I

(Rättsakter vilkas publicering är obligatorisk)

KOMMISSIONENS FÖRORDNING (EG) nr 1360/2002

av den 13 juni 2002

om anpassning för sjunde gången till den tekniska utvecklingen av rådets förordning (EEG) nr 3821/85 om färdskrivare vid vägtransporter

(Text av betydelse för EES)

EUROPEISKA GEMENSKAPERNAS KOMMISSION HAR ANTAGIT DENNA FÖRORDNING

med beaktande av Fördraget om upprättandet av Europeiska gemenskapen,

med beaktande av rådets förordning (EEG) nr 3821/85 av den 20 december 1985 om färdskrivare vid vägtransporter ([1]), senast ändrad genom förordning (EG) nr 2135/98 ([2]), särskilt artiklarna 17 och 18 i denna, och

av följande skäl:

(1) De tekniska specifikationerna i bilaga I B till förordning (EEG) nr 3821/85 måste anpassas till den tekniska utvecklingen med särskild hänsyn till den övergripande säkerheten i systemet och till kompatibiliteten mellan färdskrivare och förarkort.

(2) En anpassning av utrustningen förutsätter dessutom en anpassning av bilaga II till förordning (EEG) nr 3821/85, i vilken typgodkännandemärken och typgodkännandeintyg definieras.

(3) Den kommitté som upprättats genom artikel 18 i förordning (EG) nr 3821/85 har inte avgivit något yttrande om de åtgärder som föreskrivs i detta, och kommissionen har därför lagt fram ett förslag om dessa åtgärder inför rådet.

(4) Rådet har inte vidtagit några åtgärder inom den tidsfrist som fastställs i artikel 18.5 i förordning (EEG) nr 3821/85, och därför är det kommissionens uppgift att anta dessa åtgärder.

HÄRIGENOM FÖRESKRIVS FÖLJANDE.

Artikel 1

Bilagan till förordning (EG) nr 2135/98 skall ersättas med bilagan till denna förordning.

Artikel 2

Bilaga II till förordning (EEG) nr 3821/85 skall ändras på följande sätt:

1. Första stycket i punkt 1 i kapitel I skall ändras på följande sätt:
   — Nationalitetsbeteckningen för Grekland ”GR” skall ersättas med ”23”.
   — Nationalitetsbeteckningen för Irland ”IRL” skall ersättas med ”24”.
   — Nationalitetsbeteckningen ”12” skall läggas till för Österrike.
   — Nationalitetsbeteckningen ”17” skall läggas till för Finland.
   — Nationalitetsbeteckningen ”5” skall läggas till för Sverige.
2. Andra stycket i punkt 1 i kapitel I skall ändras på följande sätt:
   — Orden ”eller för ett färdskrivarkort” skall införas efter ordet ”diagrambladet”.
3. Punkt 2 i kapitel I skall ändras på följande sätt:
   — Orden ”och på varje färdskrivarkort” skall införas efter ordet ”diagramblad”.
4. I kapitel II skall följande ordalydelse läggas till titeln ”FÖR PRODUKTER SOM UPPFYLLER BESTÄMMELSERNA I BILAGA I”

([1]) EGT L 370, 31.12.1985, s. 8.
([2]) EGT L 274, 9.10.1998, s. 1.

5. Följande kapitel III skall läggas till:

"III. TYPGODKÄNNANDEINTYG FÖR PRODUKTER SOM UPPFYLLER BESTÄMMELSERNA I BILAGA I B

En stat som har beviljat typgodkännande skall åt sökanden utfärda ett typgodkännandeintyg enligt nedan angivna mall. När en medlemsstat informerar andra medlemsstater om utfärdade typgodkännanden eller om eventuellt återkallade sådana, skall den använda kopior av detta intyg.

MALL FÖR TYPGODKÄNNANDEINTYG FÖR PRODUKTER SOM UPPFYLLER BESTÄMMELSERNA I BILAGA I B

Namn på den behöriga myndigheten: .....

Anmälan med avseende på (*):

☐ typgodkännande av

☐ återkallelse av godkännande av

☐ färdskrivarmodell

☐ färdskrivarkomponent (**) .....

☐ ett förarkort

☐ ett verkstadskort

☐ ett företagskort

☐ ett kontrollkort

Typgodkännande nr: .....

1. Tillverkningsmärke eller varumärke: .....
2. Modellens namn: .....
3. Tillverkarens namn: .....
4. Tillverkarens adress: .....
5. Ansökan om godkännande inlämnad för: .....
6. Laboratorium/er: .....
7. Datum för provning/ar och provningsnummer: .....
8. Datum för godkännande: .....
9. Datum för återkallelse av godkännande: .....
10. Modell på den/de färdskrivarkomponenter med vilka komponenten är avsedd att användas: .....
11. Ort: .....
12. Datum: .....
13. Bifogade beskrivande handlingar: .....

---

14. Anmärkningar (inbegripet plomberingarnas placering i förekommande fall):

.....
(Underskrift)

(*) Sätt kryss i relevant ruta.
(**) Ange den komponent som anmälan avser."

Artikel 3

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

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

Utfärdad i Bryssel den 13 juni 2002.

På kommissionens vägnar
Loyola DE PALACIO
Vice ordförande

BILAGA

"BILAGA I B

KRAV I FRÅGA OM KONSTRUKTION, PROVNING, INSTALLATION OCH BESIKTNING

I syfte att bevara kompatibiliteten hos den programvara och utrustning som beskrivs i denna bilaga har vissa förkortningar, termer och dataprogrammeringsuttryck behållits på originalspråket, dvs. på engelska. I informationssyfte och för att förbättra läsbarheten har dock ordagranna svenska översättningar införts i den löpande texten, och de engelska uttrycken har givits inom parentes efter den svenska översättningen.

INNEHÅLL

I. DEFINITIONER

I denna bilaga används följande beteckningar med de betydelser som här anges:

a) **Aktivering**:

Läge där färdskrivaren är helt i drift och alla funktioner används, inbegripet säkerhetsfunktionerna.

Vid aktivering av färdskrivaren skall ett verkstadskort användas och dess PIN-kod anges.

b) **Autentisering**:

Funktion avsedd att upprätta och kontrollera en angiven identitet.

c) **Autenticitet**:

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

d) **Inbyggd provning (built-in-test – BIT)**:

Provning som utförs på begäran och utlöses av en operatör eller extern anordning.

e) **Kalenderdag**:

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

f) **Kalibrering**:

Uppdatering eller bekräftelse av de fordonsuppgifter som skall lagras i dataminnet. Dessa uppgifter inbegriper fordonsidentifiering (fordonets identifieringsnummer och 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).

När färdskrivaren kalibreras skall ett verkstadskort användas.

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.

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 som används för att åtskilja de kort som utfärdats åt ett företag eller ett organ som har rätt att få flera färdskrivarkort utfärdade. Det enskilda företaget eller organet kan identifieras med hjälp av de första 13 tecknen i kortnumret.

i) **Index för förnyelse av kort**:

Det 16:e alfanumeriska tecknet i ett kortnummer som ökar varje gång ett färdskrivarkort förnyas.

j) **Index för ersättning av kort**:

Det 15:e alfanumeriska tecknet i ett kortnummer som ökar varje gång ett färdskrivarkort ersätts.

k) **Fordonets karakteristiska koefficient**:

Det numeriska tal som anger värdet för den utgående signal som skickas av den del av fordonet som förenar fordonet med färdskrivaren (växellådans utgående axel eller fordonets hjul) medan fordonet tillryggalägger en sträcka av en kilometer under normala provningsförhållanden (se kapitel VI punkt 5 i denna bilaga). Den karakteristiska koefficienten uttrycks i impulser per kilometer (w = … imp/km).

l) **Företagskort**:

Ett färdskrivarkort som utfärdas av myndigheterna i en medlemsstat till en ägare eller nyttjanderättsiinnehavare av fordon som utrustats med färdskrivare.

Företagskortet gör det möjligt att identifiera företaget och att visa, överföra och skriva ut data som finns lagrade i en färdskrivare som detta företag har låst.

m) **Färdskrivarens konstant**:

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

n) **Sammanhängande körtid beräknas i färdskrivaren enligt följande** ([1]):

En viss förares aktuella sammanlagda körtid sedan utgången av hans 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 om minst 15 minuter). Vid de berörda beräkningarna tas efter behov hänsyn till tidigare aktiviteter som finns lagrade på förarkortet. Om föraren inte har satt i sitt kort bygger de berörda beräkningarna på de registreringar i dataminnet som avser den innevarande period då inget kort satts i och motsvarande kortplats.

o) **Kontrollkort**:

Ett färdskrivarkort som utfärdats av myndigheterna i en medlemsstat till en nationell behörig kontrollmyndighet.

Genom kontrollkortet kan kontrollorganet och eventuellt den som utfört kontrollen identifieras och det gör det möjligt att få tillgång till data som lagras i dataminnet eller på förarkorten för att läsa, skriva ut, och/eller överföra dem.

p) **Sammanlagd avbrottstid beräknas i färdskrivaren enligt följande** ([1]):

Den sammanlagda tiden för avbrott från körtiden beräknas som en viss förares innevarande sammanlagda tider av tillgänglighet (AVAILABILITY) eller rast/vila (BREAK/REST) eller okända (UNKNOWN) ([2]) tider av 15 minuter eller mer, sedan slutet av hans 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 om minst 15 minuter).

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

Om föraren inte har satt i sitt kort, bygger de berörda beräkningarna på de registreringar i dataminnet som avser den innevarande period där inget kort satts i och motsvarande kortplats.

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 datamängd som gör det möjligt för mottagaren av datamängden att bekräfta datamängdens autenticitet och integritet.

s) **Överföring**:

Kopiering och digital signatur av samtliga eller en del av en data som finns lagrade i fordonets dataminne eller färdskrivarkortets minne.

Överföringen får inte ändra eller radera lagrade data.

([1]) Detta sätt att beräkna sammanhängande körtid och sammanlagd avbrottstid använder färdskrivaren för beräkning av varning med avseende på sammanlagd körtid. Det påverkar inte den juridiska tolkning som skall göras av dessa tider.

([2]) Okända (UNKNOWN) perioder motsvarar de perioder där förarkortet inte var isatt i en färdskrivare och för vilka ingen manuell angivelse av föraraktivitet gjordes.

t) **Förarkort**:

Ett färdskrivarkort som myndigheterna i en medlemsstat utfärdar till en viss förare.

Genom förarkortet kan föraren identifieras och det gör det möjligt att lagra data om förarens aktiviteter.

u) **Däckens effektiva omkrets**:

Genomsnittsvärdet för de sträckor som tillryggalagts av de hjul som förflyttar fordonet (drivhjul) under loppet av ett fullt varv. Uppmätning av dessa avstånd skall ske under normala provningsförhållanden (se kapitel VI.5) och uttrycks i formen: 1 = … mm. Fordonstillverkare får ersätta uppmätningen av dessa avstånd med en teoretisk beräkning där axeltrycket i fordon utan last i körklart skick beaktas ([1]). Metoderna för denna teoretiska beräkning skall godkännas av en behörig myndighet i en medlemsstat.

v) **Händelse**:

Onormal drift som upptäcks av färdskrivaren och som kan bero på försök till bedrägeri.

w) **Fel**:

Onormal drift som upptäcks av färdskrivaren och som kan bero på att den inte fungerar riktigt eller inte fungerar alls.

x) **Installation**:

Montering av en färdskrivare i ett fordon.

y) **Rörelsesensor**:

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

z) **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.

aa) **Omfattas ej (out of scope)**:

När användning av färdskrivare inte krävs enligt bestämmelserna i rådets förordning (EEG) nr 3820/85.

bb) **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 av den 10 februari om montering och användning av hastighetsbegränsande anordningar i vissa kategorier av motorfordon inom gemenskapen ([2]).

cc) **Periodisk besiktning**:

En uppsättning åtgärder för att kontrollera att färdskrivaren fungerar korrekt och att dess inställningar överensstämmer med fordonsparametrarna.

dd) **Skrivare**:

Komponent i färdskrivaren som tillhandahåller utskrifter av lagrade data.

ee) **Färdskrivare**:

All utrustning avsedd att installeras i vägfordon med uppgift att visa, registrera och automatiskt eller halvautomatiskt lagra detaljerad information om fordonets förflyttningar och om förarnas arbetspass.

([1]) Europaparlamentets och rådets direktiv 97/27/EG av den 22 juli 1997 om massa och dimensioner för vissa kategorier av motorfordon och släpvagnar till dessa fordon och om ändring av direktiv 70/156/EEG (EGT L 233, 25.8.1997, s. 1).

([2]) EGT L 57, 2.3.1992, s. 27.

ff) **Förnyelse**:

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

gg) **Reparation**:

All reparation av en rörelsesensor eller av en fordonsenhet som förutsätter urkoppling av strömtillförseln, urkoppling av andra färdskrivarkomponenter, eller att den öppnas.

hh) **Ersättning**:

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.

ii) **Säkerhetscertifiering**:

Förfarandet för ett certifieringsorgan för informationsteknologisk säkerhet (ITSEC) ([1]) att intyga att den färdskrivare (eller den komponent) eller det färdskrivarkort som undersöks uppfyller säkerhetskraven i bilaga 10 om allmänna säkerhetsmål.

jj) **Självprovning**:

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

kk) **Färdskrivarkort**:

Ett smartkort som är avsett att användas med färdskrivaren. Färdskrivarkort gör det möjligt för färdskrivaren att fastställa kortinnehavarens identitet (eller identitetsgrupp) och att överföra och lagra data. Färdskrivarkorten kan delas upp i följande typer:

— Förarkort.

— Kontrollkort.

— Verkstadskort.

— Företagskort.

ll) **Typgodkännande**:

Ett förfarande för medlemsstaten för att intyga att den färdskrivare (eller den komponent) eller det färdskrivarkort som undersöks uppfyller kraven i denna förordning.

mm) **Däcksdimension**:

Angivelse av däckens dimensioner (drivhjul) enligt direktiv 92/23/EEG ([2]).

nn) **Fordonsidentifiering**:

Nummer för identifiering av fordonet: Fordonets registreringsnummer (VRN) med angivelse av registrerande medlemsstat och fordonets chassinummer (VIN) ([3]).

oo) **Fordonsenhet**:

Färdskrivaren förutom rörelsesensor och anslutningskablar till rörelsesensorn. Fordonsenheten kan antingen vara en enda enhet eller flera enheter som fördelas i fordonet, så länge som den överensstämmer med säkerhetskraven i denna förordning.

([1]) Rådets rekommendation 95/144/EG av den 7 april 1995 om gemensamma kriterier för utvärdering av informationsteknologisk säkerhet (EGT L 93, 26.4.1995, s. 27).
([2]) EGT L 129, 14.5.1992, s. 95.
([3]) Direktiv 76/114/EEG (EGT L 24, 30.1.1976, s. 1).

pp) **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.

qq) **Verkstadskort**:

Ett färdskrivarkort som myndigheterna i en medlemsstat har utfärdat till en tillverkare av färdskrivare, en montör, en fordonstillverkare eller en verkstad, som har godkänts av denna medlemsstat.

Verkstadskortet identifierar kortinnehavaren och gör det möjligt att prova, kalibrera och/eller överföra data från färdskrivaren.

II. ALLMÄN BESKRIVNING AV OCH FUNKTIONER HOS FÄRDSKRIVAREN

000 Alla fordon som har utrustats med en färdskrivare som överensstämmer med bestämmelserna i denna bilaga måste inbegripa en hastighetsmätare och en vägmätare. Dessa funktioner får inbegripas i färdskrivaren.

1. **Allmän beskrivning**

Syftet med en färdskrivare är att registrera, lagra, visa, skriva ut och mata ut data om föraraktiviteter.

001 Färdskrivaren inbegriper kablar, en rörelsesensor och en fordonsenhet.

002 Fordonsenheten inbegriper en beräkningsenhet, ett dataminne, en klocka som visar realtid, två kortplatser för smartkort (förare och medförare), en skrivare, en display, en visuell varningsanordning, en kalibrerings-/överföringsanslutning, och en anordning för att mata in användarens uppgifter.

Färdskrivaren får kopplas till andra anordningar med hjälp av ytterligare anslutningar.

003 Inbegripande i eller koppling till färdskrivaren av en funktion, anordning eller anordningar, oavsett om de är godkända, skall inte påverka eller kunna påverka en korrekt och säker drift av färdskrivaren eller överensstämmelsen med bestämmelserna i förordningen.

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

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

Färdskrivaren registrerar och lagrar data i sitt dataminne 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]).

2. **Funktioner**

005 Färdskrivaren skall inbegripa följande funktioner:

— Övervakning av isättning och urtagning av kort.

— Mätning av hastighet och sträcka.

— Tidmätning.

— Övervakning av förarens aktiviteter.

— Övervakning av förarens status.

— Följande manuella angivelser av föraren:

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

  — Manuell angivelse av förarens aktiviteter.

  — Angivelse av särskilda omständigheter.

([1]) EGT L 281, 23.11.1995, s. 31.

— Hantering av företagslås.

— Övervakning av kontrollaktiviteter.

— Upptäckt av händelser och/eller fel.

— Inbyggd provning och självprovning.

— Avläsning av dataminnet.

— Registrering och lagring i dataminnet.

— Avläsning av färdskrivarkort.

— Registrering och lagring på färdskrivarkort.

— Visning.

— Utskrift.

— Varning.

— Överföring av data till externa media.

— Utgående data till ytterligare externa anordningar.

— Kalibrering.

— Tidsinställning.

3. **Driftlägen**

006 Färdskrivaren skall ha följande fyra driftlägen:

— Driftläge.

— Kontrolläge.

— Kalibreringsläge.

— Företagsläge.

007 Färdskrivaren skall ställa in följande driftlägen enligt det giltiga färdskrivarkort som sätts in i kortläsaren:

Driftlägen		Förarens öppning				
		Inget kort	Förarkort	Kontrollkort	Verkstadskort	Företagskort
Medförarens kortplats	Inget kort	Driftläge	Driftläge	Kontroll	Kalibrering	Företag
	Förarkort	Driftläge	Driftläge	Kontroll	Kalibrering	Företag
	Kontrollkort	Kontroll	Kontroll	Kontroll (*)	Driftläge	Driftläge
	Verkstadskort	Kalibrering	Kalibrering	Driftläge	Kalibrering (*)	Driftläge
	Företagskort	Företag	Företag	Driftläge	Driftläge	Företag (*)

008 (*) I dessa situationer skall färdskrivaren enbart använda det färdskrivarkort som satts in i förarens kortplats.

009 Färdskrivaren skall bortse från ogiltiga kort som införts, förutom visning, utskrift eller överföring av data från ett utgånget kort, som skall vara möjliga.

010 Alla funktioner som förtecknas i II.2. skall fungera i alla driftlägen med följande undantag:

— Kalibreringsfunktionen skall endast vara tillgänglig i kalibreringsläge.

— Funktionen för inställning av tid skall vara begränsad när kalibreringsläget inte är inställt.

— Förarens manuella angivelser skall endast vara möjliga i driftläge eller kalibreringsläge.

— Funktionen för hantering av företagslås skall endast vara tillgänglig i företagsläge.

— Funktionen för övervakning av kontrollaktiviteter skall endast vara i drift i kontrolläge.

— Överföringsfunktionen skall inte vara tillgänglig i driftläge (med undantag av bestämmelserna i krav 150).

