddat dataflöde från början till slut. En provningsavläsare för DSRC behövs för detta prov. Provningsavläsaren för DSRC har samma funktionalitet och är utformad utifrån samma specifikationer som den avläsare som används av kontrolltjänstemännen (även kallade *law enforcer*), med undantaget att ett verkstadskort i stället för ett kontrollkort ska användas för att autentisera användaren av provningsavläsaren. Provet kan utföras efter den första aktiveringen av en smart färdskrivare eller i slutet av kalibreringsförfarandet. Efter aktiveringen ska fordonsenheten generera skyddade data för tidig upptäckt och överföra dessa till fordonsenhetens DSRC-modul.

DSC_86 Verkstadspersonalen ska placera provningsavläsaren för DSRC på ett avstånd av mellan 2 och 10 meter framför fordonet.

DSC_87 Verkstadspersonalen ska sedan sätta in ett verkstadskort i provningsavläsaren för att begära avläsning av data för tidig upptäckt i fordonsenheten. Efter en lyckad avläsning ska verkstadspersonalen kontrollera mottagna data för att säkerställa att deras integritet har validerats och att de har dekrypterats.

▼B

Tillägg 15

MIGRERING: PARALLELL HANTERING AV FLERA UTRUSTNINGSGENERATIONER

INNEHÅLLSFÖRTECKNING

1 DEFINITIONER

2. ALLMÄNNA BESTÄMMELSER

2.1. Övergången i stora drag

2.2. Driftskompatibilitet mellan fordonsenhet och kort

2.3. Driftskompatibilitet mellan fordonsenhet och rörelsesensor

2.4. Driftskompatibilitet mellan fordonsenheter, färdskrivarkort och utrustning för dataöverföring

2.4.1 Direkt överföring från kort till IDE-enhet

2.4.2 Överföring från kort via fordonsenhet

2.4.3 Överföring från fordonsenhet

2.5. Driftskompatibilitet mellan fordonsenhet och kalibreringsutrustning

3. VIKTIGA STEG UNDER PERIODEN FÖRE INFÖRANDEDAGEN

4. BESTÄMMELSER FÖR PERIODEN EFTER INFÖRANDEDAGEN

1 DEFINITIONER

Följande definitioner används i detta tillägg:

smart färdskrivarsystem*:* Enligt definition i denna bilaga (kapitel 1, definition bbb).

första generationens färdskrivarsystem*:* Enligt definition i denna förordning (artikel 2, definition 1).

andra generationens färdskrivarsystem*:* Enligt definition i denna förordning (artikel 2, definition 7).

införandedag*:* Enligt definition i denna bilaga (kapitel 1, definition ccc).

IDE (*Intelligent Dedicated Equipment*)*:* Utrustning som används för dataöverföring, enligt definition i tillägg 7 till denna bilaga.

2. ALLMÄNNA BESTÄMMELSER

2.1. **Övergången i stora drag**

I inledningen till denna bilaga beskrivs i stora drag övergången mellan första och andra generationens färdskrivarsystem.

Utöver bestämmelserna i denna inledning gäller följande:

— Första generationens rörelsesensorer kommer inte att vara driftskompatibla med andra generationens fordonsenheter.

— Andra generationens rörelsesensorer kommer att installeras i fordon samtidigt som andra generationens fordonsenheter.

▼B

— Dataöverförings- och kalibreringsutrustning kommer att behöva utvecklas för att stödja användning av båda generationerna av färdskrivare och färdskrivarkort.

2.2. **Driftskompatibilitet mellan fordonsenhet och kort**

Det är underförstått att första generationens färdskrivarkort är driftskompatibla med första generationens fordonsenheter (i enlighet med bilaga 1B till denna förordning), medan andra generationens färdskrivarkort är driftskompatibla med andra generationens fordonsenheter (i enlighet med bilaga 1C till denna förordning). Dessutom gäller följande krav:

MIG_001 Första generationens färdskrivarkort får fortsätta att användas i andra generationens fordonsenheter fram till deras sista giltighetsdag, med undantag för det som föreskrivs i krav MIG_004 och MIG_005. Innehavarna får dock efterfråga att de ersätts med andra generationens färdskrivarkort så snart de finns tillgängliga.