011 Färdskrivaren skall kunna mata ut alla data till display-, skrivar- eller externa gränssnitt med följande undantag:

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

— I företagsläge skall data om föraren (kraven 081, 084 och 087) endast kunna matas ut för perioder som inte har låsts av ett annat företag (enligt identifiering genom de första 13 siffrorna i företagskortets nummer).

— När inget kort är isatt i färdskrivaren skall data om föraren kunna matas ut endast för den innevarande och de åtta föregående kalenderdagarna.

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 utbyts mellan rörelsesensorn och fordonsenheten, att skydda integriteten och autenticiteten hos data som utbyts mellan färdskrivaren och färdskrivarkorten, och att kontrollera integriteten och autenticiteten hos data som överförs.

012 För att systemsäkerheten skall kunna uppnås måste färdskrivaren uppfylla de krav som anges i de allmänna säkerhetsmålen för rörelsesensorer och fordonsenheter (tillägg 10).

III. KONSTRUKTIONS- OCH FUNKTIONSKRAV FÖR FÄRDSKRIVARE

1. **Övervakning av isättning och urtagning av kort**

013 Färdskrivaren skall övervaka kortläsarna för att upptäcka isättningar och urtagningar av kort.

014 När kortet sätts i skall färdskrivaren känna av huruvida det införda kortet är ett giltigt färdskrivarkort och i så fall identifiera korttypen.

015 Färdskrivaren skall utformas så att färdskrivarkortet låses i sitt läge när det sätts in på korrekt sätt i kortläsaren.

016 Färdskrivarkortet skall gå att ta ut endast när fordonet har stannat och efter det att relevanta data har lagrats på korten. Kortet kan tas ut endast efter aktivering av den som använder det.

2. **Mätning av hastighet och sträcka**

017 Denna funktion skall ständigt mäta och kunna tillhandahålla det vägmätarvärde som motsvarar den sammanlagda sträcka som fordonet har tillryggalagt.

018 Denna funktion skall ständigt mäta och kunna tillhandahålla fordonets hastighet.

019 Funktionen för mätning av hastigheten skall dessutom tillhandahålla informationen oavsett om fordonet är i rörelse eller om det stannat. Fordonet skall anses vara i rörelse så snart som funktionen upptäcker mer än 1 imp/sek under minst 5 sekunder från rörelsesensorn och i annat fall skall fordonet anses ha stannat.

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 skall uppfylla de krav i fråga om största tillåtna toleranser som anges i denna bilaga (kapitel III.2.1 och III.2.2).

2.1 ***Mätning av tillryggalagd vägsträcka***

020 Tillryggalagd sträcka får uppmätas och registreras antingen

— genom att körning framåt och bakåt slås samman, eller

— genom att endast körning framåt räknas.

021 Färdskrivaren skall mäta sträckor från 0 till 9 999 999,9 km.

022 Den uppmätta sträckan skall 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.

023 Uppmätta sträckor skall ha en upplösning av minst 0,1 km.

2.2 ***Hastighetsmätning***

024 Färdskrivaren skall mäta hastigheter från 0 till 220 km/h.

025 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 ingående variationer (däckvariationer, …),

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

skall 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).

Obs: Upplösningen på lagrade data ger en ytterligare tolerans av ± 0,5 km/h för hastigheter som lagras av färdskrivaren.

025a Hastigheten skall mätas korrekt inom de normala toleranserna inom två sekunder efter det att hastighetsändringen har avslutats, när hastigheten har ändrats med upp till 2 m/s^2.

026 Uppmätta hastigheter skall ha en upplösning av minst 1 km/h.

3. **Tidmätning**

027 Funktionen för tidmätning skall ständigt mäta och digitalt ange UTC- datum och UTC-tid.

028 UTC-datum och UTC-tid skall användas för datering i färdskrivarens alla funktioner (registrering, utskrifter, datautbyte, visning, …).

029 För att man skall kunna se lokal tid, skall det vara möjligt att ändra tidsskillnaden på det klockslag som displayen visar, med steg om halva timmar.

030 Tidsavvikelsen från UTC skall vara mindre än ± 2 sekunder per dag när det gäller typgodkännande.

031 Uppmätt tid skall ha en upplösning av minst 1 sekund.

032 Tidmätningen skall inte påverkas av externa avbrott av strömtillförseln på mindre än 12 månader när det gäller typgodkännande.

4. **Övervakning av förarens aktiviteter**

033 Denna funktion skall ständigt och separat övervaka en förares och en medförares aktiviteter.

034 Förarens aktiviteter skall delas upp i körning (DRIVING), tillgänglighet (WORK), tillgänglighet (AVAILABILITY), eller rast/vila (BREAK/REST).

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

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

037 När fordonet stannar skall arbete (WORK) väljas automatiskt för föraren.

038 Den första aktivitetsändring som sker inom 120 sekunder efter den automatiska omkopplingen till arbete (WORK) på grund av att fordonet stannar skall antas ha skett när fordonet stannar (och därmed sker eventuellt inte omkopplingen till arbete (WORK)).

039 Denna funktion skall mata ut aktivitetsändringar till registerfunktionerna med en upplösning av en minut.

040 För en viss kalenderminut skall hela minuten betraktas som körning (DRIVING) om någon körning (DRIVING) har skett inom denna minut.

041 För en viss kalenderminut skall hela minuten betraktas som körning (DRIVING) om någon körning (DRIVING) har skett både inom den närmast föregående och den närmast efterkommande minuten.

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

043 Denna funktion skall dessutom ständigt övervaka den sammanhängande körtiden och förarens sammanlagda avbrottstid.

5. **Övervakning av förarens status**

044 Denna funktion skall ständigt och automatiskt övervaka förarens status.

045 Körningsstatus 'flera förare' (CREW) skall väljas när två giltiga förarkort sätts in i färdskrivaren, körningsstatus 'ensam' (SINGLE) skall väljas i alla andra fall.

6. **Förarens manuella angivelser**

6.1 ***Angivelse av de platser där dagens arbetspass påbörjas och/eller avslutas***

046 Denna funktion skall göra det möjligt att ange de platser där dagens arbetspass påbörjas och/eller avslutas för en förare och/eller en medförare.

047 Platser definieras som landet och, där så är tillämpligt, regionen.

048 När ett förarkort (eller verkstadskort) tas ut skall färdskrivaren uppmana (med)föraren att ange 'den plats där dagens arbetspass avslutas'.

049 Färdskrivaren skall göra det möjligt att bortse från denna begäran.

050 Det skall vara möjligt att mata in de platser där dagens arbetsperioder påbörjas och/eller avslutas utan kort, eller vid andra tidpunkter än när kortet sätts in eller tas ut.

6.2 ***Manuell angivelse av förarens aktiviteter***

050a När förarkortet (eller verkstadskortet) sätts in, och endast då, skall färdskrivaren

— påminna kortinnehavaren om datum och tidpunkt då han tog ut kortet senast, och

— be kortinnehavaren ange om den aktuella isättningen av kortet är en fortsättning av dagens innevarande arbetspass.

Färdskrivaren skall göra det möjligt för kortinnehavaren att bortse från frågan utan att svara eller att svara jakande eller nekande.

— Om kortinnehavaren bortser från frågan skall färdskrivaren uppmana kortinnehavaren att ange 'den plats där dagens arbetspass påbörjas'. Färdskrivaren skall göra det möjligt att bortse från denna begäran. Om en plats anges skall den registreras i dataminnet och på färdskrivarkortet och hänföras till den tidpunkt då kortet sattes i.

— Om svaret är jakande eller nekande skall färdskrivaren uppmana kortinnehavaren att ange aktiviteterna manuellt, med datum och tidpunkt för påbörjande och avslutande, bland endast arbete (WORK), tillgänglighet (AVAILABILITY), eller rast/vila (BREAK/REST), som endast omfattar perioden från senaste urtagning av kort till aktuell isättning av kort, och utan att dessa aktiviteter kan överlappa varandra. Detta skall göras i enlighet med följande förfaranden:

  — Om kortinnehavaren svarar jakande på frågan, skall färdskrivaren uppmana kortinnehavaren att manuellt ange aktiviteterna i kronologisk ordning för perioden från senaste urtagning av kort till aktuell isättning. Förfarandet skall avslutas när sluttiden för en manuellt angiven aktivitet är densamma som tiden för isättningen av kortet.

  — Om kortinnehavaren svarar nekande på frågan skall färdskrivaren

    — uppmana kortinnehavaren att manuellt ange aktiviteterna i kronologisk ordning från tidpunkten för urtagning av kortet till tidpunkten för avslutande av berört arbetspass (eller av aktiviteterna för detta fordon om dagens arbetspass fortsätter på ett diagramblad). Färdskrivaren skall därför, innan kortinnehavaren manuellt kan slå in varje aktivitet, uppmana kortinnehavaren att ange om tidpunkten för avslutande av den senaste registrerade aktiviteten utgörs av slutet på ett föregående arbetspass (se anmärkning nedan).

      Obs: Om kortinnehavaren underlåter att ange när det föregående arbetspasset avslutades och manuellt anger en aktivitet vars sluttid är densamma som tiden för isättningen av kortet, skall färdskrivaren

      — anta att dagens arbetspass avslutades när den första viloperioden (REST) (eller återstående okänd (UNKNOWN) period) efter urtagning av kortet påbörjades, eller vid tidpunkten för urtagning av kortet om ingen viloperiod har angivits (och om ingen period fortfarande är okänd (UNKNOWN)),

      — anta att starttiden (se nedan) är densamma som tidpunkten för isättning av kortet,

      — fortsätta enligt nedan.

    — Därefter, om den tidpunkt då det berörda arbetspasset avslutades inte är densamma som den tidpunkt då kortet togs ut, eller om ingen plats för avslutande av dagens arbetspass angivits vid den tidpunkten, uppmana kortinnehavaren att 'bekräfta eller ange den plats där dagens arbetspass avslutades' (färdskrivaren skall göra det möjligt att bortse från denna begäran). Om en plats anges skall den registreras enbart på färdskrivarkortet och endast om den inte är densamma som den plats som angavs när kortet togs ut (om det hade satts i) och avser den tidpunkt då arbetspasset avslutades.

    — Därefter uppmana kortinnehavaren att 'ange en starttid' för dagens innevarande arbetspass (eller för aktiviteterna för det aktuella fordonet, om kortinnehavaren tidigare använde ett diagramblad under denna period), och uppmana kortinnehavaren att ange 'en plats där dagens arbetspass påbörjas' (färdskrivaren skall göra det möjligt att bortse från denna begäran). Om en plats anges skall den registreras på färdskrivarkortet och avse denna starttid. Om denna starttid är densamma som tidpunkten för isättningen av kortet skall platsen även registreras i dataminnet.

    — Därefter, om denna starttid skiljer sig från den tidpunkt då kortet sattes i, uppmana kortinnehavaren att ange aktiviteter i kronologisk ordning från denna starttid till den tidpunkt då kortet sattes i. Förfarandet skall avslutas när sluttiden för en manuellt angiven aktivitet är densamma som den tidpunkt då kortet sätts i.

  — Färdskrivaren skall sedan göra det möjligt för kortinnehavaren att ändra de aktiviteter som angivits manuellt, innan de bekräftas genom ett särskilt kommando, och sedan skall sådana ändringar inte längre vara möjliga.

  — De svar på den första frågan som åtföljs av angivelser om avsaknad av aktiviteter skall färdskrivaren tolka som att kortinnehavaren har bortsett från frågan.

Under hela detta förfarande skall färdskrivaren inte längre invänta angivelser under följande omständigheter:

— om ingen interaktion sker med färdskrivarens användargränssnitt under en minut (med en visuell, och eventuellt hörbar, varningssignal efter 30 sekunder), eller

— om kortet tas ut eller ett annat förarkort (eller verkstadskort) sätts in, eller

— så snart som fordonet är i rörelse.

I detta fall skall färdskrivaren bekräfta alla de angivelser som redan har gjorts.

6.3 ***Angivelse av särskilda omständigheter***

050b Färdskrivaren skall göra det möjligt för föraren att i realtid ange följande två särskilda omständigheter:

— omfattas ej (OUT OF SCOPE) (start, slut).

— transport med färja/tåg (FERRY/TRAIN CROSSING).

Transport med färja/tåg (FERRY/TRAIN CROSSING) får inte äga rum om omständigheten 'omfattas ej' (OUT OF SCOPE) inletts.

En inledd omständighet av typen 'omfattas ej' (OUT OF SCOPE) måste automatiskt avslutas av färdskrivaren om ett förarkort sätts i eller tas ut.

7. **Hantering av företagslås**

051 Denna funktion skall göra det möjligt att hantera de lås som ett företag har för att begränsa egen tillgång till data i företagsläge.

052 Företagslås utgörs av tidpunkt/datum för start (låsning) och tidpunkt/datum för avslutande (öppning) för identifiering av företaget enligt företagskortets nummer (vid låsning).

053 Låsning och öppning kan endast ske i realtid.

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

055 öppning skall ske automatiskt om ett annat företag låser.

055a När ett företag låser och det föregående låset var för samma företag kommer det att antas att det föregående låset inte har öppnats utan fortfarande är låst.

8. **Övervakning av kontrollaktiviteter**

056 Denna funktion skall övervaka visning (DISPLAYING), utskrift (PRINTING), fordonsenhet (VEHICLE UNIT) och överföring (DOWNLOADING) av data från kort, då detta sker i kontrolläge.

057 Denna funktion skall även övervaka kontroll av överskriden hastighet (OVER SPEEDING CONTROL) i kontrolläge. En kontroll av överskriden hastighet anses ha ägt rum när utskriften 'överskriden hastighet' i kontrolläge har sänts till skrivaren eller till displayen, eller när 'händelse- eller feldata' har överförts från fordonsenhetens (VU) dataminne.

9. **Upptäckt av händelser och/eller fel**

058 Denna funktion skall upptäcka följande händelser och/eller fel:

9.1 ***Händelsen 'isättning av ett ogiltigt kort'***

059 Denna händelse skall utlösas om ett ogiltigt kort sätts i och/eller när ett infört giltigt kort slutar att gälla.

9.2 ***Händelsen 'kortkonflikt'***

060 Denna händelse skall utlösas om någon av de kombinationer av giltiga kort som är markerade med X i följande 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

9.3 ***Händelsen 'överlappning av tider'***

061 Denna funktion skall utlösas när datum/tidpunkt för den senaste urtagningen av ett förarkort enligt detta kort ligger senare än aktuellt datum/tidpunkt i den färdskrivare i vilken kortet införts.

9.4 ***Händelsen 'körning utan korrekt kort'***

062 Denna händelse skall utlösas när någon av kombinationerna av färdskrivarkort som är markerade med X i följande tabell uppstår, när föraraktiviteten ändras till körning (DRIVING), eller vid ändring av driftläge när föraraktiviteten är körning (DRIVING):

Körning utan korrekt kort		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

9.5 ***Händelsen 'isättning av kort vid körning'***

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

9.6 ***Händelsen 'senaste kortanvändning ej korrekt avslutad'***

064 Denna händelse skall utlösas om färdskrivaren vid isättning av ett kort upptäcker att föregående kortanvändning, trots bestämmelserna i kapitel III. 1, inte har avslutats korrekt (kortet har tagits ut innan alla relevanta data har lagrats på det). Denna händelse gäller endast förarkort och verkstadskort.

9.7 ***Händelsen 'hastighetsöverträdelse'***

065 Denna händelse skall utlösas vid varje hastighetsöverträdelse.

9.8 ***Händelsen 'avbrott av strömtillförsel'***

066 Denna händelse skall utösas när kalibreringsläget inte är inställt om strömtillförseln i rörelsesensorn och/eller fordonsenheten är avbruten under mer än 200 millisekunder. Tröskeln för avbrottet skall fastställas av tillverkaren. Sänkt strömtillförsel på grund av att fordonets motor startas skall inte utlösa denna händelse.

9.9 ***Händelsen 'fel i rörelsedata'***

067 Denna händelse skall utlösas vid avbrott av det normala dataflödet mellan rörelsesensorn och fordonsenheten och/eller vid integritetsfel eller autentiseringsfel under utbyte av data mellan rörelsesensorn och fordonsenheten.

9.10 ***Händelsen 'försök till säkerhetsöverträdelse'***

068 Denna händelse skall utlösas vid varje övrig händelse som påverkar säkerheten i rörelsesensorn och/eller fordonsenheten, i enlighet med de allmänna säkerhetsmålen för dessa komponenter när kalibreringsläget inte är inställt.

9.11 ***Kortfel***

069 Denna händelse skall utlösas om ett fel på ett färdskrivarkort uppstår vid drift.

9.12 ***Färdskrivarfel***

070 Denna händelse skall utlösas vid något av följande fel om kalibreringsläget inte är inställt:

— Internt fel i fordonsenheten (VU).

— Skrivarfel.

— Displayfel.

— Överföringsfel.

— Sensorfel.

10. **Inbyggd provning och självprovning**

071 Färdskrivaren skall upptäcka fel genom självprovning och inbyggd provning, i enlighet med följande tabell:

Enhet som provas	Självprovning	Inbyggd provning
Programvara		Integritet
Dataminne	Tillträde	Tillträde, dataintegritet
Kortläsare	Tillträde	Tillträde
Tangentbord		Manuell kontroll
Skrivare	(Upp till tillverkaren)	Utskrift
Display		Visuell kontroll
Överföring (utförs endast vid överföring)	Korrekt drift	
Sensor	Korrekt drift	Korrekt drift

11. **Avläsning av dataminne**

072 Färdskrivaren skall kunna läsa alla data som finns lagrade i dess dataminne.

12. **Registrering och lagring i dataminne**

I detta stycke används följande beteckningar med de betydelser som här anges:

— 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 isättning och urtagning av kort, och 256 aktivitetsändringar. ’365 dagar’ inbegriper därför åtminstone 2 190 (med)förare, 2 190 cykler med isättning och urtagning av kort, och 93 440 aktivitetsändringar.

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

— Vägmätarvärden registreras med en upplösning av en kilometer.

— Hastigheter registreras med en upplösning av en km/h.

073 Data som finns lagrade i dataminnet skall inte påverkas av externa avbrott av strömtillförseln på mindre än 12 månader när det gäller typgodkännande.

074 Färdskrivaren skall i sitt dataminne direkt eller indirekt kunna registrera och lagra följande:

12.1 ***Data för identifiering av utrustning***

12.1.1 *Data för identifiering av fordonsenhet*

075 Det skall gå att lagra följande data för identifiering av fordonsenheter i färdskrivarens minne:

— Tillverkarens namn.

— Tillverkarens adress.

— Delnummer.

— Serienummer.

— Programvaruversionens nummer.

— Datum för installation av programvaruversionen.

— Utrustningens tillverkningsår.

— Typgodkännandenummer.

076 Tillverkaren av fordonsenheter registrerar och lagrar data för identifiering av fordonsenheter permanent, utom när det gäller programvarudata och typgodkännandenummer, som får ändras om programvaran uppgraderas.

12.1.2 *Data för identifiering av rörelsesensor*

077 Det skall gå att lagra följande identifieringsdata i rörelsesensorns minne:

— Tillverkarens namn.

— Delnummer.

— Serienummer.

— Typgodkännandenummer.

— Inbyggd identifiering av säkerhetskomponent (exempelvis delnummer på internt chip eller intern processor).

— Identifiering av operativsystem (exempelvis nummer på programvaruversionen).

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

079 Det skall gå att registrera och lagra följande data för identifiering av den för närvarande kopplade rörelsesensorn i fordonsenhetens dataminne:

— Serienummer.

— Typgodkännandenummer.

— Datum för första hopkoppling.