MIG_002 Andra generationens fordonsenheter ska kunna använda alla giltiga förar-, kontroll- och företagskort av första generationen som sätts in.

MIG_003 Denna förmåga kan komma att slutgiltigt tas bort i samband med verkstadsbesök, så att första generationens färdskrivarkort inte längre godtas. Detta kan endast ske efter det att Europeiska kommissionen har inlett ett förfarande i syfte att begära detta av verkstäderna, t.ex. vid varje periodisk färdskrivarbesiktning.

MIG_004 Andra generationens fordonsenheter får endast använda andra generationens verkstadskort.

MIG_005 När det gäller att avgöra funktionsläge ska andra generationens fordonsenheter endast beakta typen av giltigt kort som sätts in, oavsett dess generation.

MIG_006 Ett giltigt andra generationens färdskrivarkort ska kunna användas i första generationens fordonsenheter på exakt samma sätt som ett första generationens färdskrivarkort av samma typ.

2.3. **Driftskompatibilitet mellan fordonsenhet och rörelsesensor**

Det är underförstått att första generationens rörelsesensorer är driftskompatibla med första generationens fordonsenheter, medan andra generationens rörelsesensorer är driftskompatibla med andra generationens fordonsenheter. Dessutom gäller följande krav:

MIG_007 Andra generationens fordonsenheter kan inte paras och användas med första generationens rörelsesensorer.

MIG_008 Andra generationens rörelsesensorer kan paras och användas endast med andra generationens fordonsenheter, eller med båda generationerna av fordonsenheter.

2.4. **Driftskompatibilitet mellan fordonsenheter, färdskrivarkort och utrustning för dataöverföring**

MIG_009 Utrustning för dataöverföring får användas med endast en generation av fordonsenheter och färdskrivarkort, eller med båda.

▼B

2.4.1 *Direkt överföring från kort till IDE-enhet*

MIG_010 Vid dataöverföring från ett färdskrivarkort av en viss generation som är insatt i en kortläsare till en IDE-enhet ska säkerhetsmekanismerna och dataöverföringsprotokollet för denna generation användas, och överförda data ska ha det format som definierats för denna generation.

MIG_011 För förarkontroll genom andra än EU:s kontrollmyndigheter ska det också vara möjligt att överföra andra generationens förarkort (och verkstadskort) på exakt samma sätt som första generationens förarkort (och verkstadskort). En sådan överföring ska omfatta följande:

— Icke signerade elementfiler `IC` och `ICC`.

— Icke signerade elementfiler (för första generationen) `Card_Certificate` och `CA_Certificate`.

— Andra elementfiler med tillämpningsdata (under den dedikerade filen `TACHO`) 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 med tillämpningsdata som endast finns på andra generationens förarkort (och verkstadskort) (elementfiler med tillämpningsdata under den dedikerade filen `TACHO_G2`).

2.4.2 *Överföring från kort via fordonsenhet*

MIG_012 Vid dataöverföring från ett andra generationens kort som är insatt i en första generationens fordonsenhet ska första generationens dataöverföringsprotokoll användas. Kortet ska svara på fordonsenhetens kommandon på exakt samma sätt som ett första generationens kort, och överförda data ska ha samma format som data som överförs från första generationens kort.

MIG_013 Vid dataöverföring från ett första generationens kort som är insatt i en andra generationens fordonsenhet ska det dataöverföringsprotokoll som är definierat i tillägg 7 till denna bilaga användas. Fordonsenheten ska skicka kommandon till kortet på exakt samma sätt som en första generationens fordonsenhet, och överförda data ska följa det format som definierats för första generationens kort.

2.4.3 *Överföring från fordonsenhet*

MIG_014 Vid dataöverföring från en andra generationens fordonsenhet som använder andra generationens säkerhetsmekanismer ska det dataöverföringsprotokoll som är definierat i tillägg 7 till denna bilaga användas.

MIG_015 För förarkontroll genom andra än EU:s kontrollmyndigheter och dataöverföring från fordonsenheten i verkstäder utanför EU kan det också vara möjligt att överföra data från andra generationens fordonsenheter genom att använda första generationens säkerhetsmekanismer och första generationens dataöverföringsprotokoll. Överförda data ska ha samma format som data som överförs från en första generationens fordonsenhet. Denna förmåga kan väljas fritt genom kommandon i menyerna.

▼B

2.5. **Driftskompatibilitet mellan fordonsenhet och kalibreringsutrustning**

MIG_016 Kalibreringsutrustning ska kunna utföra kalibrering av varje generation av färdskrivare med hjälp av kalibreringsprotokollet för respektive generation. Kalibreringsutrustning får användas för endast en färdskrivargeneration, eller för båda.

3. VIKTIGA STEG UNDER PERIODEN FÖRE INFÖRANDEDAGEN

MIG_017 Nycklar och certifikat för provning ska vara tillgängliga för tillverkare senast **30 månader** före införandedagen.

MIG_018 Driftskompatibilitetsprov ska kunna inledas på begäran från tillverkare senast **15 månader** före införandedagen.

MIG_019 Officiella nycklar och certifikat ska vara tillgängliga för tillverkare senast **12 månader** före införandedagen.

MIG_020 Medlemsstater ska kunna utfärda andra generationens verkstadskort senast **3 månader** före införandedagen.

MIG_021 Medlemsstater ska kunna utfärda alla typer av andra generationens färdskrivarkort senast **1 månad före införandedagen**.

4. BESTÄMMELSER FÖR PERIODEN EFTER INFÖRANDEDAGEN

MIG_022 Efter införandedagen ska medlemsstaterna endast utfärda andra generationens färdskrivarkort.

MIG_023 Tillverkare av fordonsenheter/rörelsesensorer ska tillåtas producera första generationens fordonsenheter/rörelsesensorer så länge de används i praktiken, så att felaktiga komponenter kan bytas ut.

MIG_024 Tillverkare av fordonsenheter/rörelsesensorer ska ha möjlighet att begära och erhålla fortsatta typgodkännanden för första generationens typer av fordonsenheter/rörelsesensorer som redan typgodkänts.

▼B

Tillägg 16

ADAPTER FÖR FORDONSKATEGORIERNA M1 OCH N1

INNEHÅLLSFÖRTECKNING

1. FÖRKORTNINGAR OCH REFERENSDOKUMENT

1.1. Förkortningar

1.2. Hänvisningar till standarder

2. ALLMÄN BESKRIVNING AV ADAPTERN OCH DESS FUNKTIONER

2.1. Allmän beskrivning av adaptern

2.2. Funktioner

2.3. Säkerhet

3. KRAV PÅ FÄRDSKRIVAREN NÄR EN ADAPTER ÄR INSTALLERAD

4. KONSTRUKTIONS- OCH FUNKTIONSKRAV FÖR ADAPTERN

4.1. Gränssnitt mot och anpassning av inkommande hastighetspulser

4.2. Inducering av de inkommande pulserna till den inbyggda rörelsesensorn

4.3. Inbyggd rörelsesensor

4.4. Säkerhetskrav

4.5. Prestanda

4.6. Material

4.7. Märkningar

5. INSTALLATION AV FÄRDSKRIVARE NÄR EN ADAPTER ANVÄNDS

5.1. Installation

5.2. Plombering

6. KONTROLLER, BESIKTNINGAR OCH REPARATIONER

6.1. Periodiska besiktningar

7. TYPGODKÄNNANDE FÖR FÄRDSKRIVARE NÄR EN ADAPTER ANVÄNDS

7.1. Allmänt

7.2. Funktionsintyg

1. FÖRKORTNINGAR OCH REFERENSDOKUMENT

1.1. Förkortningar

TBD To Be Defined (ej fastställt)

VU Vehicle Unit (fordonsenhet)

1.2. Hänvisningar till standarder

ISO16844-3 Road vehicles – Tachograph systems – Part 3: Motion sensor interface

2. ALLMÄN BESKRIVNING AV ADAPTERN OCH DESS FUNKTIONER

2.1. Allmän beskrivning av adaptern

ADA_001 Adaptern ska förse en ansluten fordonsenhet med krypterade rörelsedata som ständigt visar fordonets hastighet och tillryggalagda sträcka.

Adaptern är endast avsedd för de fordon som ska vara utrustade med färdskrivare enligt denna förordning.