12.2 ***Säkerhetskomponenter***

080 Det skall gå att lagra följande säkerhetskomponenter i färdskrivaren:

— Europeisk kryptering med öppen kod.

— Intyg från medlemsstaten.

— Utrustningsintyg.

— Privat kod.

Tillverkaren av fordonsenheten skall föra in färdskrivarens säkerhetskomponenter i färdskrivaren.

12.3 ***Övervakning av isättning och urtagning av kort***

081 För varje cykel med isättning och urtagning av förarkort eller verkstadskort i utrustningen skall färdskrivaren registrera och lagra följande uppgifter i sitt dataminne:

— Kortinnehavarens efternamn och förnamn sådana de lagrats på kortet.

— Kortnummer, utfärdande medlemsstat och sista giltighetsdatum sådana de lagrats på kortet.

— Datum och tidpunkt för isättning.

— Vägmätarvärde när kortet sattes in.

— Den kortplats som kortet sätts in i.

— Datum och tidpunkt för urtagning.

— Vägmätarvärde när kortet togs ut.

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

  — Fordonets registreringsnummer (VRN) och registrerande medlemsstat.

  — Datum och tidpunkt för urtagning av kortet.

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

082 Det skall gå att lagra dessa data i dataminnet i minst 365 dagar.

083 När lagringskapaciteten har utnyttjats till fullo skall nya data ersätta de data som är äldst.

12.4 ***Data om föraraktiviteter***

084 Färdskrivaren skall när föraren och/eller medföraren ändrar aktivitet, och/eller när förarstatusen ändras, och/eller när ett förarkort eller verkstadskort sätts in eller tas ut, registrera och lagra följande i sitt dataminne:

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

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

— Kortets status i den berörda kortplatsen (isatt (INSERTED), ej isatt (NOT INSERTED)) (Se anmärkning).

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

— Datum och tidpunkt för ändringen.

Obs: Isatt (INSERTED) innebär att ett giltigt förarkort eller verkstadskort har satts in i kortplatsen. Ej insatt (NOT INSERTED) innebär motsatsen, dvs. att något giltigt förarkort eller verkstadskort inte har satts in i kortplatsen (exempelvis har ett företagskort eller inget kort alls satts in).

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

085 Det skall gå att lagra föraraktivitetsdata i dataminnet i minst 365 dagar.

086 När lagringskapaciteten har utnyttjats till fullo skall nya data ersätta de data som är äldst.

12.5 ***Platser där dagens arbetspass påbörjas och/eller avslutas***

087 Färdskrivaren skall, när en (hjälp)förare kommer till den plats där dagens arbetspass påbörjas eller avslutas, registrera och lagra följande uppgifter i sitt dataminne:

— I förekommande fall, (med)förarens kortnummer och medlemsstat som utfärdat kortet.

— Datum och tidpunkt för angivelsen (eller datum/tidpunkt för angivelsen när den görs under förfarandet för manuell angivelse).

— Typ av angivelse (påbörjande eller avslutande, angivelsevillkor).

— Det land och den region som anges.

— Fordonets vägmätarställning.

088 Det skall gå att lagra data om påbörjande och/eller avslutande av dagens arbetspass i minst 365 dagar i dataminnet (under förutsättning att en förare gör två registreringar per dygn).

089 När lagringskapaciteten har utnyttjats till fullo skall nya data ersätta de data som är äldst.

12.6 ***Vägmätardata***

090 Färdskrivaren skall vid midnatt varje kalenderdag registrera fordonets vägmätarställning och motsvarande datum i sitt dataminne.

091 Det skall gå att lagra vägmätarvärden vid midnatt i minst 365 dagar.

092 När lagringskapaciteten har utnyttjats till fullo skall nya data ersätta de data som är äldst.

12.7 ***Detaljerade hastighetsdata***

093 Färdskrivaren skall 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 varit i rörelse.

12.8 ***Händelsedata***

För händelsedata skall tiden registreras med en upplösning av en sekund.

094 Färdskrivaren skall i sitt dataminne registrera och lagra följande data för varje händelse som upptäcks i enlighet med följande lagringsregler:

Händelse	Lagringsregler	Data som skall registreras per händelse
Kortkonflikt	— De senaste tio händelserna	— Datum och tidpunkt för händelsens början — Datum och tidpunkt för händelsens slut — Korttyp, kortnummer och medlemsstat som utfärdat de två kort som orsakat konflikten
Körning utan korrekt kort	— Den längsta händelsen för vart och ett av de senaste tio dygn händelsen inträffat — De fem längsta händelserna under de senaste 365 dygnen	— Datum och tidpunkt för händelsens början — Datum och tidpunkt för händelsens slut — Korttyp, kortnummer och medlemsstat som utfärdat kort som satts in vid händelsens början och/eller slut — Antal liknande händelser samma dag
Isättning av kort under körning	— Den senaste händelsen för vart och ett av de senaste tio dygn händelsen inträffat	— Datum och tidpunkt för händelsens slut — Korttyp, kortnummer och utfärdande medlemsstat — Antal liknande händelser samma dag
Senaste kortanvändning ej korrekt avslutad	— De senaste tio händelserna	— Datum och tidpunkt för isättning av kortet — Korttyp, kortnummer och utfärdande medlemsstat — Data om senaste användning enligt kortet: — Datum och tidpunkt för isättning av kort — Fordonets registreringsnummer (VRN) och registrerande medlemsstat
Hastighetsöverträdelse ([1])	— Den mest allvarliga händelsen under vart och ett av de senaste tio dygn händelsen inträffat (dvs. den med högsta genomsnittliga hastighet) — De fem mest allvarliga händelserna under de senaste 365 dygnen — Den första händelse 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 — Förarens korttyp, kortnummer och utfärdande medlemsstat (i förekommande fall) — Antal liknande händelser samma dag

Händelse	Lagringsregler	Data som skall registreras per händelse
Avbrott av strömtillförsel ([2])	— Den längsta händelsen för vart och ett av de senaste tio dygn händelsen inträffat — De fem längsta händelserna under de senaste 365 dygnen	— Datum och tidpunkt för händelsens början — Datum och tidpunkt för händelsens slut — Korttyp, kortnummer och medlemsstat som utfärdat kort som satts in vid händelsens början och/eller slut — Antal liknande händelser samma dag
Fel i rörelsedata	— Den längsta händelsen för vart och ett av de senaste tio dygn händelsen inträffat — De fem längsta händelserna under de senaste 365 dygnen	— Datum och tidpunkt för händelsens början — Datum och tidpunkt för händelsens slut — Korttyp, kortnummer och medlemsstat som utfärdat kort som satts in 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 och medlemsstat som utfärdat kort som satts in vid händelsens början och/eller slut — Händelsetyp

095 ([1]) Färdskrivaren skall dessutom registrera och lagra följande uppgifter i sitt dataminne:
— Datum och tidpunkt för senaste kontroll av hastighetsöverträdelse (OVER SPEEDING CONTROL).
— Datum och tidpunkt för första hastighetsöverträdelse efter denna kontroll av hastighetsöverträdelse (OVER SPEEDING CONTROL).
— Antal hastighetsöverträdelsehändelser sedan senaste kontroll av hastighetsöverträdelse (OVER SPEEDING CONTROL).
([2]) Dessa data får endast registreras då strömtillförseln återkopplas och tidpunkter får anges på minuten när.

12.9 ***Feldata***

För feldata skall tiden registreras med en upplösning av en sekund.

096 Färdskrivaren skall i sitt dataminne söka registrera och lagra följande data för varje fel som upptäcks i enlighet med följande lagringsregler:

Fel	Lagringsregler	Data som skall registreras per fel
Kortfel	— De tio senaste förarkortsfelen	— Datum och tidpunkt för felets början — Datum och tidpunkt för felets slut — Korttyp, kortnummer och utfärdande medlemsstat
Färdskrivarfel	— De tio senaste felen för varje typ av fel — Det första felet efter senaste kalibrering	— Datum och tidpunkt för felets början — Datum och tidpunkt för felets slut — Typ av fel — Korttyp, kortnummer och medlemsstat som utfärdat kort som satts in vid felets början och/eller slut

12.10 ***Kalibreringsdata***

097 Färdskrivaren skall registrera och lagra data med avseende på följande i sitt dataminne:

— Kända kalibreringsparametrar vid aktivering.

— Första kalibrering efter aktivering.

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

— De fem senaste kalibreringarna (om flera kalibreringar görs under en kalenderdag skall endast den sista kalibreringen det dygnet lagras).

098 Följande data skall registreras för var och en av följande kalibreringar:

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

— Verkstadens namn och adress.

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

— 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).

099 Rörelsesensorn skall registrera följande data om installationen av rörelsesensorn och lagra dem i:

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

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

12.11 ***Data om tidsinställning***

100 Färdskrivaren skall registrera och lagra data med avseende på följande i sitt dataminne:

— Senaste tidsinställning.

— De fem största tidsinställningarna sedan senaste kalibrering

utförda i kalibreringsläge vid annat än normal kalibrering (def. f).

101 Följande data skall registreras för var och en av följande tidsinställningar:

— Datum och tidpunkt, gammalt värde.

— Datum och tidpunkt, nytt värde.

— Verkstadens namn och adress.

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

12.12 ***Data om kontrollaktiviteter***

102 Färdskrivaren skall i sitt dataminne registrera och lagra följande data med avseende på de senaste 20 kontrollaktiviteterna:

— 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).

103 Vid överföring skall även datum för tidigaste och senaste nedladdade dagar registreras.

12.13 ***Data om företagslås***

104 Färdskrivaren skall i sitt dataminne registrera och lagra följande data med avseende på de 20 senaste företagslåsningarna:

— Datum och tidpunkt för låsning.

— Datum och tidpunkt för öppning.

— Företagskortsnummer och medlemsstat som utfärdat kortet.

— Företagets namn och adress.

12.14 ***Överföringsdata***

105 Färdskrivaren skall i sitt minne registrera och lagra följande data med avseende på senaste dataöverföring till externa media i företags- eller kalibreringsläge:

— Datum och tidpunkt för överföringen.

— Företagskortnummer eller verkstadskortnummer och medlemsstat som utfärdat kortet.

— Företagets eller verkstadens namn.

12.15 ***Data om särskilda omständigheter***

105a Färdskrivaren skall i sitt dataminne registrera följande data med avseende på särskilda omständigheter:

— Datum och tidpunkt för angivelsen.

— Typ av särskild omständighet.

105b Det skall 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 skall nya data ersätta de data som är äldst.

13. **Avläsning av färdskrivarkort**

106 Färdskrivaren skall i förekommande fall kunna läsa av nödvändiga data från färdskrivarkorten för att

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

— kontrollera att den senaste användningen av kortet 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 förarkort till externa media.

107 Vid avläsningsfel skall färdskrivaren högst tre gånger pröva samma läskommando, och om detta misslyckas skall den förklara kortet felaktigt och ogiltigt.

14. **Registrering och lagring på färdskrivarkort**

108 Färdskrivaren skall ställa in data om kortanvändning på förarkortet eller verkstadskortet omedelbart efter det att kortet satts in.

109 Färdskrivaren skall uppdatera de data som lagras på giltiga förar-, provnings- och/eller kontrollkort med alla nödvändiga data för den period då kortet är isatt och som avser kortinnehavaren. De data som lagras på dessa kort specificeras i kapitel IV.

109a Färdskrivaren skall uppdatera de data om föraraktivitet och plats (i enlighet med kapitel IV.5.2.5 och 5.2.6), som finns lagrade på giltiga förarkort eller verkstadskort, med de data om aktivitet och plats som kortinnehavaren anger manuellt.

110 Uppdateringen av färdskrivarkortsdata skall, vid behov och med hänsyn till kortets faktiska lagringskapacitet, ske på så sätt att senaste data ersätter äldsta data.

111 Vid skrivfel skall färdskrivaren högst tre gånger pröva samma skrivkommando, och om detta misslyckas skall den förklara kortet felaktigt och ogiltigt.

112 Innan färdskrivaren ger tillbaka ett förarkort, och efter det att alla relevanta data har lagrats på kortet, skall den återställa data om kortanvändningen.

15. **Display**

113 Displayen skall innefatta minst 20 tecken.

114 Minsta teckenstorlek skall vara en höjd på 5 mm och en bredd på 3,5 mm.

114a Displayen skall stödja teckenmängderna för Latin1 och grekiska enligt ISO 8859 del 1 och 7, i enlighet med kapitel 4 i tillägg 1 'Teckenmängder'. Förenklade tecken får användas (exempelvis får tecken med accent visas utan accent, och gemener får ersättas med versaler).

115 Displayen skall vara försedd med lämplig belysning som inte bländar.

116 Tecknen skall vara synliga utanför färdskrivaren.

117 Färdskrivaren skall kunna visa följande:

— Feldata.

— 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.

118 Färdskrivarens display skall 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.

119 Displayen skall alltid vara på (ON) när fordonet är i rörelse.

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

Displayformatet anges i tillägg 5.

15.1 ***Automatiskt visade uppgifter***

121 När ingen annan information behöver visas skall färdskrivaren automatiskt visa följande:

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

— Driftläge.

— Förarens och medförarens innevarande aktiviteter.

— Följande information om föraren:

— Om hans aktuella aktivitet är körning (DRIVING), hans aktuella körningstid och hans aktuella sammanlagda avbrottstid.

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

— Följande information om medföraren:

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

122 Visningen av data för varje förare skall vara klar, enkel och otvetydig. I de fall där informationen om föraren och medföraren inte kan visas samtidigt skall färdskrivaren automatiskt visa informationen om föraren och göra det möjligt för användaren att visa informationen om medföraren.

123 I de fall där displaybredden inte gör det möjligt att automatiskt visa driftläget skall färdskrivaren kort visa det nya driftläget när det ändras.

124 Färdskrivaren skall kort visa kortinnehavarens namn då kortet sätts in.

124a När omständigheten 'omfattas ej' (OUT OF SCOPE) påbörjas måste displayen med hjälp av relevant piktogram visa att omständigheten har påbörjats (förarens innevarande aktivitet behöver inte visas samtidigt).

15.2 ***Visade varningar***

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

15.3 ***Tillträde till meny***

126 Färdskrivaren skall tillhandahålla nödvändiga kommandon genom en lämplig menystruktur.

15.4 ***Övrig visad information***

127 Det skall vara möjligt att på begäran visa följande:

— UTC-datum och UTC-tid.

— Driftläge (om det inte visas automatiskt).

— Förarens sammanhängande körningstid och sammanlagda avbrottstid.

— Medförarens sammanhängande körningstid och sammanlagda avbrottstid.

— Förarens sammanlagda körningstid för föregående och innevarande vecka.

— Medförarens sammanlagda körningstid för föregående och innevarande vecka.

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

128 Innehållet i utskrifterna skall visas i en följd, rad för rad. Om displaybredden är mindre än 24 tecken skall användaren få komplett information på lämpligt sätt (flera rader, rullning, …). De utskriftsrader som är avsedda för handskriven information behöver inte visas.

16. **Utskrift**

129 Det skall gå att skriva ut information från färdskrivarens dataminne och/eller från färdskrivarkorten i enlighet med följande sex utskrifter:

— Daglig utskrift från kort av föraraktiviteter.

— Daglig utskrift 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.

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 sex ovan nämnda utskrifterna.

130 'Daglig utskrift från kort av föraraktiviteter' och 'Utskrift från kort av händelser och fel' skall endast finnas tillgängliga om ett förarkort eller ett verkstadskort sätts in i färdskrivaren. De data som finns på det berörda kortet skall uppdateras av färdskrivaren innan utskriften inleds.

131 För att tillhandahålla 'Daglig utskrift från kort av föraraktiviteter' eller 'Utskrift från kort av händelser och fel', skall färdskrivaren

— antingen automatiskt välja förarkort eller verkstadskort om endast ett av dess kort har satts in,

— eller ge ett kommando om val av källkort eller av kort i förarens kortplats, om två av dessa kort har satts i färdskrivaren.

132 Skrivaren skall kunna skriva ut 24 tecken per rad.

133 Minsta teckenstorlek skall vara en höjd på 2,1 mm och en bredd på 1,5 mm.

133a Skrivaren skall stödja teckenmängderna för Latin1 och grekiska enligt ISO 8859 del 1 och 7, i enlighet med kapitel 4 i tillägg 1 'Teckenmängder'.

134 Skrivarna skall kunna tillhandahålla dessa utskrifter med en skärpa som utesluter tvetydighet.

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

136 Det papper som används i färdskrivaren skall vara försett med giltigt typgodkännandemärke och angivelse av typ(er) av färdskrivare som det får användas med. Utskrifterna skall vara klart läsbara och identifierbara under minst ett år under normala lagringsvillkor, med avseende på ljusintensitet, luftfuktighet och temperatur.

137 Det skall även gå att lägga till handskrivna anmärkningar, exempelvis förarens namnteckning, i dessa handlingar.

138 Om papperet tar slut vid utskrift skall färdskrivaren, när papperet har fyllts på, börja om från början i utskriften eller fortsätta utskriften med en otvetydig hänvisning till den föregående delen.

17. **Varningar**

139 Färdskrivaren skall varna föraren när den upptäcker en händelse eller ett fel.

140 Varning om händelsen avbrott av strömtillförsel får uppskjutas till det att strömmen åter kopplats på.

141 Färdskrivaren skall varna föraren 15 minuter före och vid den tidpunkt då den sammanhängande körtiden överskrider 4 timmar och 30 minuter.

142 Varningarna skall vara visuella. Ljudvarningar får också ges utöver de visuella varningarna.

143 Användaren skall tydligt kunna urskilja de visuella varningarna, som skall vara placerade i hans synfält och vara tydligt läsbara både dag och natt.

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

145 I det senare fallet skall färdskrivaren vara försedd med symbolen 'T' som är gul eller orange.

146 Varningarna skall vara minst 30 sekunder långa, om inte användaren bekräftar dem genom att trycka på valfri knapp på färdskrivaren. Den första bekräftelsen får inte radera ut den visning av orsaken till varningen som anges i nästa stycke.

147 Orsaken till varningen skall visas på färdskrivaren och vara synlig tills det att användaren bekräftar den med hjälp av en särskild tangent eller ett kommando i färdskrivaren.

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

18. **Överföring av data till externa media**

149 Det skall 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 skall uppdateras av färdskrivaren innan utskriften inleds.

150 Dessutom skall färdskrivaren i alla driftlägen, som tillvalsfunktion, kunna överföra data genom en annan anslutning till ett företag som har autentiserats genom denna anslutning. I detta fall skall alla tillträdesrättigheter till data i företagsläge tillämpas på denna överföring.

151 Överföringen får inte påverka eller ta bort lagrade data.

Det elektriska gränssnittet för kalibrerings-/överföringsanslutningen anges i tillägg 6.

Överföringsprotokoll anges i tillägg 7.

19. **Utgående data till ytterligare externa anordningar**

152 Om färdskrivaren inte inbegriper funktioner för visning av hastighet och/eller tillryggalagd sträcka skall den ge utgående signal(er) för att göra det möjligt att visa fordonets hastighet (hastighetsmätare) och/eller den sammanlagda sträcka som fordonet har tillryggalagt (vägmätare).

153 Fordonsenheten skall även kunna mata ut följande data med hjälp av en särskild seriell anslutning som är oberoende av en frivillig CAN-bus anslutning (ISO 11898 Vägfordon – Datakommunikation, hög hastighet – Kommunikation enligt CAN), för att göra det möjligt för elektroniska anordningar som har installerats i fordonet att behandla dem:

— Aktuellt UTC-datum och aktuell UTC-tid.

— Fordonets hastighet.

— Av fordonet tillryggalagd sträcka.