▼B

Den ska installeras och användas endast i de fordonstyper som definieras i definition ”yy” (”adapter”) i bilaga 1C, där det inte är mekaniskt möjligt att installera någon annan typ av existerande rörelsesensor som i övrigt överensstämmer med bestämmelserna i denna bilaga och dess tillägg 1–16.

Adaptern får inte ha ett mekaniskt gränssnitt med en rörlig fordonsdel, utan ska vara ansluten till de impulser för hastighet/sträcka som avges av integrerade sensorer eller alternativa gränssnitt.

ADA_002 En typgodkänd rörelsesensor (enligt bestämmelserna i avsnitt 8 i bilaga IC om typgodkännande för färdskrivare och färdskrivarkort) ska monteras inuti adapterns hölje, som också ska rymma en pulsomvandlare som inducerar de inkommande pulserna till den inbyggda rörelsesensorn. Denna inbyggda rörelsesensor ska själv vara ansluten till fordonsenheten, så att gränssnittet mellan fordonsenheten och adaptern överensstämmer med de krav som anges i ISO 16844-3.

2.2. **Funktioner**

ADA_003 Adaptern ska inbegripa följande funktioner:

— Gränssnitt mot och anpassning av de inkommande hastighetspulserna.

— Inducering av de inkommande pulserna till den inbyggda rörelsesensorn.

— Alla funktioner i den inbyggda rörelsesensorn, så att krypterade rörelsedata tillhandahålls fordonsenheten.

2.3. **Säkerhet**

ADA_004 Adaptern får inte vara säkerhetscertifierad enligt det allmänna säkerhetsmålet för rörelsesensorer i tillägg 10 till denna bilaga. I stället ska säkerhetskraven i avsnitt 4.4 i detta tillägg gälla.

3. KRAV PÅ FÄRDSKRIVAREN NÄR EN ADAPTER ÄR INSTALLERAD

I de följande kapitlen anges hur kraven i denna bilaga ska tolkas när en adapter används. De relaterade kravnumren i bilaga 1C anges i parentes.

ADA_005 Varje färdskrivare i fordon som har utrustats med en adapter ska överensstämma med alla bestämmelser, om inte annat anges i detta tillägg.

ADA_006 När en adapter är installerad inbegriper färdskrivaren kablar, adaptern (inklusive en rörelsesensor) och en fordonsenhet (krav 01).

ADA_007 Färdskrivarens funktion för upptäckt av en händelse och/eller fel ändras enligt följande:

— Händelsen ”avbrott i strömtillförseln” (*Power Supply Interruption*) ska utlösas av fordonsenheten om strömtillförseln i den inbyggda rörelsesensorn är avbruten under mer än 200 millisekunder när kalibreringsläget inte är inställt (krav 79).

▼B

— Händelsen ”fel i rörelsedata” ska utlösas av fordonsenheten vid avbrott av det normala dataflödet mellan den inbyggda rörelsesensorn och fordonsenheten och/eller vid integritetsfel eller autentiseringsfel under utbyte av data mellan den inbyggda rörelsesensorn och fordonsenheten (krav 83).

— Händelsen ”försök till säkerhetsöverträdelse” ska utlösas av fordonsenheten vid varje övrig händelse som påverkar säkerheten i den inbyggda rörelsesensorn när kalibreringsläget inte är inställt (krav 85).

— ”Färdskrivarfel” ska utlösas av fordonsenheten för varje fel i den inbyggda rörelsesensorn när kalibreringsläget inte är inställt (krav 88).

ADA_008 De adapterfel som kan upptäckas av färdskrivaren ska vara de som är relaterade till den inbyggda rörelsesensorn (krav 88).

ADA_009 Fordonsenhetens kalibreringsfunktion ska möjliggöra automatisk parning av den inbyggda rörelsesensorn med fordonsenheten (krav 202, 204).

4. KONSTRUKTIONS- OCH FUNKTIONSKRAV FÖR ADAPTERN

4.1. **Gränssnitt mot och anpassning av inkommande hastighetspulser**

ADA_011 Adapterns gränssnitt för indata ska acceptera frekvenspulser som motsvarar fordonets hastighet och/eller tillryggalagda sträcka. De inkommande pulserna har följande elektriska egenskaper: *TBD (ska definieras av tillverkaren)*. Inställningar som endast finns tillgängliga för adaptertillverkaren och den godkända verkstad som utför installationen av adaptern ska möjliggöra ett korrekt gränssnitt för adapterns indata till fordonet, i förekommande fall.

ADA_012 Gränssnittet för adapterns indata ska, i förekommande fall, kunna multiplicera eller dividera frekvenspulserna i de inkommande hastighetspulserna med hjälp av en fast faktor, för att anpassa signalen till en k-konstant inom det intervall som definieras i denna bilaga (4 000 till 25 000 imp/km). Denna fastställda faktor får endast programmeras av adaptertillverkaren och den godkända verkstad som utför installationen av adaptern.

4.2. **Inducering av de inkommande pulserna till den inbyggda rörelsesensorn**

ADA_013 De inkommande pulserna, eventuellt anpassade enligt vad som anges ovan, ska induceras till den inbyggda rörelsesensorn, så att varje inkommande puls upptäcks av rörelsesensorn.

4.3. **Inbyggd rörelsesensor**

ADA_014 Den inbyggda rörelsesensorn ska stimuleras av de inducerade pulserna, för att på så sätt kunna generera rörelsedata som korrekt motsvarar fordonets rörelse, som om den var mekaniskt ihopkopplad med en rörlig del av fordonet.

ADA_015 Identifieringsdata i den inbyggda rörelsesensorn ska användas av fordonsenheten för att identifiera adaptern (krav 95).

▼B

ADA_016 Installationsdata som lagras i den inbyggda rörelsesensorn ska anses motsvara adapterns installationsdata (krav 122).

4.4. **Säkerhetskrav**

ADA_017 Adapterns hölje ska vara utformat så att det inte kan öppnas. Den ska vara plomberad, så att försök till fysisk manipulering lätt kan upptäckas (exempelvis genom okulär besiktning, se ADA_035). Plomberingar ska uppfylla samma krav som rörelsesensorns plomberingar (krav 398–406).

ADA_018 Det ska inte vara möjligt att avlägsna den inbyggda rörelsesensorn från adaptern utan att bryta plomberingen/plomberingarna på adapterns hölje, eller bryta plomberingen mellan rörelsesensorn och adapterns hölje (se ADA_034).

ADA_019 Adaptern ska säkerställa att de rörelsedata som genereras och behandlas endast kommer från adapterns indata.

4.5. **Prestanda**

ADA_020 Adaptern ska vara helt funktionsduglig inom ett temperaturintervall som definieras av tillverkaren.

ADA_021 Adaptern ska vara helt funktionsduglig vid en luftfuktighet i intervallet 10–90 % (krav 214).

ADA_022 Adaptern ska skyddas mot överspänning, mot omkastning av polerna i dess strömtillförsel och mot kortslutning (krav 216).

ADA_023 Adaptern ska antingen

— reagera på ett magnetfält som stör avkänningen av fordonets rörelse (i så fall ska fordonsenheten registrera och lagra ett sensorfel (krav 88)), eller

— ha ett sensorelement som är skyddat eller immunt mot magnetfält (krav 217).

ADA_024 Adaptern ska uppfylla kraven i den internationella förordningen UN ECE R10 i fråga om elektromagnetisk kompatibilitet, och ska skyddas mot elektrostatiska laddningar och transienter (krav 218).

4.6. **Material**

ADA_025 Adaptern ska uppfylla kriterierna för skyddsklass (*TBD, ska definieras av tillverkaren, beroende på installationsplats*) (krav 220, 221).

ADA_026 Färgen på adapterns hölje ska vara gul.

4.7. **Märkningar**

ADA_027 En typskylt ska fästas på adaptern, och den ska ange följande:

— Adaptertillverkarens namn och adress.

— Tillverkarens artikelnummer och tillverkningsår för adaptern.

— Typgodkännandemärke för adaptertypen eller för färdskrivartypen som innehåller adaptern.

— Installationsdatum för adaptern.

▼B

— Identifieringsnummer för det fordon som adaptern har installerats i.