— Vald förar- och medföraraktivitet.

— Information om huruvida något färdskrivarkort för närvarande är isatt i förarens kortplats och i medförarens kortplats och (i förekommande fall) information om motsvarande kort (kortnummer och utfärdande medlemstat).

Övriga data får också matas ut utöver denna minsta tillåtna förteckning.

När fordonets tändning är på (ON) skall dessa data sändas kontinuerligt. När fordonets tändning är av (OFF) skall minst en ändring av förar- eller medföraraktivitet och/eller en isättning eller urtagning av ett färdskrivarkort ge motsvarande utgående data. Om utgående data har tillbakahållits medan fordonets tändning är av (OFF) skall dessa data göras tillgängliga när fordonets tändning har slagits på (ON) igen.

20. **Kalibrering**

154 Kalibreringsfunktionen skall göra det möjligt att

— automatiskt koppla ihop rörelsesensorn med fordonsenheten (VU),

— digitalt anpassa färdskrivarens konstant (k) till den karakteristiska koefficienten för fordonet (w) (fordon med två eller flera bakaxelutväxlingar skall vara utrustade med en omställningsanordning, med vars hjälp de olika utväxlingsförhållandena automatiskt anpassas till det utväxlingsförhållande som färdskrivarutrustningen i fordonet är avsedd för),

— (utan begränsning) ställa in aktuell tid,

— ändra aktuellt vägmätarvärde,

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

— uppdatera eller bekräfta följande parametrar som är kända för färdskrivaren: Identifiering av fordon, w, l, däcksdimension och hastighetsbegränsande anordning i förekommande fall.

155 Hopkopplingen av rörelsesensorn med fordonsenheten (VU) skall 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.

156 Kalibreringsfunktionen skall kunna mata in nödvändiga data genom kalibrerings-/överföringsanslutningen i enlighet med det kalibreringsprotokoll som anges i tillägg 8. Kalibreringsfunktionen får också mata in nödvändiga data genom andra anslutningar.

21. **Tidsinställning**

157 Funktionen för tidsinställning skall göra det möjligt att ställa in aktuell tid på högst en minut när, minst var sjunde dag.

158 Funktionen för tidsinställning skall göra det möjligt att ställa in aktuell tid utan begränsning, i kalibreringsläge.

22. **Prestanda**

159 Fordonsenheten skall vara helt funktionsduglig vid temperaturer från − 20 °C till + 70 °C, och rörelsesensorn vid temperaturer från − 40 °C till + 135 °C. Innehållet i dataminnet skall bevaras vid temperaturer ned till − 40 °C.

160 Färdskrivaren skall vara helt funktionsduglig vid en luftfuktighet av 10 procent till 90 procent.

161 Färdskrivaren skall skyddas mot överspänning, omkastning av polerna i dess strömtillförsel, och strömavbrott.

162 Färdskrivaren skall uppfylla kraven i kommissionens direktiv 95/54/EG ([1]) om anpassning till den tekniska utvecklingen av rådets direktiv 72/245/EEG, om elektromagnetisk kompatibilitet, och skall skyddas mot elektrostatiska laddningar och transienter.

23. **Material**

163 Färdskrivarutrustningens samtliga beståndsdelar skall vara tillverkade av material med tillräcklig stabilitet och mekanisk hållfasthet samt med stabila elektrotekniska och magnetiska egenskaper.

164 Vid normala driftsförhållanden skall samtliga inre delar av färdskrivarutrustningen vara skyddade mot fukt och damm.

165 Fordonsenheten skall uppfylla kriterierna för skyddsklass IP 40 och rörelsesensorn skall uppfylla kriterierna för skyddsklass IP 64, i enlighet med standard IEC 529.

([1]) EGT L 266, 8.11.1995, s. 1.

166 Färdskrivaren skall uppfylla tillämpliga tekniska krav med avseende på ergonomisk utformning.

167 Färdskrivaren skall skyddas mot oavsiktlig skada.

24. **Märkningar**

168 Om färdskrivaren visar fordonets vägmätarvärde och hastighet skall följande uppgifter visas på dess display:

— Intill den siffra som vägmätaren visar, enheten för sträckan, med förkortningen 'km'.

— Intill den siffra som hastighetsmätaren visar, angivelsen 'km/h'.

Färdskrivaren får också ställas om till att visa hastigheten i 'miles per hour', varvid hastigheten skall visas med förkortningen 'mph'.

169 En typskylt skall fästas på varje enskild komponent i färdskrivaren och den skall ange följande:

— Färdskrivartillverkarens namn och adress.

— Tillverkarens delnummer och tillverkningsår för utrustningen.

— Färdskrivarens serienummer.

— Typgodkännandemärke för färdskrivartypen.

170 När utrymmet inte räcker till för att visa alla ovan nämnda detaljer skall typskylten minst ange följande: Tillverkarens namn eller logotyp, och färdskrivarens delnummer.

IV. KONSTRUKTIONS- OCH FUNKTIONSKRAV FÖR FÄRDSKRIVARKORT

1. **Synliga data**

Framsidan skall innehålla följande:

171 Orden 'förarkort', 'kontrollkort', 'verkstadskort', eller 'företagskort' i stort typsnitt på det eller de officiella språken i den medlemsstat som utfärdar kortet, beroende på korttyp.

172 Samma ord på gemenskapens övriga officiella språk skall tryckas så att de bildar bakgrund på kortet enligt följande:

ES	TARJETA DEL CONDUCTOR	TARJETA DE CONTROL	TARJETA DEL CENTRO DE ENSAYO	TARJETA DE LA EMPRESA
DK	FØRERKORT	KONTROLKORT	VÆRKSTEDSKORT	VIRKSOMHEDSKORT
DE	FAHRERKARTE	KONTROLLKARTE	WERKSTATTKARTE	UNTERNEHMENSKARTE
EL	ΚΑΡΤΑ ΟΔΗΟΥ	ΚΑΡΤΑ ΕΛΕΓΧΟΥ	ΚΑΡΤΑ ΚΕΝΤΡΟΥ ΔΟΚΙΜΩΝ	ΚΑΡΤΑ ΕΠΙΧΕΙΡΗΣΗΣ
EN	DRIVER CARD	CONTROL CARD	WORKSHOP CARD	COMPANY CARD
FR	CARTE DE CONDUCTEUR	CARTE DE CONTROLEUR	CARTE D'ATELIER	CARTE D'ENTREPRISE
GA	CÁRTA TIOMÁNAÍ	CÁRTA STIÚRTHA	CÁRTA CEARDLAINNE	CÁRTA COMHLACHTA
IT	CARTA DEL CONDUCENTE	CARTA DI CONTROLLO	CARTA DELL'OFFICINA	CARTA DELL'AZIENDA
NL	BESTUURDERS KAART	CONTROLEKAART	WERKPLAATSKAART	BEDRIJFSKAART
PT	CARTÃO DE CONDUTOR	CARTÃO DE CONTROLO	CARTÃO DO CENTRO DE ENSAIO	CARTÃO DE EMPRESA
FI	KULJETTAJA KORTTILLA	VALVONTA KORTILLA	TESTAUSASEMA KORTILLA	YRITYSKORTILLA
SV	FÖRARKORT	KONTROLLKORT	VERKSTADSKORT	FÖRETAGSKORT

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

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

B Belgien

DK Danmark

D Tyskland

GR Grekland

E Spanien

F Frankrike

IRL Irland

I Italien

L Luxemburg

NL Nederländerna

A Österrike

P Portugal

FIN Finland

S Sverige

UK Förenade kungariket

175 De uppgifter som är särskiljande för kortet, numrerade enligt följande:

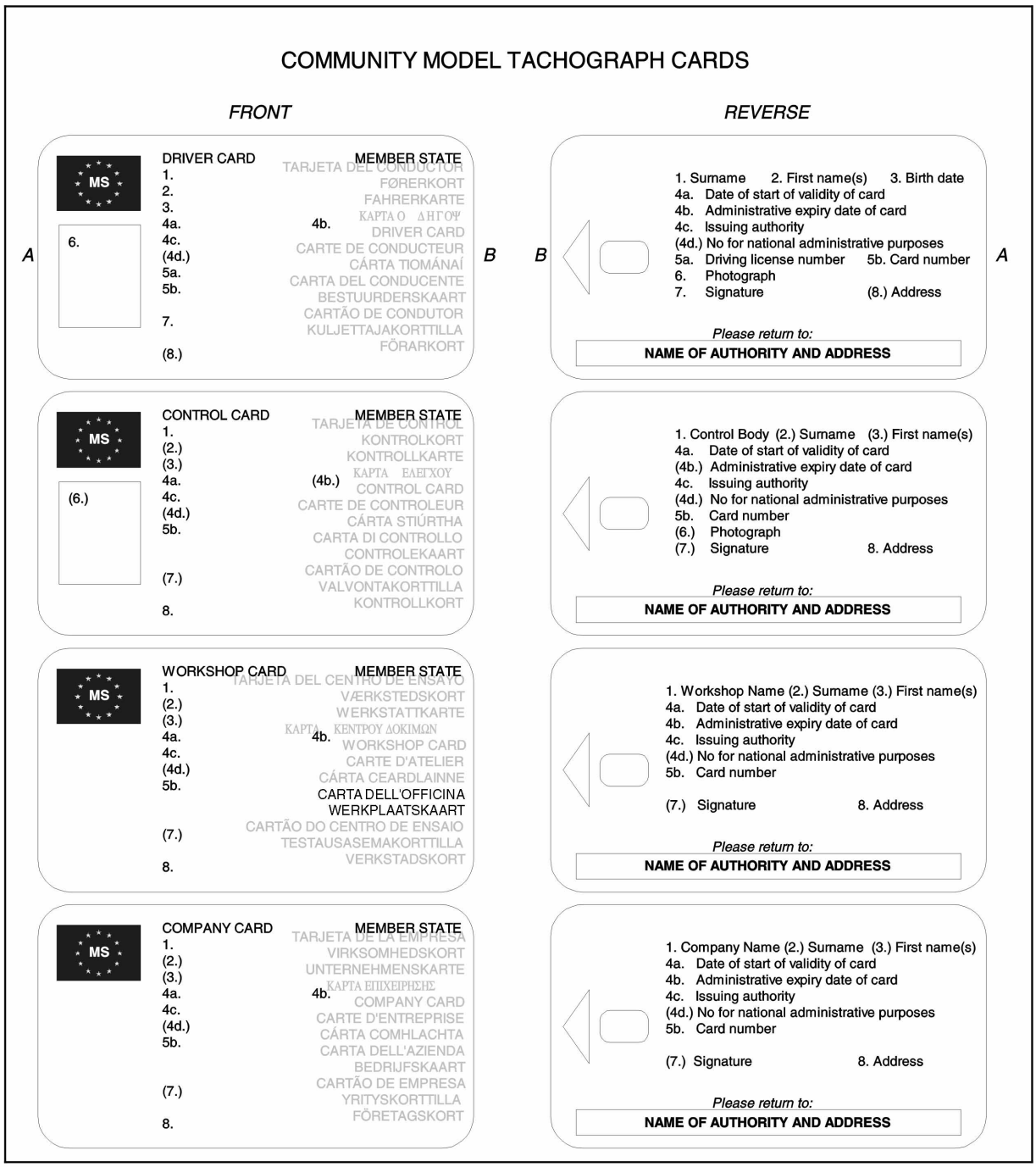
	Förarkort	Kontrollkort	Företagskort eller verkstadskort
1.	Förarens efternamn	Kontrollorganets namn	Företagets eller verkstadens namn
2.	Förarens förnamn	Kontrollantens efternamn (i förekommande fall)	Kortinnehavarens efternamn (i förekommande fall)
3.	Förarens födelsedatum	Kontrollantens förnamn (i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

176 Datum skall skrivas i formatet ’dd/mm/åååå’ eller ’dd.mm.åååå’ (dag, månad, år).

Baksidan skall innehålla följande:

177 En förklaring av de numrerade punkterna på kortets framsida.

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



179 Färdskrivarkorten skall tryckas i följande dominerande bakgrundsfärger:

— Förarkort: Vitt.

— Kontrollkort: Blått.

— Verkstadskort: Rött.

— Företagskort: Gult.

180 Färdskrivarkorten skall åtminstone ha följande skydd mot förfalskning och manipulering:

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

— Kring fotografiet skall säkerhetsmönstret och fotografiet överlappa varandra.

— Minst en tvåfärgad mikrotextrad.

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

2. **Säkerhet**

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

182 För att systemsäkerhet skall kunna uppnås måste färdskrivarkorten uppfylla de säkerhetskrav som anges i det allmänna säkerhetsmålet för färdskrivarkort (tillägg 10).

183 Färdskrivarkorten skall vara läsbara för annan utrustning, såsom personliga datorer.

3. **Normer**

184 Färdskrivarkorten skall uppfylla följande normer:

— ISO/IEC 7810 Transaktionskort – Material, mått och egenskaper,

— ISO/IEC 7816 Transaktionskort – Aktivt kort:

  — Del 1: Fysiska egenskaper.

  — Del 2: Kontaktdon.

  — Del 3: Signaler och protokoll.

  — Del 4: Inter-industry commands for interchange.

  — Del 8: Security related inter-industry commands.

— ISO/IEC 10373 Identification cards – Test methods.

4. **Miljö- och elspecifikationer**

185 Färdskrivarkorten skall fungera korrekt under alla klimatförhållanden som vanligtvis förekommer inom gemenskapens territorium och vid temperaturer mellan − 25 °C till + 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.

186 Färdskrivarkortet skall fungera korrekt vid en luftfuktighet av 10 procent till 90 procent.

187 Färdskrivarkorten skall fungera korrekt under en femårsperiod om de används i enlighet med miljö- och elspecifikationerna.

188 Vid användning skall färdskrivarkorten uppfylla bestämmelserna i kommissionens direktiv 95/54/EG av den 31 oktober 1995 ([1]), om elektromagnetisk kompatibilitet, och de skall skyddas mot elektrostatiska laddningar.

5. **Lagring av data**

Under denna punkt används följande beteckningar med de betydelser som här anges:

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

— Vägmätarvärden registreras med en upplösning av en kilometer.

— Hastigheter registreras med en upplösning av en km/h.

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

([1]) EGT L 266, 8.11.1995, s. 1.

189 Under denna punkt anges minsta lagringskapacitet för de olika datafiler som används. Färdskrivarkorten skall kunna ange dessa datafilers faktiska lagringskapacitet till färdskrivaren.

Alla övriga data som finns lagrade på färdskrivarkorten, och som avser andra eventuella korttillämpningar, skall lagras i enlighet med direktiv 95/46/EG ([1])

5.1 ***Kortidentifiering och säkerhetsdata***

5.1.1 *Användaridentifiering*

190 Det skall gå att lagra följande användardata för identifiering på färdskrivarkortet:

— Användaridentifiering av färdskrivare.

— Identifiering av typ av färdskrivarkort.

5.1.2 *Identifiering av chip*

191 Det skall gå att lagra följande identifieringsdata för integrerade kretsar (IC) på färdskrivarkortet:

— De integrerade kretsarnas serienummer.

— Tillverkningsuppgifter för de integrerade kretsarna.

5.1.3 *Identifiering av IC-kort*

192 Det skall gå att lagra följande identifieringsdata för smartkort på färdskrivarkortet:

— Kortets serienummer (inbegripet tillverkningsuppgifter).

— Typgodkännandenummer för korttypen.

— Kortets identifiering (ID).

— Inbäddat ID.

— IC-identifiering.

5.1.4 *Säkerhetskomponenter*

193 Det skall gå att lagra följande säkerhetskomponenter på färdskrivarkorten:

— Europeisk kryptering med öppen kod.

— Intyg från medlemsstaten.

— Kortintyg.

— Privat kortkod.

5.2 ***Förarkort***

5.2.1 *Kortidentifiering*

194 Det skall gå att lagra följande kortidentifieringsdata på förarkortet:

— Kortnummer.

— Utfärdande medlemsstat, utfärdande myndighet, utfärdandedatum.

— Kortets första och sista giltighetsdag.

([1]) EGT L 281, 23.11.1995, s. 31.

5.2.2 *Identifiering av kortinnehavare*

195 Det skall gå att lagra följande identifieringsdata för kortinnehavare på förarkortet:

— Innehavarens efternamn.

— Innehavarens förnamn.

— Födelsedatum.

— Valt språk.

5.2.3 *Information om körkort*

196 Det skall gå att lagra följande körkortsdata på förarkortet:

— Utfärdande medlemsstat, utfärdande myndighet.

— Körkortsnummer (den dag körkortet utfärdades).

5.2.4 *Data om använda fordon*

197 Det skall 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 isättnings-/urtagningscykler i fordonet för kortet i fråga):

— Datum och tidpunkt för första användning av fordonet (dvs. första kortisättning under denna användningsperiod för fordonet eller 00.00 om användningsperioden är pågående vid den tidpunkten).

— Fordonets vägmätarvärde vid den tidpunkten

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

— Fordonets vägmätarvärde vid den tidpunkten.

— Fordonets registreringsnummer (VRN) och registrerande medlemsstat.

198 Det skall gå att lagra minst 84 sådana registreringar på förarkortet.

5.2.5 *Data om föraraktiviteter*

199 Det skall gå att lagra följande data på förarkortet för varje kalenderdag då kortet har använts eller för vilken föraren har angett aktiviteterna manuellt:

— Datum.

— En närvaroräknare (ökad med en för varje av dessa kalenderdagar).

— Den sammanlagda sträcka som föraren har tillryggalagt den dagen.

— Förarstatus kl. 00.00.

— Följande data när föraren har ändrat aktivitet och/eller har ändrat förarstatus, och/eller har satt i eller tagit ut sitt kort:

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

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

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

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

  — Tidpunkt för ändringen.

200 Det skall gå att lagra data om föraraktiviteter i minst 28 dagar i kortminnet (en förares genomsnittliga aktivitet är fastställd till 93 aktivitetsändringar per dygn).

201 De data som är förtecknade under krav 197 och 199 skall lagras på ett sätt som möjliggör att aktiviteter tas fram i den ordning de har ägt rum, även om tiderna överlappar varandra.

5.2.6 *Platser där dagens arbetspass påbörjas och/eller avslutas*

202 Det skall gå att på förarkortet lagra följande data om de platser som anges av föraren där dagens arbetspass påbörjas och/eller avslutas:

— Datum och tidpunkt för angivelsen (eller datum/tidpunkt för angivelsen om den görs under förfarandet för manuell angivelse).

— Typ av angivelse (påbörjande eller avslutande, angivelsevillkor).

— Det land och den region som anges.

— Fordonets vägmätarställning.

203 Det skall gå att lagra minst 42 par av sådana registreringar i förarkortets minne.

5.2.7 *Händelsedata*

För händelsedata skall tiden lagras med en upplösning av en sekund.

204 Det skall gå att på förarkortet lagra data om följande händelser som upptäckts av färdskrivaren när kortet var isatt:

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

— Isättning av kort under körning (om detta kort är orsak till händelsen).

— Senaste kortanvändning ej korrekt avslutad (om detta kort är orsak till händelsen).

— Avbrott av strömtillförseln.

— Fel i rörelsedata.

— Försök till säkerhetsöverträdelse.

205 Det skall gå att lagra följande data om dessa händelser på förarkortet:

— Händelsekod.

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

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

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

Obs: När det gäller händelsen 'överlappning av tider' skall

— datum och tidpunkt för händelsens början motsvara datum och tidpunkt för urtagning av kortet i föregående fordon, datum och tidpunkt för händelsens slut motsvara datum och tidpunkt för isättning av kortet i aktuellt fordon,

— fordonsdata skall avse det fordon som givit upphov till händelsen.