ADA_028 Typskylten ska också visa följande uppgifter (om de inte är direkt läsbara från utsidan av den inbyggda rörelsesensorn):

— Namn på tillverkaren av den inbyggda rörelsesensorn.

— Tillverkarens artikelnummer och tillverkningsår för den inbyggda rörelsesensorn.

— Typgodkännandemärke för den inbyggda rörelsesensorn.

5. INSTALLATION AV FÄRDSKRIVARE NÄR EN ADAPTER ANVÄNDS

5.1. **Installation**

ADA_029 Adaptrar för installation i fordon får endast installeras av fordonstillverkare eller av godkända verkstäder som har tillstånd att installera, aktivera och kalibrera digitala och smarta färdskrivare.

ADA_030 Den godkända verkstad som installerar adaptern ska justera gränssnitt för indata och välja fördelningsförhållandet för insignalen (i förekommande fall).

ADA_031 Plomberingen av adapterns hölje ska utföras av en godkänd verkstad.

ADA_032 Adaptern ska monteras så nära den del av fordonet som förser den med dess inkommande pulser som möjligt.

ADA_033 Kablarna för adapterns strömtillförsel ska vara röda (positiv strömförsörjning) och svarta (jord).

5.2. **Plombering**

ADA_034 Följande krav för plombering ska gälla:

— Adapterns hölje ska vara plomberat (se ADA_017).

— Den inbyggda sensorns hölje ska vara plomberat till adapterns hölje, såvida det inte är omöjligt att avlägsna sensorn från adapterns hölje utan att bryta adapterhöljets plombering(ar) (se ADA_018).

— Adapterns hölje ska vara plomberat till fordonet.

— Anslutningen mellan adaptern och den utrustning som tillhandahåller dess inkommande pulser ska vara plomberad i båda ändar (i den mån det är rimligen möjligt).

6. KONTROLLER, BESIKTNINGAR OCH REPARATIONER

6.1. **Periodiska besiktningar**

ADA_035 När en adapter används ska varje periodisk besiktning (med periodisk besiktning avses besiktningar i enlighet med krav 409–413 i bilaga I C) av färdskrivaren omfatta följande kontroller:

— Kontroll av att lämpligt typgodkännandemärke finns på adaptern.

— Kontroll av att plomberingarna på adaptern och dess anslutningar är orörda.

▼B

— Kontroll av att adaptern är installerad enligt vad som anges på typskylten.

— Kontroll av att adaptern är installerad enligt anvisningar från tillverkaren av adaptern och/eller fordonet.

— Kontroll av att det är tillåtet att montera en adapter på det besiktigade fordonet.

ADA_036 Dessa besiktningar ska inbegripa en kalibrering och ett byte av samtliga plomberingar, oavsett deras skick.

7. TYPGODKÄNNANDE FÖR FÄRDSKRIVARE NÄR EN ADAPTER ANVÄNDS

7.1. **Allmänt**

ADA_037 Adaptern ska finnas med vid ansökan om typgodkännande av färdskrivare (krav 425).

ADA_038 En adapter får lämnas in för eget typgodkännande eller för typgodkännande som en komponent i en färdskrivare.

ADA_039 Ett sådant typgodkännande ska inbegripa funktionsprovning av adaptern. Positiva resultat från vart och ett av dessa prov ska anges i ett lämpligt intyg (krav 426).

7.2. **Funktionsintyg**

ADA_040 Ett funktionsintyg för en adapter eller en färdskrivare som innehåller en adapter får inte utfärdas till adaptertillverkaren förrän minst alla följande funktionsprov har genomgåtts med positivt resultat.

Nr	Prov	Beskrivning	Tillämpliga krav
1.	**Administrativ provning**		
1.1	Dokumentation	Är adapterns dokumentation korrekt?	
2.	**Okulär besiktning**		
2.1.	Adapterns överensstämmelse med dokumentationen		
2.2.	Identifiering/märkningar på adaptern		ADA_027, ADA_028
2.3	Adapterns material		(krav 219–223) ADA_026
2.4.	Plombering		ADA_017, ADA_018, ADA_034
3.	**Funktionsprov**		
3.1	Inducering av hastighetspulserna till den inbyggda rörelsesensorn		ADA_013