Obs: När det gäller händelsen 'senaste kortanvändning ej korrekt avslutad' skall:

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

— datum och tidpunkt för händelsens slut motsvara datum och tidpunkt för isättning av kortet för den användningsperiod då händelsen upptäcktes (innevarande användningsperiod),

— fordonsdata motsvara det fordon där användningen inte avslutades korrekt.

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

5.2.8 *Feldata*

För feldata skall tiden registreras med en upplösning av en sekund.

207 Det skall gå att på förarkortet lagra data om följande fel som upptäckts av färdskrivaren när kortet var isatt:

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

— Färdskrivarfel.

208 Det skall gå att lagra följande data om dessa fel på förarkortet:

— Felkod.

— Datum och tidpunkt för felets början (eller för kortisättning om felet var pågående vid den tidpunkten).

— Datum och tidpunkt för felets slut (eller för urtagning av kort om felet var pågående vid den tidpunkten).

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

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

5.2.9 *Data om kontrollaktiviteter*

210 Det skall 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.

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

Obs: Enligt säkerhetskraven skall överföring av data från kort endast registreras om den gjorts genom en färdskrivare.

211 Det skall gå att lagra en sådan registrering på förarkortet.

5.2.10 *Data om kortanvändning*

212 Det skall gå att på förarkortet lagra följande data om det fordon som påbörjade den aktuella användningen:

— Datum och tidpunkt för när användningen påbörjades (dvs. kortisättning) med en upplösning av en sekund.

— Fordonets registreringsnummer (VRN) och registrerande medlemsstat.

5.2.11 *Data om särskilda omständigheter*

212a Det skall gå att på förarkortet lagra följande data om de särskilda omständigheter som angavs medan kortet var isatt (oavsett kortplats):

— Datum och tidpunkt för angivelsen.

— Typ av särskild omständighet

212b Det skall gå att lagra 56 sådana registreringar på förarkortet.

5.3 ***Verkstadskort***

5.3.1 *Säkerhetskomponenter*

213 Det skall gå att lagra ett personligt identifieringsnummer (PIN-kod) på verkstadskortet.

214 Det skall gå att på verkstadskortet lagra de krypterade koder som behövs för att koppla ihop rörelsesensorer med fordonsenheter.

5.3.2 *Kortidentifiering*

215 Det skall gå att lagra följande data om kortidentifiering på verkstadskortet:

— Kortnummer.

— Utfärdande medlemsstat, utfärdande myndighet, utfärdandedatum.

— Kortets första och sista giltighetsdag.

5.3.3 *Identifiering av kortinnehavare*

216 Det skall gå att lagra följande data om identifiering av kortinnehavare på verkstadskortet:

— Verkstadens namn.

— Verkstadens adress.

— Innehavarens efternamn.

— Innehavarens förnamn.

— Valt språk.

5.3.4 *Data om använda fordon*

217 På verkstadskortet skall det gå att lagra data om använda fordon på samma sätt som på ett förarkort.

218 Det skall gå att lagra minst 4 sådana registreringar på verkstadskortet.

5.3.5 *Data om föraraktiviteter*

219 På verkstadskortet skall det gå att lagra data om föraraktiviteter på samma sätt som på ett förarkort.

220 Det skall gå att lagra föraraktivitetsdata på verkstadskortet för minst en dag av genomsnittlig föraraktivitet.

5.3.6 *Data om påbörjande och/eller avslutande av dagens arbetspass*

221 På verkstadskortet skall det gå att lagra data om påbörjande och/eller avslutande av dagens arbetspass på samma sätt som på ett förarkort.

222 Det skall gå att lagra minst 3 par av sådana registreringar på verkstadskortet.

5.3.7 *Data om händelser och fel*

223 På verkstadskortet skall det gå att lagra data om händelser och fel på samma sätt som på ett förarkort.

224 På verkstadskortet skall 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).

5.3.8 *Data om kontrollaktiviteter*

225 På verkstadskortet skall det gå att lagra data om kontrollaktiviteter på samma sätt som på ett förarkort.

5.3.9 *Data om kalibrering och tidsinställning*

226 På verkstadskortet skall det gå att lagra registreringar av kalibreringar och/eller tidsinställningar som utförts medan kortet var isatt i färdskrivaren.

227 Det skall gå att inbegripa följande data i varje kalibreringsregistrering:

— Syfte med kalibreringen (första installation, installation och 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 delnummer, fordonsenhetens serienummer, rörelsesensorns serienummer).

228 Det skall gå att lagra minst 88 sådana registreringar på verkstadskortet.

229 Verkstadskortet skall vara försett med en räknare som anger det sammanlagda antal kalibreringar som gjorts med kortet.

230 Verkstadskortet skall vara försett med en räknare som anger det antal kalibreringar som gjorts sedan dess senaste överföring.

5.3.10 *Data om särskilda omständigheter*

230a På verkstadskortet skall det gå att lagra data om särskilda omständigheter på samma sätt som på förarkortet. Det skall gå att lagra två sådana registreringar på

5.4 ***Kontrollkort***

5.4.1 *Kortidentifiering*

231 Det skall gå att lagra följande data om kortidentifiering på kontrollkortet:

— Kortnummer.

— Utfärdande medlemsstat, utfärdande myndighet, utfärdandedatum.

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

5.4.2 *Identifiering av kortinnehavare*

232 Det skall gå att lagra följande data om identifiering av kortinnehavare på kontrollkortet:

— Kontrollorganets namn.

— Kontrollorganets adress.

— Innehavarens efternamn.

— Innehavarens förnamn.

— Valt språk.

5.4.3 *Data om kontrollaktiviteter*

233 Det skall 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).

— 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.

234 Det skall gå att lagra minst 230 sådana registreringar på kontrollkortet.

5.5 ***Företagskort***

5.5.1 *Kortidentifiering*

235 Det skall gå att lagra följande data om kortidentifiering på företagskortet:

— Kortnummer.

— Utfärdande medlemsstat, utfärdande myndighet, utfärdandedatum.

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

5.5.2 *Identifiering av kortinnehavare*

236 Det skall gå att lagra följande data om identifiering om kortinnehavare på företagskortet:

— Företagets namn.

— Företagets adress.

5.5.3 *Data om företagsaktiviteter*

237 Det skall gå att lagra följande data om företagsaktiviteter på företagskortet:

— Datum och tidpunkt för aktiviteten.

— Typ av aktivitet (låsning och/eller öppning, 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 av kort).

238 Det skall gå att lagra minst 230 sådana registreringar på företagskortet.

V. INSTALLATION AV FÄRDSKRIVAREN

1. **Installation**

239 Nya färdskrivare skall inte vara aktiverade när de levereras till montörer eller fordonstillverkare, och alla de kalibreringsparametrar som är förtecknade i kapitel III.20 skall vara inställda på passande och giltiga automatiska värden. Om det inte finns något passande värde skall bokstavsparametrar ställas in på rader med '?' och sifferparametrar på '0'.

240 Innan färdskrivaren aktiveras skall den ge tillgång till kalibreringsfunktionen även om den inte är i kalibreringsläge.

241 Innan färdskrivaren aktiveras skall den varken registrera eller lagra de data som anges i III.12.3 till och med III.12.9 och III.12.12 till och med III.12.14.

242 Vid installationen skall fordonstillverkaren förinställa alla kända parametrar.

243 Fordonstillverkare eller montörer skall aktivera den installerade färdskrivaren innan fordonet lämnar den anläggning där installationen utfördes.

244 Aktiveringen av färdskrivaren skall utlösas automatiskt första gången ett verkstadskort sätts in i någon av kortläsarna.

245 Den särskilda koppling som krävs mellan rörelsesensor och fordonsenhet skall i förekommande fall ske automatiskt före eller under aktivering.

246 Efter det att färdskrivaren har aktiverats skall den till fullo upprätthålla funktioner och tillträdesrättigheter till data.

247 Färdskrivarens registrerings- och lagringsfunktioner skall vara helt i drift när den har aktiverats.

248 Installationen skall följas av en kalibrering. Vid den första kalibreringen skall fordonets registreringsnummer (VRN) anges och den skall äga rum inom två veckor efter denna installation eller efter det att ett registreringsnummer har tilldelats fordonet, om detta sker senare.

248a Färdskrivaren skall placeras i fordonet på så sätt att de nödvändiga funktionerna kan nås från förarplatsen.

2. **Installationsskylt**

249 Efter det att färdskrivaren har kontrollerats vid installationen, skall en installationsskylt som är väl synlig och lätt tillgänglig anbringas på, inuti eller bredvid färdskrivaren. Efter varje besiktning av en godkänd montör eller verkstad skall skylten ersättas med en ny skylt.

250 På skylten skall åtminstone följande uppgifter anges:

— Godkänd montörs eller verkstads namn och adress eller handelsbeteckning.

— Fordonets karakteristiska koefficient, uttryckt i ’w = … imp/km’,

— Färdskrivarens konstant, uttryckt i ’w = … imp/km’,

— Däckens effektiva omkrets, uttryckt i ’l = … mm’,

— Däcksdimension.

— Datum då fordonets karakteristiska koefficient och däckens effektiva omkrets fastställdes.

— Fordonets chassinummer (VIN).

3. **Plombering**

251 Följande komponenter skall plomberas:

— Varje anslutning som i händelse av urkoppling skulle orsaka icke påvisbara förvanskningar eller förluster av uppgifter.

— Installationsskylten, om den inte är anbringad på sådant sätt att den inte kan avlägsnas utan att texten på den förstörs.

252 Ovan nämnda plomberingar får avlägsnas

— i nödsituationer,

— för att installera, anpassa eller reparera hastighetsbegränsande anordningar eller andra anordningar som bidrar till trafiksäkerheten, förutsatt att färdskrivaren fortsätter att fungera på tillförlitligt och avsett sätt och att den åter förseglas av en godkänd montör eller verkstad (i enlighet med kapitel VI) omedelbart efter det att den hastighetsbegränsande anordningen eller annan anordning som bidrar till trafiksäkerhet har monterats eller inom 7 dagar i övriga fall.

253 Varje gång dessa plomberingar bryts skall en skriftlig rapport upprättas som redovisar skälen för åtgärden och ställs till behörig myndighets förfogande.

VI. KONTROLLER, BESIKTNINGAR OCH REPARATIONER

Bestämmelserna för när plomberingarna får avlägsnas, i enlighet med artikel 12.5 i rådets förordning (EEG) nr 3821/85, senast ändrad genom rådets förordning (EG) nr 2135/98, anges i kapitel V.3 i denna bilaga.

1. **Godkännande av montörer eller verkstäder**

Medlemsstaterna skall godkänna, regelbundet kontrollera och auktorisera de organ som skall utföra

— installationer,

— kontroller,

— besiktningar,

— reparationer.

Inom ramen för artikel 12.1 i denna förordning skall verkstadskort endast utfärdas till de montörer och/eller verkstäder som godkänts för aktivering och/eller kalibrering av färdskrivare i enlighet med denna bilaga och, om det inte vederbörligen motiveras,

— som inte har rätt till ett företagskort,

— och vars övriga yrkesverksamhet inte utgör en möjlig kompromiss av den övergripande systemsäkerheten i enlighet med bilaga 10.

2. **Kontroller av nya eller reparerade instrument**

254 Varje enskild anordning, vare sig den är ny eller reparerad, skall kontrolleras med avseende på att instrumentet fungerar riktigt och att dess avlästa och registrerade värden ligger inom de i kapitel III.2.1 och III.2.2 fastställda gränsvärdena, genom plombering i enlighet med kapitel V.3 och kalibrering.

3. **Installationsbesiktning**

255 När hela utrustningen (inbegripet färdskrivaren) monteras i ett fordon skall den överensstämma med bestämmelserna om största tillåtna toleranser i kapitel III.2.1 och III.2.2.

4. **Periodiska besiktningar**

256 Periodiska besiktningar av färdskrivarutrustning i fordon skall 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.

257 Dessa besiktningar skall omfatta

— kontroll av att färdskrivaren fungerar riktigt, inbegripet funktionen för datalagring på färdskrivarkort,

— kontroll av att efterlevnaden av bestämmelserna i kapitel III.2.1 och III.2.2 om största tillåtna toleranser vid installation efterlevs,

— kontroll av att typgodkännandemärke finns på färdskrivaren,

— kontroll av att installationsskylt finns,

— kontroll av att plomberingarna på färdskrivaren och de andra delarna av utrustningen är orörda,

— kontroll av däcksdimension och däckens faktiska omkrets.

258 Dessa besiktningar skall inbegripa en kalibrering.

5. **Uppmätning av fel**

259 Uppmätning av fel vid montering och i drift skall genomföras under följande förutsättningar, vilka skall anses utgöra standardiserade provningsförhållanden:

— Fordon utan last i körklart skick.

— Däcktryck enligt tillverkarens anvisningar.

— Däckförslitning inom av nationell lag tillåtna gränsvärden.

— Fordonets rörelse:

  — Fordonet skall, framdrivet av sin egen motor, röra sig framåt i rät linje och på jämnt underlag med en hastighet av 50 ± 5 km/tim. Mätsträckan skall vara åtminstone 1 000 m.

— Förutsatt att provningen kan ske med jämförbar precision får alternativa metoder, exempelvis en passande provbänk, även användas vid provningen.

6. **Reparationer**

260 Verkstäderna skall kunna överföra data från färdskrivare för att återlämna dem till berört transportföretag.

261 Godkända verkstäder skall 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 skall behålla en kopia av varje utfärdat intyg i minst ett år.

VII. UTFÄRDANDE AV KORT

De förfaranden för utfärdande av kort som medlemsstaterna upprättar skall överensstämma med följande:

262 Numret på det första färdskrivarkortet som utfärdas till en sökande skall ha ett löpnummer (i förekommande fall) och ett ersättningsindex och ett förnyelseindex som sätts till ’0’.

263 Kortnumren på alla opersonliga färdskrivarkort som har utfärdats till ett enskilt kontrollorgan, en enskild verkstad eller ett enskilt transportföretag skall ha samma 13 första siffror och samtliga skall ha sitt eget löpnummer.

264 Ett färdskrivarkort som utfärdas som ersättning för ett befintligt färdskrivarkort skall ha samma kortnummer som det ersatta kortet förutom att ersättningsindex skall ökas med ’1’ (i ordningen 0, …, 9, A, …, Z).

265 Ett färdskrivarkort som utfärdats som ersättning för ett befintligt färdskrivarkort skall ha samma sista giltighetsdatum som det ersatta kortet.

266 Ett färdskrivarkort som utfärdas som förnyelse av ett befintligt färdskrivarkort skall ha samma kortnummer som det förnyade kortet förutom att ersättningsindex åter skall sättas till "0" och att förnyelseindex skall ökas med ’1’ (i ordningen 0, …, 9, A, …, Z).

267 Utbyte av ett befintligt färdskrivarkort för att ändra administrativa uppgifter, skall 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.

268 I fältet ’Kortinnehavarens efternamn’ på opersonliga provnings- eller kontrollkort skall verkstadens eller kontrollorganets namn anges.

VIII. TYPGODKÄNNANDE FÖR FÄRDSKRIVARE OCH FÄRDSKRIVARKORT

1. **Allmänt**

I detta kapitel avses med begreppet ’färdskrivare’ ’färdskrivare eller dess komponenter’. Inget typgodkännande krävs för den eller de kablar med vilka rörelsesensorn ansluts till fordonsenheten. Det papper som används i färdskrivaren skall anses som en av färdskrivarens komponenter.

269 Eventuell integrerad extrautrustning skall finnas med vid ansökan om godkännande av färdskrivare.

270 Typgodkännande av färdskrivare och färdskrivarkort skall inbegripa säkerhetsprovningar, funktionella provningar och provningar med avseende på driftskompatibilitet. Positiva resultat från var och en av dessa provningar skall anges i ett lämpligt intyg.

271 Medlemsstaternas myndigheter för typgodkännande får inte bevilja något intyg om typgodkännande i enlighet med artikel 5 i denna förordning 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.

272 Varje ändring av färdskrivarens programvara eller maskinvara eller av det slag av material som används för dess tillverkning skall, innan den tas i bruk, anmälas till den myndighet som har beviljat typgodkännandet av färdskrivaren. Denna myndighet skall för tillverkaren bekräfta utvidgningen av typgodkännandet, eller får begära en uppdatering eller bekräftelse av berörda funktionsintyg, säkerhetsintyg, och/eller intyg om driftskompatibilitet.

273 Förfaranden för att uppgradera programvaran i färdskrivaren på plats skall godkännas av den myndighet som beviljade typgodkännandet av färdskrivaren. Uppgraderingen av mjukvaran får inte innebära att de föraraktivitetsdata som finns lagrade i färdskrivaren ändras eller tas bort. Programvaran får bara uppgraderas under färdskrivaretillverkarens ansvar.

2. **Säkerhetsintyg**

274 Säkerhetsintyget skall utfärdas i enlighet med bestämmelserna i tillägg 10 till denna bilaga.

3. **Funktionsintyg**

275 Alla som ansöker om typgodkännande skall förse medlemsstatens myndighet för typgodkännande med allt det material och alla de handlingar som myndigheten anser nödvändiga.

276 Ett funktionsintyg får inte utfärdas till en tillverkare förrän minst alla de funktionsprovningar som anges i tillägg 9 har genomgåtts med positivt resultat.

277 Myndigheten för typgodkännande skall utfärda funktionsintyget. Förutom mottagarens namn och identifiering av modellen, skall detta intyg innehålla en detaljerad förteckning över utförda provningar och erhållna resultat.

4. **Intyg om driftskompatibilitet**

278 Provningar av driftskompatibilitet skall utföras av ett enda laboratorium under Europeiska kommissionens ansvar och överinseende.

279 Laboratoriet skall registrera de ansökningar om provningar av driftskompatibilitet som tillverkare inlämnar i den ordning som de inkommer.

280 Ansökningarna får inte registreras officiellt förrän laboratoriet förfogar över

— allt det material och alla de handlingar som krävs för provningen av driftskompatibilitet,

— motsvarande säkerhetsintyg, och

— motsvarande funktionsintyg.

Registreringsdatum för ansökan skall anmälas till tillverkaren.

281 Laboratoriet får inte utföra några provningar av driftskompatibiliteten hos en färdskrivare eller ett färdskrivarkort för vilka något säkerhetsintyg och funktionsintyg inte har beviljats.

282 En tillverkare som ansöker om provningar av driftskompatibilitet skall 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.

283 Provningar av driftskompatibilitet skall, i enlighet med bestämmelserna i punkt 5 i tillägg 9 till denna bilaga, utföras för alla de typer av färskrivare och färdskrivarkort

— för vilka typgodkännandet fortfarande gäller, eller

— för vilka typgodkännandet håller på att avgöras och ett giltigt intyg om driftskompatibilitet redan finns.

284 Laboratoriet får inte utfärda intyget om driftskompatibilitet till tillverkaren förrän alla begärda provningar av driftskompatibilitet har genomgåtts med positivt resultat.

285 Om provningarna av driftskompatibilitet inte har genomgåtts med positivt resultat för en eller flera färdskrivare eller färdskrivarkort enligt krav 283, får något intyg om driftskompatibilitet inte utfärdas förrän den ansökande tillverkaren har genomfört nödvändiga ändringar och klarat provningarna av driftskompatibilitet. Laboratoriet skall identifiera orsaken till problemet med hjälp av de tillverkare som berörs av detta driftskompatibilitetsfel och det skall söka hjälpa den ansökande tillverkaren att finna en teknisk lösning. Om tillverkaren har ändrat sin produkt åligger det honom att från berörda myndigheter förvissa sig om att säkerhetsintygen och funktionsintygen fortfarande gäller.

286 Intyget om driftskompatibilitet gäller i sex månader. Det dras in vid utgången av denna period om tillverkaren inte har erhållit ett motsvarande intyg om typgodkännande. Tillverkaren skall vidarebefordra det till den myndighet för typgodkännande i medlemsstaten som har utfärdat funktionsintyget.

287 Delar som kan ligga till grund för driftskompatibilitetsfel får inte användas i vinstsyfte eller leda till dominant ställning.

5. **Intyg om typgodkännande**

288 Medlemsstatens myndighet för typgodkännande får utfärda intyget om typgodkännande så snart som den har de tre begärda intygen.

289 Myndigheten för typgodkännande skall ge en kopia av intyget om typgodkännande till det laboratorium som ansvarar för provningarna av driftskompatibiliteten vid den tidpunkt då intyget utfärdades till tillverkaren.

290 Det laboratorium som är behörigt för provningar av driftskompatibilitet skall 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.

6. **Undantagsförfarande: De första intygen om driftskompatibilitet**

291 Inom fyra månader efter det att en första uppsättning färdskrivare och färdskrivarkort (förarkort, verkstadskort, kontrollkort och företagskort) har intygats vara driftskompatibla, skall alla utfärdade intyg om driftskompatibilitet (inbegripet det allra första) med avseende på de ansökningar som registrerats under denna period, anses vara provisoriska.

292 Om alla berörda produkter vid utgången av denna period är ömsesidigt driftskompatibla, skall alla motsvarande intyg om driftskompatibilitet bli slutliga.

293 Om driftskompatibilitetsfel påträffas under denna period skall 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.

294 Om driftskompatibilitetsproblemen kvarstår vid utgången av denna period skall 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, varpå kommissionen, om ingen gemensam lösning har hittats, efter att ha rådfrågat det laboratorium som ansvarar för provningarna av driftskompatibiliteten skall avgöra för vilken eller vilka färdskrivare och för vilket eller vilka kort ett slutligt intyg om driftskompatibilitet beviljas, och motivera detta.

295 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 anges i krav 294, skall senareläggas tills de ursprungliga kompatibilitetsproblemen har lösts. Dessa ansökningar handläggs sedan i den ordning de registrerats.

Tillägg 1

DATAORDLISTA

INNEHÅLL

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 Abstract Syntax Notation One (ASN.1) 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 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 av värdeområden (value range identifiers). Identifierare av värdeområden definieras i punkt 3.

1.2 **Referenser**

Följande referenser används i detta tillägg:

ISO 639	Code for the representation of names of languages. Första utgåvan: 1988.
EN 726-3	Transaktionskort – Aktiva kort och terminaler vid telekommunikation Tillämpningsoberoende kortkrav. December 1994.
ISO 3779	Bilar – Identifieringsnumrering av fordon (VIN). Utgåva 3: 1983.
ISO/IEC 7816-5	Transaktionskort – Aktivt kort. Nummersystem och registreringsregler för identifiering av tillämpningar. Första utgåvan: 1994 + Ändring 1: 1996.
ISO/IEC 8824-1	Information technology – Abstract Syntax Notation 1 (ASN.1): Specification of basic notation. Utgåva 2: 1998.
ISO/IEC 8825-2	Information technology – ASN.1 encoding rules: Specification of Packed Encoding Rules (PER). Utgåva 2: 1998.
ISO/IEC 8859-1	Information technology – 8 bit single-byte coded graphic character sets – Part 1: Latin alphabet No.1. Första utgåvan: 1998.
ISO/IEC 8859-7	Information technology – 8 bit single-byte coded graphic character sets – Part 7: Latin/Greek alphabet. Första utgåvan: 1987.
ISO 16844-3	Road vehicles – Tachograph systems – Motion Sensor Interface. WD 3-20/05/99.

2. DEFINITIONER AV DATATYPER

För samtliga nedanstående datatyper kommer det förvalda värdet för ett 'okänt' (unknown) eller 'ej tillämpligt' (not applicable) innehåll att bestå i att dataelementet fylls med 'FF'-byte.

2.1 **ActivityChangeInfo**

Denna datatyp gör det möjligt att inom ett ord på två byte koda en öppningsstatus kl. 00.00 och/eller förarstatus kl. 00.00 och/eller ändringar av aktivitet och/eller ändringar av körningsstatus för en förare eller medförare. Denna datatyp berörs av krav 084, 109a, 199 och 219.

```
ActivityChangeInfo ::= OCTET STRING (SIZE(2))
```

Värdetilldelning – Octet Aligned (oktettgrupperad): 'scpaatttttttttttt'B (16 bitar)

För dataminnesregistreringar:

's'B Kortplats (eller kortplatsstatus):

'0'B: DRIVER (förare)

'1'B: CO-DRIVER (medförare)

'c'B Körningsstatus:

'0'B: SINGLE (ensam)

'1'B: CREW (flera förare)

'p'B Förarkorts (eller verkstadskorts) status i relevant kortplats:

'0'B: INSERTED, ett kort har satts i.

'1'B: NOT INSERTED, inget kort har satts i (eller ett kort har tagits ut).

'aa'B Aktivitet:

'00'B: BREAK/REST (rast/vila)

'01'B: AVAILABILITY (tillgänglighet)

'10'B: WORK (arbete)

'11'B: DRIVING (körning)

'ttttttttttt'B Tidpunkt för ändring: Antal minuter sedan 00h00 dagen ifråga.

För förarkorts- (eller verkstadskorts-)poster (och förarstatus):

's'B kortplats (ej relevant när 'p' = 1 förutom anmärkning nedan):

'0'B: DRIVER,

'1'B: CO-DRIVER,

'c'B Körningsstatus (fall 'p' = 0) eller Följande aktivitetsstatus (fall 'p' = 1):

'0'B: SINGLE '0'B: CREW

'1'B: UNKNOWN (okänd) '1'B: KNOWN (känd = manuellt angiven)

'p'B Kortstatus:

'0'B: INSERTED, kortet är isatt i en färdskrivare.

'1'B: NOT INSERTED, kortet har inte satts i (eller kortet har tagits ut).

'aa'B Aktivitet (ej relevant när 'p' = 1 och 'c' = 0 förutom anmärkning nedan):

'00'B: BREAK/REST

'01'B: AVAILABILITY

'10'B: WORK

'11'B: DRIVING

'ttttttttttt'B Tidpunkt för ändring: Antal minuter sedan 00h00 dagen ifråga.

Observera när det gäller 'urtagning av kort':

När kortet är urtaget:

— 's' är relevant och anger den kortplats från vilken kortet har tagits ut,

— 'c' måste sättas till 0,

— 'p' måste sättas till 1,

— 'aa' måste koda den innevarande aktivitet som valts vid den tidpunkten.

Till följd av en manuell angivelse, får bitarna 'c' och 'aa' i ordet (som lagras på 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 den del av ISO/IEC 8859 som används för att koda adressen.

address är en adress som kodats enligt ISO/IEC 8859-codePage.

2.3 **BCDString**

BCDString tillämpas för binärkodad decimal notation (Binary Code Decimal (BCD) representation). Denna datatyp används för att återge en decimalsiffra i en semi-oktett (4 bitar). BCDString bygger på ISO/IEC 8824-1 'CharacterString-Type'.

```
BCDString ::= CHARACTER STRING (WITH COMPONENTS {
   identification ( WITH COMPONENTS {
   fixed PRESENT }) })
```

BCDString använder en 'hstring'-notation. Den hexadecimala siffran längst till vänster skall vara den mest signifikanta semi-oktetten i den första oktetten. För att producera en multipel av oktetter, skall 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.

2.4 **CalibrationPurpose**

Kod som förklarar varför en mängd kalibreringsparametrar registrerades. Denna datatyp berörs av krav 097 och 098.

```
CalibrationPurpose ::= OCTET STRING (SIZE(1))
```

Värdetilldelning:

'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.

2.5 **CardActivityDailyRecord**

Information som finns lagrad på ett kort om föraraktiviteter under en viss kalenderdag. Denna datatyp berörs av krav 199 och 219.

```
CardActivityDailyRecord ::= SEQUENCE {
   activityPreviousRecordLength            INTEGER(0..CardActivityLengthRange),
   activityPreviousRecordLength            INTEGER(0..CardActivityLengthRange),
   activityRecordDate                      TimeReal,
   activityDailyPresenceCounter            DailyPresenceCounter,
   activityDayDistance                     Distance,
   activityChangeInfo                      SET SIZE(1..1440) OF ActivityChangeInfo
}
```

activityPreviousRecordLength är den totala längden i byte av föregående daglig post. Det största värdet ges av längden på den OCTET STRING (oktettsträng) som innehåller dessa poster (se CardActivityLengthRange punkt 3). När denna post är den äldsta dagliga posten måste värdet av activityPreviousRecordLength sättas till 0.

activityRecordLength är denna posts totala längd. Det största värdet ges av längden på den OCTET STRING (oktettsträng) som innehåller dessa poster.

activityRecordDate är datum för posten.

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 1 440 värden (en aktivitetsändring per minut). Denna mängd omfattar alltid activityChangeInfo där förarstatus kodas som kl. 00.00.

2.6 **CardActivityLengthRange**

Antal byte på ett förarkort eller ett verkstadskort som finns tillgängliga för lagring av föraraktivitetsposter.

```
CardActivityLengthRange ::= INTEGER(0..2^16-1)
```

Värdetilldelning: se punkt 3.

2.7 **CardApprovalNumber**

Kortets typgodkännandenummer.

```
CardApprovalNumber ::= IA5String(SIZE(8))
```

Värdetilldelning: Ospecificerad.

2.8 **CardCertificate**

Certifikat för kortets öppna nyckel.

```
CardCertificate ::= Certificate
```

2.9 **CardChipIdentification**

Information som finns lagrad på ett kort om identifiering av kortets integrerade krets (IC) ((krav 191).

```
CardChipIdentification ::= SEQUENCE {
   icSerialNumber                          OCTET STRING (SIZE(4)),
   icManufacturingReferences               OCTET STRING (SIZE(4))
}
```

icSerialNumber är IC-serienummer enligt EN 726-3.

icManufacturingReferences är identifierare av IC-tillverkare och fabrikationselement enligt EN 726-3.

2.10 **CardConsecutiveIndex**

Ett löpnummer för kortet (definition h)).

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

Värdetilldelning: (se kapitel VII i denna bilaga).

Ökningsföljd: '0, …, 9, A, … , Z, a, … , z'

2.11 **CardControlActivityDataRecord**

Information som finns lagrad på ett förarkort eller verkstadskort om den senaste kontrollen av föraren (krav 210 och 225).

```
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 hos den kontrollant som har utfört kontrollen.

controlVehicleRegistration är fordonets registreringsnummer (VRN) och registrerande medlemsstat för det fordon vilket kontrollen ägde rum.

controlDownloadPeriodBegin och **controlDownloadPeriodEnd** är överförd period, om överföring utfördes.

2.12 **CardCurrentUse**

Information om den faktiska användningen av kortet (krav 212).

```
CardCurrentUse ::= SEQUENCE {
   sessionOpenTime                      TimeReal,
   sessionOpenVehicle                   VehicleRegistrationIdentification
}
```

sessionOpenTime är den tid då kortet sätts i 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 införande av kortet. Detta element sätts till noll då kortet tas ut.

2.13 **CardDriverActivity**

Information som finns lagrad på ett förarkort eller verkstadskort om förarens aktiviteter (krav 199 och 219).

```
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.

activityPointerNewestRecord är specificering av början av lagringsplats (antal byte från strängens början) av senaste dagspost i activityDailyRecords-strängen. Det största värdet ges av strängens längd.

activityDailyRecords är det utrymme som finns tillgängligt för att lagra data om föraraktiviteter (datastruktur: CardActivityDailyRecord) för varje kalenderdag som kortet har 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 (förstoring av innevarande activityDailyRecord, eller placering av en ny activityDailyRecord) som ersätter äldre aktivitetsdata, måste activityPointerOldestDayRecord uppdateras till att återspegla den nya placeringen av den äldsta kompletta dagsposten, och activityPreviousRecordLength av denna (nya) äldsta fullständiga dagspost måste återställas till 0.

2.14 **CardDrivingLicenceInformation**

Information som finns lagrad på förarkortet om kortinnehavarens körkortsdata (krav 196).

```
CardDrivingLicenceInformation ::= SEQUENCE {

   drivingLicenceIssuingAuthority           Name,

   drivingLicenceIssuingNation              NationNumeric,

   drivingLicenceNumber                     IA5String(SIZE(16))

}
```

drivingLicenceIssuingAuthority är den myndighet som ansvarar för utfärdandet av körkortet.

drivingLicenceIssuingNation är nationaliteten hos den myndighet som utfärdade körkortet.

drivingLicenceNumber är körkortsnumret.

2.15 **CardEventData**

Information som finns lagrad på ett förarkort eller verkstadskort om händelser som förknippas med kortinnehavaren (krav 204 och 223).

```
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 den sista mängden av sekvensen).

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

2.16 **CardEventRecord**

Information som finns lagrad på ett förarkort eller verkstadskort om en händelse som förknippas med kortinnehavaren (krav 205 och 223).

```
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 där händelsen ägde rum.

2.17 **CardFaultData**

Information som finns lagrad på ett förarkort eller verkstadskort om fel som förknippas med kortinnehavaren (krav 207 och 223).

```
CardFaultData ::= SEQUENCE SIZE(2) OF {
   cardFaultRecords                    SET SIZE(NoOfFaultsPerType) OF
                                       CardFaultRecord
}
```

CardFaultData är en sekvens av postmängd för färdskrivarfel följd av postmängd för kortfel.

cardFaultRecords är en mängd av felposter för en viss felkategori (färdskrivare eller kort).

2.18 **CardFaultRecord**

Information som finns lagrad på ett förarkort eller verkstadskort om ett fel som förknippas med kortinnehavaren (krav 208 och 223).

```
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 fordonets registreringsnummer (VRN) och registrerande medlemsstat för det fordon där felet ägde rum.

2.19 **CardIccIdentification**

Information som finns lagrad på ett kort om identifiering av kortet med integrerade kretsar (IC-kortet) (krav 192).

```
CardIccIdentification ::= SEQUENCE {
   clockStop                           OCTET STRING (SIZE(1)),
   cardExtendedSerialNumber            ExtendedSerialNumber,
   cardApprovalNumber                  CardApprovalNumber
   cardPersonaliserID                  OCTET STRING (SIZE(1)),
   embedderIcAssemblerId               OCTET STRING (SIZE(5)),
   icIdentifier                        OCTET STRING (SIZE(2))
}
```

clockStop är det klockstoppläge (Clockstop mode) som definieras i EN 726-3.

cardExtendedSerialNumber är IC-kortets serienummer och IC-kortets tillverkningsreferens enligt definition i EN 726-3 och enligt närmare specifikation genom datatypen ExtendedSerialNumber.

cardApprovalNumber är kortets typgodkännandenummer.

cardPersonaliserID är identitet hos den som anpassar kortet (card personaliser ID) enligt definition i EN 726-3.

embedderIcAssemblerId är identifierare av inbyggare (embedder)/IC-montör enligt EN 726-3.

icIdentifier är identifierare av integrerad krets på kortet och dess IC-tillverkare enligt definition i EN 726-3.

2.20 **CardIdentification**

Information som finns lagrad på ett kort om identifiering av kortet (krav 194, 215, 231, 235).

```
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.

2.21 **CardNumber**

Ett kortnummer som definieras genom 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.

Den första sekvensen i alternativet (CHOICE) är lämplig för kodning av ett förarkortsnummer, den andra sekvensen är lämplig för kodning av nummer på verkstadskort, kontrollkort och företagskort.

2.22 **CardPlaceDailyWorkPeriod**

Information som finns lagrad på ett förarkort eller verkstadskort om de platser där dagens arbetspass påbörjas och/eller avslutas (krav 202 och 221).

```
CardPlaceDailyWorkPeriod ::= SEQUENCE {

   placePointerNewestRecord                 INTEGER(0..NoOfCardPlaceRecords-1),

   placeRecords                             SET SIZE(NoOfCardPlaceRecords) OF PlaceRe-
                                            cord

}
```

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 av poster som innehåller information om de platser som angivits.

2.23 **CardPrivateKey**

Ett korts privata nyckel.

```
CardPrivateKey ::= RSAKeyPrivateExponent
```

2.24 **CardPublicKey**

Ett korts öppna nyckel.

```
CardPublicKey ::= PublicKey
```

2.25 **CardRenewalIndex**

Ett korts förnyelseindex (definition i)).

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

Värdetilldelning: (se kapitel VII i denna bilaga).

′0′ Första utgåvan.

Ökningsföljd: ′0, …, 9, A, …, Z′

2.26 **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′

2.27 **CardSlotNumber**

Kod för att skilja de två kortplatserna i en fordonsenhet åt.

```
CardSlotNumber ::= INTEGER {

   driverSlot                               (0),

   co-driverSlot                            (1)

}
```

Värdetilldelning: ej närmare angiven.

2.28 **CardSlotsStatus**

Kod som anger den typ av kort som satts i de två kortplatserna i fordonsenheten.

```
CardSlotsStatus ::= OCTET STRING (SIZE(1))
```

Värdetilldelning — Octet Aligned (oktettgrupperad): 'ccccdddd'B:

'cccc'B Identifiering av typ av kort som satts i medförarens kortplats,

'dddd'B Identifiering av typ av kort som satts i förarens kortplats,

med följande identifieringskoder:

'0000'B Inget kort är isatt.

'0001'B Ett förarkort är isatt.

'0010'B Ett verkstadskort är isatt.

'0011'B Ett kontrollkort är isatt.

'0100'B Ett företagskort är isatt.

2.29 **CardStructureVersion**

En kod som anger versionen av den struktur som används i ett färdskrivarkort.

```
CardStructureVersion ::= OCTET STRING (SIZE(2))
```

Värdetilldelning: 'aabb'H:

'aa'H Index för strukturändringar.

'bb'H Index för ändringar när det gäller användning av dataelement som definierats för strukturen till följd av den höga byten.

2.30 **CardVehicleRecord**

Information som finns lagrad på ett förar- eller verkstadskort om en period då ett fordon använts under en kalenderdag (krav 197 och 217).

```
CardVehicleRecord ::= SEQUENCE {
   vehicleOdometerBegin                    OdometerShort,
   vehicleOdometerEnd                      OdometerShort,
   vehicleFirstUse                         TimeReal,
   vehicleLastUse                          TimeReal,
   vehicleRegistration                     VehicleRegistrationIdentification,
   vuDataBlockCounter                      VuDataBlockCounter
}
```

vehicleOdometerBegin är fordonets vägmätarställning vid början av den period då fordonet används.

vehicleOdometerEnd är fordonets vägmätarställning vid slutet av den period då fordonet används.

vehicleFirstUse är datum och tidpunkt för påbörjande av den period då fordonet används.

vehicleLastUse är datum och tidpunkt för avslutande av den period då fordonet används.

vehicleRegistration är fordonets registreringsnummer och den medlemsstat där fordonet är registrerat.

vuDataBlockCounter är värdet i VuDataBlockCounter vid senaste hämtning (extraction) för den period då fordonet använts.