▼B

Nr	Prov	Beskrivning	Tillämpliga krav
3.2	Gränssnitt mot och anpassning av inkommande hastighetspulser		ADA_011, ADA_012
3.3	Rörelsemätningens noggrannhet		(krav 30–35, 217)
4.	**Miljöprovningar**		
4.1	Tillverkarens provresultat	Resultat av tillverkarens miljöprovningar	ADA_020, ADA_021, ADA_022, ADA_023, ADA_024
5.	**EMC**		
5.1	Utstrålning och känslighet	Kontrollera överensstämmelse med direktiv ECE R10	ADA_024
5.2	Tillverkarens provresultat	Resultat av tillverkarens miljöprovningar	ADA_024

▼C1

BILAGA II

TYPGODKÄNNANDEMÄRKE OCH TYPGODKÄNNANDEINTYG

I. TYPGODKÄNNANDEMÄRKE

1. Typgodkännandemärket ska bestå av följande:

a) En rektangel, inom vilken bokstaven ”e” ska vara inskriven, följd av en särskiljande siffer- eller bokstavskod för det land som har utfärdat typgodkännandet enligt följande:

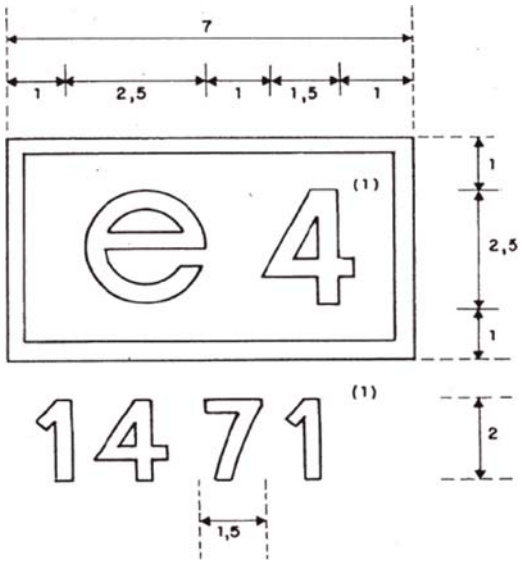
Belgien	6
Bulgarien	34
Tjeckien	8
Danmark	18
Tyskland	1
Estland	29
Irland	24
Grekland	23
Spanien	9
Frankrike	2
Kroatien	25
Italien	3
Cypern	CY
Lettland	32
Litauen	36
Luxemburg	13
Ungern	7
Malta	MT
Nederländerna	4
Österrike	12
Polen	20
Portugal	21
Rumänien	19
Slovenien	26
Slovakien	27
Finland	17
Sverige	5
Förenade kungariket	11

b) Ett typgodkännandenummer som motsvarar numret på det intyg om typgodkännande som utfärdats för färdskrivarens prototyp, diagrambladet eller färdskrivarkortet. Detta nummer ska vara anbringat i rektangelns omedelbara närhet.

▼C1

2. Typgodkännandemärket ska finnas på typskylten för varje färdskrivarutrustning och på varje diagramblad och på varje färdskrivarkort. Märket ska inte kunna utplånas och det ska alltid förbli tydligt läsbart.

3. Typgodkännandemärkets mått, som visas här nedan ([1]), är uttryckta i millimeter och utgör de minsta tillåtna. Förhållandena mellan måtten ska bibehållas.



([1]) Dessa uppgifter visas endast som vägledning.

▼C1

II. TYPGODKÄNNANDEINTYG FÖR ANALOGA FÄRDSKRIVARE

En medlemsstat som har beviljat typgodkännande ska åt sökanden utfärda ett typgodkännandeintyg enligt nedan angivna förlaga. När en medlemsstat informerar andra medlemsstater om utfärdade typgodkännanden eller om eventuellt återkallade sådana, ska den använda kopior av detta intyg.

TYPGODKÄNNANDEINTYG

Namn på behörig myndighet .....

Underrättelse rörande ([1]):

— Typgodkännande av färdskrivare

— Återkallande av typgodkännande av färdskrivare

— Typgodkännande av förlaga till diagramblad

— Återkallande av typgodkännande av förlaga till diagramblad

Typgodkännandenummer:

.....