2.31 **CardVehiclesUsed**

Information som finns lagrad på ett förarkort eller verkstadskort om de fordon som kortinnehavaren använder (krav 197 och 217).

```
CardVehiclesUsed := SEQUENCE {
   vehiclePointerNewestRecord              INTEGER(0..NoOfCardVehicleRecords-1),
   cardVehicleRecords                      SET SIZE(NoOfCardVehicleRecords) OF
                                           CardVehicleRecord
}
```

vehiclePointerNewestRecord är index för senast uppdaterad fordonspost.

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.

2.32 **Certificate**

Ett certifikat för en öppen nyckel som utfärdas av en certifieringsinstans.

```
Certificate ::= OCTET STRING (SIZE(194))
```

Värdetilldelning: Digital signatur med partiell återskapning av CertificateContent (certifikatinnehåll) i enlighet med tillägg 11 (Gemensamma säkerhetsmekanismer): Signature (signatur) (128 byte) || Public Key remainder (öppen nyckel rest) (58 byte) || Certification Authority Reference (certifieringsinstansens referens) (8 byte).

2.33 **CertificateContent**

Innehållet (i klartext) i certifikatet för en öppen nyckel i enlighet med tillägg 11 (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 hans öppna nyckel.

publicKey är den öppna nyckel som certifieras genom detta certifikat.

2.34 **CertificateHolderAuthorisation**

Identifiering av en certifikatinnehavares rättigheter.

```
CertificateHolderAuthorisation ::= SEQUENCE {
   tachographApplicationID                  OCTET STRING(SIZE(6))
   equipmentType                            EquipmentType
}
```

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 för EquipmentType. 0 om certifikatet tillhör en medlemsstat.

2.35 **CertificateRequestID**

Unik identifiering av en begäran om certifikat. Den kan också användas som en identifierare av 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-kod för månad (två siffror) och år (två sista siffrorna).

crIdentifier: är en identifierare för att skilja en begäran om certifikat från ett förlängt serienummer.

Värdetilldelning: 'FFh'.

manufacturerCode: är den numeriska koden för den tillverkare som begär certifikatet.

2.36 **CertificationAuthorityKID**

Identifierare av öppen nyckel för certifieringsinstans (en medlemsstats eller europeisk certifieringsinstans).

```
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.

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 skilja nyckelidentifierare av certifieringsinstans från andra nyckelidentifierare.

Värdetilldelning: '01h'.

2.37 **CompanyActivityData**

Information som finns lagrad på ett företagskort om aktiviteter som utförts med kortet (krav 237).

```
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 (post för företagsaktiviteter).

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 på det kort som överförts och den medlemsstat som utfärdat det, 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.är den period som överförs från fordonsenheten, i förekommande fall.

2.38 **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)
}
```

2.39 **CompanyCardApplicationIdentification**

Information som finns lagrad på ett företagskort om identifiering av tillämpningen av kortet (krav 190).

```
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.

2.40 **CompanyCardHolderIdentification**

Information som finns lagrad på ett företagskort om identifiering av kortinnehavare (krav 236).

```
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.

2.41 **ControlCardApplicationIdentification**

Information som finns lagrad på ett kontrollkort om identifiering av tillämpning av kortet (krav 190).

```
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.

2.42 **ControlCardControlActivityData**

Information som finns lagrad på ett kontrollkort om den kontrollaktivitet som utförts med kortet (krav 233).

```
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 på det kontrollerade kortet och den medlemsstat som utfärdat det.

controlledVehicleRegistration är registreringsnummer (VRN) och registrerande medlemsstat för det fordon i vilket kontrollen ägde rum.

controlDownloadPeriodBegin och **controlDownloadPeriodEnd** är den period som slutligen överförs.

2.43 **ControlCardHolderIdentification**

Information som finns lagrad på ett kontrollkort om identifiering av kortinnehavare (krav 232).

```
ControlCardHolderIdentification ::= SEQUENCE {
   controlBodyName                          Name,
   controlBodyAddress                       Address,
   cardHolderName                           HolderName,
   cardHolderPreferredLanguage              Language
}
```

controlBodyName är namn på kontrollorganet för kortinnehavaren.

controlBodyAddress är adress till kontrollorganet för kortinnehavaren.

cardHolderName är kontrollkortsinnehavarens namn och förnamn.

cardHolderPreferredLanguage är det språk som kortinnehavaren väljer.

2.44 **ControlType**

Kod som anger de aktiviteter som utförts vid en kontroll. Denna datatyp berörs av krav 102 , 210 och 225.

```
ControlType ::= OCTET STRING (SIZE(1))
```

Värdetilldelning – Oktett Aligned (oktettgrupperad): 'cvpdxxxx'B (8 bitar)

'c'B Kortöverföring.

'0'B: Kortet ej överfört under denna kontrollaktivitet.

'1'B: Kortet överfört under denna kontrollaktivitet.

'v'B Överföring av fordonsenhet:

'0'B: Fordonsenheten ej överförd under denna kontrollaktivitet.

'1'B: Fordonsenheten överförd under denna kontrollaktivitet.

'p'B Utskrift:

'0'B: Ingen utskrift gjord under denna kontrollaktivitet.

'1'B: Utskrift gjord under denna kontrollaktivitet.

'd'B Display:

'0'B: Ingen display använd under denna kontrollaktivitet.

'1'B: Display använd under denna kontrollaktivitet.

'xxxx'B Ej använd.

2.45 **CurrentDateTime**

Färdskrivarens aktuella datum och tidpunkt.

```
CurrentDateTime ::= TimeReal
```

Värdetilldelning: ej närmare angiven.

2.46 **DailyPresenceCounter**

Räknare, som finns lagrad på ett förar- eller verkstadskort, som ökas med ett steg för varje kalenderdag som kortet har satts i en fordonsenhet. Denna datatyp berörs av krav 199 och 219.

```
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.

2.47 **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 inte något datum.

2.48 **Distance**

En tillryggalagd sträcka (resultat av beräkning av skillnaden i kilometer mellan två vägmätarställningar i ett fordon.

```
Distance ::= INTEGER(0..2^16-1)
```

Värdetilldelning: Osignerad binär. Värde i km i området 0 till 9 999 km.

2.49 **DriverCardApplicationIdentification**

Information som finns lagrad på ett förarkort om identifiering av tillämpningen av kortet (krav 190).

```
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 antal händelser per typ av händelse som kortet kan registrera.

noOfFaultsPerType är antal fel per typ av fel som kortet kan registrera.

activityStructureLength anger antal byte som finns tillgängliga för lagring av aktivitetsposter.

noOfCardVehicleRecords är antal fordonsposter som kortet kan lagra.

noOfCardPlaceRecords är antal platser som kortet kan registrera.

2.50 **DriverCardHolderIdentification**

Information som finns lagrad på ett förarkort om identifiering av kortinnehavare (krav 195).

```
DriverCardHolderIdentification ::= SEQUENCE {
   cardHolderName                          HolderName,
   cardHolderBirthDate                     Datef,
   cardHolderPreferredLanguage             Language
}
```

cardHolderName är förarkortsinnehavarens namn och förnamn.

cardHolderBirthDate förarkortsinnehavarens födelsedatum.

cardHolderPreferredLanguage är det språk som kortinnehavaren väljer.

2.51 **EntryTypeDailyWorkPeriod**

Kod för att åtskilja påbörjande och avslutande av en angivelse av plats för ett dagligt arbetspass och angivelsevillkor.

```
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.

2.52 **EquipmentType**

Kod för att åtskilja olika typer av utrustning för färdskrivartillämpningen.

```
EquipmentType ::= INTEGER(0..255)
- - 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).

2.53 **EuropeanPublicKey**

Europeisk öppen nyckel.

```
EuropeanPublicKey ::= PublicKey
```

2.54 **EventFaultType**

Kod för typ av händelse eller fel.

```
EventFaultType ::= OCTET STRING (SIZE(1))
```

Värdetilldelning:

'0x'H	Allmänna händelser.
'00'H	Inga närmare detaljer.
'01'H	Isättning av ett ogiltigt kort.
'02'H	Kortkonflikt.
'03'H	Överlappning av tider.
'04'H	Körning utan korrekt kort.
'05'H	Isättning av kort under körning.
'06'H	Senaste kortsession ej korrekt avslutad.
'07'H	Hastighetsöverträdelse.

'08'H	Avbrott av strömtillförseln.
'09'H	Fel i rörelsedata.
'0A'H .. '0F'H	RFU (reserved for future use – reserverat för framtida användning).
'1x'H	Händelser när det 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 kåpan.
'18'H	Maskinvarusabotage.
'19'H .. '1F'H	RFU.
'2x'H	Händelser av typen 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 kåpan.
'25'H	Maskinvarusabotage.
'26'H .. '2F'H	RFU.
'3x'H	Färdskrivarfel.
'30'H	Inga närmare detaljer.
'31'H	Internt fel i fordonsenheten (VU).
'32'H	Skrivarfel.
'33'H	Displayfel.
'34'H	Överföringsfel.
'35'H	Sensorfel.
'36'H .. '3F'H	RFU.
'4x'H	Kortfel.
'40'H	Inga närmare detaljer.
'41'H .. '4F'H	RFU.
'50'H .. '7F'H	RFU.
'80'H .. 'FF'H	Tillverkarspecifik.

2.55 **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 under ett av de senaste tio dygnen händelsen inträffat.
'04'H	Den allvarligaste händelsen under 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 .. '7F'H	RFU.
'80'H .. 'FF'H	Tillverkarspecifik.

2.56 **ExtendedSerialNumber**

Unik identifiering av en utrustning. Det kan även användas som en identifierare av en utrustnings öppna nyckel.

```
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 nedan.

monthYear är identifiering av månad och år för tillverkning (eller för tilldelning av serienummer).

Värdetilldelning: BCD-kodning för månad (två siffror) och år (två sista siffrorna).

type är en identifierare av typ av utrustning.

Värdetilldelning: Tillverkarspecifik, med 'FFh' som reserverat värde.

manufacturerCode är den numeriska koden för tillverkaren av utrustningen.

2.57 **FullCardNumber**

Kod som identifierar ett färdskrivarkort fullständigt.

```
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.

2.58 **HighResOdometer**

Fordonets vägmätarställning: Sammanlagd sträcka som tillryggalagts av fordonet vid drift.

```
HighResOdometer ::= INTEGER(0..2^32-1)
```

Värdetilldelning: Osignerad binär. Värde i 1/200 km i området 0 till 21 055 406 km.

2.59 **HighResTripDistance**

En sträcka som tillryggalagts under en hel eller en del av en resa.

```
HighResTripDistance ::= INTEGER(0..2^32-1)
```

Värdetilldelning: Osignerad binär. Värde i 1/200 km i området 0 till 21 055 406 km.

2.60 **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.

2.61 **K-ConstantOfRecordingEquipment**

Färdskrivarens konstant (definition m)).

```
K-ConstantOfRecordingEquipment ::= INTEGER(0..2^16-1)
```

Värdetilldelning: Pulser per kilometer i området 0 till 64 255 pulser/km.

2.62 **KeyIdentifier**

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

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

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.

2.63 **L-TyreCircumference**

Däckens effektiva omkrets (definition u)):

```
L-TyreCircumference ::= INTEGER(0..2^16-1)
```

Värdetilldelning: Osignerad binär, värde i 1/8 mm i området 0 till 8 031 mm.

2.64 **Language**

Kod för ett språk.

```
Language ::= IA5String(SIZE(2))
```

Värdetilldelning: Kodning med två gemener enligt ISO 639.

2.65 **LastCardDownload**

Datum och tidpunkt, som finns lagrade på förarkortet, för den senaste kortöverföringen (för andra än kontrolländamål). Detta datum kan uppdateras av en fordonsenhet och alla typer av kortläsare.

```
LastCardDownload ::= TimeReal
```

Värdetilldelning: Ej närmare angiven.

2.66 **ManualInputFlag**

Kod som anger om en kortinnehavare manuellt har angivit föraraktiviteter vid kortisättning eller inte (krav 081).

```
ManualInputFlag ::= INTEGER {
   noEntry                          (0)
   manualEntries                    (1)
}
```

Värdetilldelning: Ej närmare angiven.

2.67 **ManufacturerCode**

Kod som anger en tillverkare.

```
ManufacturerCode ::= INTEGER(0..255)
```

Värdetilldelning:

'00'H	Ingen information tillgänglig.
'01'H	Reserverat värde.
'02'H .. '0F'H	Reserverat för framtida användning.
'10'H	ACTIA
'11'H .. '17'H	Reserverat för tillverkare vars namn börjar med 'A'.
'18'H .. '1F'H	Reserverat för tillverkare vars namn börjar med 'B'.
'20'H .. '27'H	Reserverat för tillverkare vars namn börjar med 'C'.
'28'H .. '2F'H	Reserverat för tillverkare vars namn börjar med 'D'.
'30'H .. '37'H	Reserverat för tillverkare vars namn börjar med 'E'.
'38'H .. '3F'H	Reserverat för tillverkare vars namn börjar med 'F'.
'40'H	Giesecke & Devrient GmbH
'41'H	GEM plus
'42'H .. '47'H	Reserverat för tillverkare vars namn börjar med 'G'.
'48'H .. '4F'H	Reserverat för tillverkare vars namn börjar med 'H'.
'50'H .. '57'H	Reserverat för tillverkare vars namn börjar med 'I'.
'58'H .. '5F'H	Reserverat för tillverkare vars namn börjar med 'J'.
'60'H .. '67'H	Reserverat för tillverkare vars namn börjar med 'K'.
'68'H .. '6F'H	Reserverat för tillverkare vars namn börjar med 'L'.
'70'H .. '77'H	Reserverat för tillverkare vars namn börjar med 'M'.
'78'H .. '7F'H	Reserverat för tillverkare vars namn börjar med 'N'.
'80'H	OSCARD
'81'H .. '87'H	Reserverat för tillverkare vars namn börjar med 'O'.
'88'H .. '8F'H	Reserverat för tillverkare vars namn börjar med 'P'.
'90'H .. '97'H	Reserverat för tillverkare vars namn börjar med 'Q'.
'98'H .. '9F'H	Reserverat för tillverkare vars namn börjar med 'R'.
'A0'H	SETEC
'A1'H	SIEMENS VDO
'A2'H	STONERIDGE
'A3'H .. 'A7'H	Reserverat för tillverkare vars namn börjar med 'S'.
'AA'H	TACHOCONTROL
'AB'H .. 'AF'H	Reserverat för tillverkare vars namn börjar med 'T'
'B0'H .. 'B7'H	Reserverat för tillverkare vars namn börjar med 'U'
'B8'H .. 'BF'H	Reserverat för tillverkare vars namn börjar med 'V'
'C0'H .. 'C7'H	Reserverat för tillverkare vars namn börjar med 'W'
'C8'H .. 'CF'H	Reserverat för tillverkare vars namn börjar med 'X'
'D0'H .. 'D7'H	Reserverat för tillverkare vars namn börjar med 'Y'
'D8'H .. 'DF'H	Reserverat för tillverkare vars namn börjar med 'Z'

2.68 **MemberStateCertificate**

Certifikat för en medlemsstats öppna nyckel utfärdat av den europeiska certifieringsinstansen.

```
MemberStateCertificate ::= Certificate
```

2.69 **MemberStatePublicKey**

En medlemsstats öppna nyckel.

```
MemberStatePublicKey ::= PublicKey
```

2.70 **Name**

Ett namn.

```
Name ::= SEQUENCE {
   codePage                                    INTEGER (0..255),
   name                                        OCTET STRING (SIZE(35))
}
```

codePage specificerar den del av ISO/IEC 8859 som används för att koda namnet,

name är ett namn som kodats enligt ISO/IEC 8859-codePage.

2.71 **NationAlpha**

Alfabetisk referens för ett land, i överensstämmelse med landsbeteckningar på bilar, och/eller som används på internationellt harmoniserade handlingar för fordonsförsäkringar (grönt kort).

```
NationAlpha ::= IA5String(SIZE(3))
```

Värdetilldelning:

' '	Ingen information tillgänglig
'A'	Österrike
'AL'	Albanien
'AND'	Andorra
'ARM'	Armenien
'AZ'	Azerbajdzjan
'B'	Belgien
'BG'	Bulgarien
'BIH'	Bosnien och Herzegovina
'BY'	Vitryssland
'CH'	Schweiz
'CY'	Cypern
'CZ'	Tjeckien
'D'	Tyskland
'DK'	Danmark
'E'	Spanien
'EST'	Estland
'F'	Frankrike
'FIN'	Finland
'FL'	Liechtenstein
'FR'	Färöarna
'UK'	Förenade kungariket, Alderney, Guernsey, Jersey, Isle of Man, Gibraltar
'GE'	Georgien
'GR'	Grekland
'H'	Ungern
'HR'	Kroatien
'I'	Italien
'IRL'	Irland
'IS'	Island
'KZ'	Kazakstan
'L'	Luxemburg
'LT'	Litauen
'LV'	Lettland
'M'	Malta
'MC'	Monaco

'MD'	Moldova
'MK'	Makedonien
'N'	Norge
'NL'	Nederländerna
'P'	Portugal
'PL'	Poland
'RO'	Rumänien
'RSM'	San Marino
'RUS'	Ryssland
'S'	Sverige
'SK'	Slovakien
'SLO'	Slovenien
'TM'	Turkmenistan
'TR'	Turkiet
'UA'	Ukraina
'V'	Vatikanstaten
'YU'	Jugoslavien
'UNK'	Okänd
'EC'	Europeiska gemenskapen
'EUR'	Resten av Europa
'WLD'	Resten av världen

2.72 **NationNumeric**

Numerisk referens för ett land.

`NationNumeric ::= INTEGER(0..255)`

Värdetilldelning:

-- Ingen information tillgänglig	(00)H,
-- Austria	(01)H,
-- Albania	(02)H,
-- Andorra	(03)H,
-- Armenia	(04)H,
-- Azerbaijan	(05)H,
-- Belgium	(06)H,
-- Bulgaria	(07)H,
-- Bosnia and Herzegovina	(08)H,
-- Belarus	(09)H,
-- Switzerland	(0A)H,
-- Cyprus	(0B)H,
-- Czech Republic	(0C)H,
-- Germany	(0D)H,
-- Denmark	(0E)H,
-- Spain	(0F)H,
-- Estonia	(10)H,
-- France	(11)H,
-- Finland	(12)H,
-- Liechtenstein	(13)H,
-- Faeroe Islands	(14)H,
-- United Kingdom	(15)H,
-- Georgia	(16)H,
-- Greece	(17)H,
-- Hungary	(18)H,
-- Croatia	(19)H,
-- Italy	(1A)H,
-- Ireland	(1B)H,
-- Iceland	(1C)H,

- - Kazakhstan	(1D)H,
- - Luxembourg	(1E)H,
- - Lithuania	(1F)H,
- - Latvia	(20)H,
- - Malta	(21)H,
- - Monaco	(22)H,
- - Republic of Moldova	(23)H,
- - Macedonia	(24)H,
- - Norway	(25)H,
- - Netherlands	(26)H,
- - Portugal	(27)H,
- - Poland	(28)H,
- - Romania	(29)H,
- - San Marino	(2A)H,
- - Russian Federation	(2B)H,
- - Sweden	(2C)H,
- - Slovakia	(2D)H,
- - Slovenia	(2E)H,
- - Turkmenistan	(2F)H,
- - Turkey	(30)H,
- - Ukraine	(31)H,
- - Vatican City	(32)H,
- - Yugoslavia	(33)H,
- - RFU	(34..FC)H,
- - European Community	(FD)H,
- - Rest of Europe	(FE)H,
- - Rest of the world	(FF)H

2.73 **NoOfCalibrationRecords**

Antal kalibreringsposter som ett verkstadskort kan lagra.

`NoOfCalibrationRecords ::= INTEGER(0..255)`

Värdetilldelning: se punkt 3.

2.74 **NoOfCalibrationsSinceDownload**

Räknare som anger det antal kalibreringar som utförts med ett verkstadskort sedan den senaste överföringen från det (krav 230).

`NoOfCalibrationsSinceDownload ::= INTEGER(0..2`^{16}`-1),`

Värdetilldelning: Ej närmare angiven.

2.75 **NoOfCardPlaceRecords**

Antal platsposter som ett förar- eller verkstadskort kan lagra.

`NoOfCardPlaceRecords ::= INTEGER(0..255)`

Värdetilldelning: se punkt 3.

2.76 **NoOfCardVehicleRecords**

Antal poster för använda fordon som ett förar- eller verkstadskort kan lagra.

`NoOfCardVehicleRecords ::= INTEGER(0..2`^{16}`-1)`

Värdetilldelning: se punkt 3.

2.77 **NoOfCompanyActivityRecords**

Antal poster för företagsaktiviteter som ett företagskort kan lagra.

`NoOfCompanyActivityRecords ::= INTEGER(0..2`^{16}`-1)`

Värdetilldelning: se punkt 3.

2.78 **NoOfControlActivityRecords**

Antal poster för kontrollaktiviteter som ett kontrollkort kan lagra.