1. Varumärke eller varunamn .....

2. Typens eller förlagans namn .....

3. Tillverkarens namn .....

4. Tillverkarens adress .....

5. Inlämnad för typgodkännande den .....

6. Provad vid .....

7. Datum och nummer för provning(ar) .....

8. Typgodkännandedatum .....

9. Återkallandedatum för typgodkännande .....

10. Typ(er) av färdskrivare där diagrambladet är avsett att användas

11. Plats .....

12. Datum .....

13. Bifogade beskrivande dokument .....

14. Anmärkningar (inklusive placering av plomberingar i förekommande fall)

(Underskrift)

([1]) Stryk det som inte är tillämpligt.

▼C1

III. TYPGODKÄNNANDEINTYG FÖR DIGITALA FÄRDSKRIVARE

En medlemsstat som har beviljat typgodkännande ska åt sökanden utfärda ett typgodkännandeintyg enligt nedan angivna förlaga. När en medlemsstat informerar andra medlemsstater om utfärdade typgodkännanden eller om eventuellt återkallade sådana, ska den använda kopior av detta intyg.

TYPGODKÄNNANDEINTYG FÖR DIGITALA FÄRDSKRIVARE

Namn på behörig myndighet .....

Underrättelse rörande ([1]):

☐ Typgodkännande av: ☐ Återkallelse av typgodkännande av:

☐ Färdskrivarmodell

☐ Färdskrivarkomponent ([2])

☐ Förarkort

☐ Verkstadskort

☐ Företagskort

☐ Kontrollkort

Typgodkännandenummer:

.....

1. Tillverkarens märke eller varumärke .....
2. Modellens namn .....
3. Tillverkarens namn .....
4. Tillverkarens adress .....
5. Inlämnad för typgodkännande den .....
6. Laboratorium (eller laboratorier) .....
7. Datum och nummer för provningsrapport .....
8. Typgodkännandedatum .....
9. Återkallandedatum för typgodkännande .....
10. Modell av färdskrivare i vilken komponenten är konstruerad för att användas
11. Plats .....
12. Datum .....
13. Bifogade beskrivande dokument .....
14. Anmärkningar (inklusive placering av plomberingar i förekommande fall)

(Underskrift)

([1]) Kryssa i tillämpliga rutor.
([2]) Ange vilken komponent underrättelsen gäller.

▼C1

IV. TYPGODKÄNNANDEINTYG FÖR SMARTA FÄRDSKRIVARE

En medlemsstat som har beviljat typgodkännande ska åt sökanden utfärda ett typgodkännandeintyg enligt nedan angivna förlaga. När en medlemsstat informerar andra medlemsstater om utfärdade typgodkännanden eller om eventuellt återkallade sådana, ska den använda kopior av detta intyg.

TYPGODKÄNNANDEINTYG FÖR SMARTA FÄRDSKRIVARE

Namn på behörig myndighet .....

Underrättelse rörande ([1]):

☐ Typgodkännande av: ☐ Återkallelse av typgodkännande av:

☐ Färdskrivarmodell

☐ Färdskrivarkomponent ([2])

☐ Förarkort

☐ Verkstadskort

☐ Företagskort

☐ Kontrollkort

Typgodkännandenummer:

.....

1. Tillverkarens märke eller varumärke .....
2. Modellens namn .....
3. Tillverkarens namn .....
4. Tillverkarens adress .....
5. Inlämnad för typgodkännande den .....
6. a) Provningslaboratorium för funktionscertifiering .....
   b) Provningslaboratorium för säkerhetscertifiering .....
   c) Provningslaboratorium för certifiering av driftskompatibilitet .....
7. a) Datum och nummer för funktionsintyg .....
   b) Datum och nummer för säkerhetsintyg .....
   c) Datum och nummer för intyg om driftskompatibilitet .....
8. Typgodkännandedatum .....
9. Återkallandedatum för typgodkännande .....
10. Modell av färdskrivare i vilken komponenten är konstruerad för att användas
11. Plats .....
12. Datum .....
13. Bifogade beskrivande dokument .....
14. Anmärkningar (inklusive placering av plomberingar i förekommande fall)

(Underskrift)

([1]) Kryssa i tillämpliga rutor.
([2]) Ange vilken komponent underrättelsen gäller.