```
NoOfControlActivityRecords ::= INTEGER(0..2^16-1)
```

Värdetilldelning: se punkt 3.

2.79 **NoOfEventsPerType**

Antal händelser per typ av händelse som ett kort kan lagra.

```
NoOfEventsPerType ::= INTEGER(0..255)
```

Värdetilldelning: se punkt 3.

2.80 **NoOfFaultsPerType**

Antal fel per typ av fel som ett kort kan lagra.

```
NoOfFaultsPerType ::= INTEGER(0..255)
```

Värdetilldelning: se punkt 3.

2.81 **OdometerValueMidnight**

Fordonets vägmätarställning vid midnatt ett visst datum (krav 090).

```
OdometerValueMidnight ::= OdometerShort
```

Värdetilldelning: Ej närmare angiven.

2.82 **OdometerShort**

Fordonets vägmätarställning i kortform.

```
OdometerShort ::= INTEGER(0..2^24-1)
```

Värdetilldelning: Osignerad binär. Värde i km i området 0 till 9 999 999 km.

2.83 **OverspeedNumber**

Antal händelser av typen hastighetsöverträdelse sedan senaste kontroll 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.

2.84 **PlaceRecord**

Information om en plats där dagens arbetspass påbörjas eller avslutas (krav 087, 202, 221).

```
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.

2.85 **PreviousVehicleInfo**

Information om det fordon som tidigare använts av en förare när han sätter i sitt kort i en fordonsenhet (krav 081).

```
PreviousVehicleInfo ::= SEQUENCE {
   vehicleRegistrationIdentification        VehicleRegistrationIdentification,
   cardWithdrawalTime                       TimeReal
}
```

VehicleRegistrationIdentification är fordonets registreringsnummer och den medlemsstat där fordonet är registrerat.

cardWithdrawalTime är tidpunkt och datum för urtagning av kort.

2.86 **PublicKey**

En öppen RSA-nyckel.

```
PublicKey ::= SEQUENCE {
   rsaKeyModulus                            RSAKeyModulus,
   rsaKeyPublicExponent                     RSAKeyPublicExponent
}
```

rsaKeyModulus är modulus för nyckelparet.

rsaKeyPublicExponent är den öppna exponenten för nyckelparet.

2.87 **RegionAlpha**

Alfabetisk referens för en region i ett visst land.

```
RegionAlpha ::= IA5STRING(SIZE(3))
```

Värdetilldelning:

' '	Ingen information tillgänglig

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

2.88 **RegionNumeric**

Numerisk referens för en region i ett visst land.

```
RegionNumeric ::= OCTET STRING (SIZE(1))
```

Värdetilldelning:

'00'H	Ingen information tillgänglig,

España:

'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

2.89 **RSAKeyModulus**

Modulus för ett RSA-nyckelpar.

```
RSAKeyModulus ::= OCTET STRING (SIZE(128))
```

Värdetilldelning: Ospecificerad.

2.90 **RSAKeyPrivateExponent**

Hemlig exponent för ett RSA-nyckelpar.

```
RSAKeyPrivateExponent ::= OCTET STRING (SIZE(128))
```

Värdetilldelning: Ospecificerad.

2.91 **RSAKeyPublicExponent**

Öppen exponent för ett RSA-nyckelpar.

```
RSAKeyPublicExponent ::= OCTET STRING (SIZE(8))
```

Värdetilldelning: Ospecificerad.

2.92 **SensorApprovalNumber**

Sensorns typgodkännandenummer.

```
SensorApprovalNumber ::= IA5String(SIZE(8))
```

Värdetilldelning: Ospecificerad.

2.93 **SensorIdentification**

Information som finns lagrad i en rörelsesensor om identifiering av rörelsesensorn (krav 077).

```
SensorIdentification ::= SEQUENCE {
   sensorSerialNumber                    SensorSerialNumber,
   sensorApprovalNumber                  SensorApprovalNumber,
   sensorSCIdentifier                    SensorSCIdentifier,
   sensorOSIdentifier                    SensorOSIdentifier
}
```

sensorSerialNumber är rörelsesensorns utökade serienummer (inbegripet delnummer och tillverkarens kod).

sensorApprovalNumber är rörelsesensorns godkännandenummer.

sensorSCIdentifier är identifierare av rörelsesensorns säkerhetskomponent.

sensorOSIdentifier är identifierare av rörelsesensorns operativsystem.

2.94 **SensorInstallation**

Information som finns lagrad i en rörelsesensor om installation av rörelsesensorn (krav 099).

```
SensorInstallation ::= SEQUENCE {
   sensorPairingDateFirst                  SensorPairingDate,
   firstVuApprovalNumber                   VuApprovalNumber,
   firstVuSerialNumber                     VuSerialNumber,
   sensorPairingDateCurrent                SensorPairingDate,
   currentVuApprovalNumber                 VuApprovalNumber,
   currentVUSerialNumber                   VuSerialNumber
}
```

sensorPairingDateFirst är datum för första hopkoppling av rörelsesensorn med en fordonsenhet.

firstVuApprovalNumber är godkännandenummer för den första fordonsenhet som koppas ihop med rörelsesensorn.

firstVuSerialNumber är serienummer för den första fordonsenhet som koppas ihop med rörelsesensorn.

sensorPairingDateCurrent är datum för innevarande hopkoppling av rörelsesensorn med fordonsenheten.

currentVuApprovalNumber är godkännandenummer för den fordonsenhet som för närvarande är hopkopplad med rörelsesensorn.

currentVuSerialNumber är serienummer för den fordonsenhet som för närvarande är hopkopplad med rörelsesensorn.

2.95 **SensorInstallationSecData**

Information som finns lagrad på ett verkstadskort om de säkerhetsdata som behövs för att koppla ihop rörelsesensorer med fordonsenheter (krav 214).

```
SensorInstallationSecData ::= TDesSessionKey
```

Värdetilldelning: Enligt ISO 16844-3.

2.96 **SensorOSIdentifier**

Identifierare av rörelsesensorns operativsystem.

```
SensorOSIdentifier ::= IA5String(SIZE(2))
```

Värdetilldelning: Tillverkarspecifik

2.97 **SensorPaired**

Information som finns lagrad i en fordonsenhet om identifiering av den rörelsesensor som är hopkopplad med fordonsenheten (krav 079).

```
SensorPaired ::= SEQUENCE {
   sensorSerialNumber                      SensorSerialNumber,
   sensorApprovalNumber                    SensorApprovalNumber,
   sensorPairingDateFirst                  SensorPairingDate
}
```

sensorSerialNumber är serienummer på den rörelsesensor som för närvarande är hopkopplad med fordonsenheten.

sensorApprovalNumber är godkännandenummer på den rörelsesensor som för närvarande är hopkopplad med fordonsenheten.

sensorPairingDateFirst är datum för första hopkoppling med en fordonsenhet av den rörelsesensor som för närvarande är hopkopplad med fordonsenheten.

2.98 **SensorPairingDate**

Datum för hopkoppling av rörelsesensorn med en fordonsenhet.

```
SensorPairingDate ::= TimeReal
```

Värdetilldelning: Ospecificerad.

2.99 **SensorSerialNumber**

Rörelsesensorns serienummer.

```
SensorSerialNumber ::= ExtendedSerialNumber
```

2.100 **SensorSCIdentifier**

Identifierare av rörelsesensorns säkerhetskomponent.

```
SensorSCIdentifier ::= IA5String(SIZE(8))
```

Värdetilldelning: Specifik för komponenttillverkaren.

2.101 **Signature**

En digital signatur.

```
Signature ::= OCTET STRING (SIZE(128))
```

Värdetilldelning: Enligt tillägg 11 (Gemensamma säkerhetsmekanismer).

2.102 **SimilarEventsNumber**

Antal liknande händelser under en viss dag (krav 094).

```
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.

2.103 **SpecificConditionType**

Kod för identifiering av särskild omständighet (krav 050b, 105a, 212a och 230a).

```
SpecificConditionType ::= INTEGER(0..255)
```

Värdetilldelning:

'00'H	RFU (reserved for future use – reserverat för framtida användning).
'01'H	Omfattas ej – Början.
'02'H	Omfattas ej – Slut.
'03'H	Transport med färja/tåg.
'04'H .. 'FF'H	RFU

2.104 **SpecificConditionRecord**

Information som finns lagrad på ett förarkort, ett verkstadskort eller i en fordonsenhet om en särskild omständighet (krav 105a, 212a och 230a).

```
SpecificConditionRecord ::= SEQUENCE {
   entryTime                                TimeReal,
   specificConditionType                    SpecificConditionType
}
```

entryTime är datum och tidpunkt för angivelsen.

specificConditionType är koden för identifiering av den särskilda omständigheten.

2.105 **Speed**

Fordonets hastighet (km/h).

```
Speed ::= INTEGER(0..255)
```

Värdetilldelning: Kilometer per timme i området 0 till 220 km/h.

2.106 **SpeedAuthorised**

Högsta tillåtna hastighet för fordonet (definition bb)).

```
SpeedAuthorised ::= Speed
```

2.107 **SpeedAverage**

Genomsnittlig hastighet under en tidigare fastställd tidsperiod (km/h).

```
SpeedAverage ::= Speed
```

2.108 **SpeedMax**

Högsta hastighet uppmätt under en tidigare fastställd tidsperiod.

```
SpeedMax ::= Speed
```

2.109 **TDesSessionKey**

En tripleDES sessionsnyckel.

```
TDesSessionKey ::= SEQUENCE {
   tDesKeyA                                 OCTET STRING (SIZE(8))
   tDesKeyB                                 OCTET STRING (SIZE(8))
}
```

Värdetilldelning: Ej närmare angiven.

2.110 **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 – Octet Aligned (oktettgrupperad) Antal sekunder sedan midnatt den 1 januari 1970 GMT.

Senaste möjliga datum/tidpunkt är under år 2106.

2.111 **TyreSize**

Angivelse av däckens dimensioner.

```
TyreSize ::= IA5String(SIZE(15))
```

Värdetilldelning: Enligt direktiv 92/23/EEG, EGT L 129, 31.3.1992, s. 95.

2.112 **VehicleIdentificationNumber**

Fordonets chassinummer (VIN) avseende fordonet som helhet, vanligtvis ramnummer eller serienummer på chassiet.

```
VehicleIdentificationNumber ::= IA5String(SIZE(17))
```

Värdetilldelning: Enligt definition i ISO 3779.

2.113 **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.

vehicleRegistrationNumber är fordonets registreringsnummer (VRN).

2.114 **VehicleRegistrationNumber**

Fordonets registreringsnummer (VRN). Registreringsnumret tilldelas av myndigheten för fordonsregistrering.

```
VehicleRegistrationNumber ::= SEQUENCE {
   codePage                                 INTEGER (0..255),
   vehicleRegNumber                         OCTET STRING (SIZE(13))
}
```

codePage specificerar den del av ISO/IEC 8859 som används för att koda vehicleRegNumber,

vehicleRegNumber är ett registreringsnummer för ett fordon som kodats enligt ISO/IEC 8859-codePage.

Värdetilldelning: Landsspecifik.

2.115 **VuActivityDailyData**

Information som finns lagrad i en fordonsenhet om ändringar av aktivitet och/eller ändringar av körningsstatus och/eller ändringar av kortstatus under en viss kalenderdag (krav 084) 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.

2.116 **VuApprovalNumber**

Fordonsenhetens typgodkännandenummer.

```
VuApprovalNumber ::= IA5String(SIZE(8))
```

Värdetilldelning: Ospecificerad.

2.117 **VuCalibrationData**

Information som finns lagrad i en fordonsenhet om kalibreringar av färdskrivaren (krav 098).

```
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.

2.118 **VuCalibrationRecord**

Information som finns lagrad i en fordonsenhet om en kalibrering av färdskrivaren (krav 098).

```
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 chassinummer (VIN).

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 tid.

nextCalibrationDate är datum för nästa kalibrering av den typ som anges i CalibrationPurpose som skall utföras av den auktoriserade besiktningsmyndigheten.

2.119 **VuCardIWData**

Information som finns lagrad i en fordonsenhet om cykler med isättning och urtagning av förarkort eller verkstadskort i fordonsenheten (krav 081).

```
VuCardIWData ::= SEQUENCE {
   noOfIWRecords                         INTEGER(0..216-1),
   vuCardIWRecords SET                   SIZE(noOfIWRecords) OF
                                         VuCardIWRecord
}
```

noOfIWRecords är antalet poster i mängden vuCardWRecords.

vuCardIWRecords är en mängd poster för cykler med isättning/urtagning av kort.

2.120 **VuCardIWRecord**

Information som finns lagrad i en fordonsenhet om en cykel med isättning och urtagning av förarkort eller verkstadskort i fordonsenheten (krav 081).

```
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.

cardExpiryDate är kortets sista giltighetsdatum sådant det lagrats på kortet.

cardInsertionTime är datum och tidpunkt för isättning.

vehicleOdometerValueAtInsertion är vägmätarställning när kortet sattes i.

cardSlotNumber är den kortplats som kortet sätts in i.

cardWithdrawalTime är tidpunkt och datum för urtagning.

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 angivit föraraktiviteter vid kortisättning.

2.121 **VuCertificate**

Certifikat för en fordonsenhets öppna nyckel.

```
VuCertificate ::= Certificate
```

2.122 **VuCompanyLocksData**

Information som finns lagrad i en fordonsenhet om företagslås (krav 104).

```
VuCompanyLocksData ::= SEQUENCE {
   noOfLocks                               INTEGER(0..20),
   vuCompanyLocksRecords                   SET SIZE(noOfLocks) OF
                                           VuCompanyLocksRecord
}
```

noOfLocks är antalet lås som finns förtecknade i vuCompanyLocksRecords.

vuCompanyLocksRecords är mängden poster för företagslås.

2.123 **VuCompanyLocksRecord**

Information som finns lagrad i en fordonsenhet om ett företagslås (krav 104).

```
VuCompanyLocksRecord ::= SEQUENCE {
   lockInTime                          TimeReal,
   lockOutTime                         TimeReal,
   companyName                         Name,
   companyAddress                      Address,
   companyCardNumber                   FullCardNumber
}
```

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.

2.124 **VuControlActivityData**

Information som finns lagrad i en fordonsenhet om kontroller som utförs med användning av denna fordonsenhet (krav 102).

```
VuControlActivityData ::= SEQUENCE {
   noOfControls                        INTEGER(0..20),
   vuControlActivityRecords            SET SIZE(noOfControls) OF
                                       VuControlActivityRecord
}
```

noOfControls är antalet kontroller som finns förtecknade i vuControlActivityRecords.

vuControlActivityRecords är mängden poster för kontrollaktiviteter.

2.125 **VuControlActivityRecord**

Information som finns lagrad i en fordonsenhet om en kontroll som utförts med användning av denna fordonsenhet (krav 102).

```
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.

2.126 **VuDataBlockCounter**

Räknare som finns lagrad på ett kort och som sekventiellt identifierar cyklerna med isättning och urtagning av kort i fordonsenheter.

```
VuDataBlockCounter ::= BCDString(SIZE(2))
```

Värdetilldelning: Löpnummer med högsta värde 9 999, som börjar åter från 0.

2.127 **VuDetailedSpeedBlock**

Information som finns lagrad i en fordonsenhet om fordonets hastighet i detalj under en minut under vilken fordonet har varit i rörelse (krav 093).

```
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 börjar vid speedBlockBeginDate (fr.o.m.).

2.128 **VuDetailedSpeedData**

Information som finns lagrad i en fordonsenhet om fordonets hastighet i detalj.

```
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 hastighet i detalj.

2.129 **VuDownloadablePeriod**

Äldsta och senaste datum för vilka en fordonsenhet har data om föraraktiviteter (krav 081, 084 eller 087).

```
VuDownloadablePeriod ::= SEQUENCE {
   minDownloadableTime                    TimeReal
   maxDownloadableTime                    TimeReal
}
```

minDownloadableTime är äldsta datum och tidpunkt för kortisättning, aktivitetsändring eller angivelse av plats som finns lagrat i fordonsenheten.

maxDownloadableTime är senaste datum och tidpunkt för korturtagning, aktivitetsändring eller angivelse av plats som finns lagrat i fordonsenheten.

2.130 **VuDownloadActivityData**

Information som finns lagrad i en fordonsenhet om senaste överföring från den (krav 105).

```
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.

2.131 **VuEventData**

Information som finns lagrad i en fordonsenhet om händelser (krav 094, 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.

2.132 **VuEventRecord**

Information som finns lagrad i en fordonsenhet om en händelse (krav 094, utom händelse av typen hastighetsöverträdelse).

```
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 satts i förarens kortplats vid händelsens början.

cardNumberCodriverSlotBegin identifierar det kort som satts i medförarens kortplats vid händelsens början.

cardNumberDriverSlotEnd identifierar det kort som satts i förarens kortplats vid händelsens slut.

cardNumberCodriverSlotEnd identifierar det kort som satts i medförarens kortplats vid händelsens slut.

similarEventsNumber är antalet liknande händelser den dagen.

Denna sekvens skall användas vid alla händelse utom händelser av typen hastighetsöverträdelse.

2.133 **VuFaultData**

Information som finns lagrad i en fordonsenhet om fel (krav 096).

```
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.

2.134 **VuFaultRecord**

Information som finns lagrad i en fordonsenhet om ett fel (krav 096).

```
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 satts i förarens kortplats vid felets början.

cardNumberCodriverSlotBegin identifierar det kort som satts i medförarens kortplats vid felets början.

cardNumberDriverSlotEnd identifierar det kort som satts i förarens kortplats vid felets slut.

cardNumberCodriverSlotEnd identifierar det kort som satts i medförarens kortplats vid felets slut.

2.135 **VuIdentification**

Information som finns lagrad i en fordonsenhet om identifiering av fordonsenheten (krav 075).

```
VuIdentification ::= SEQUENCE {
   vuManufacturerName                  VuManufacturerName,
   vuManufacturerAddress               VuManufacturerAddress,
   vuPartNumber                        VuPartNumber,
   vuSerialNumber                      VuSerialNumber,
   vuSoftwareIdentification            VuSoftwareIdentification,
   vuManufacturingDate                 VuManufacturingDate,
   vuApprovalNumber                    VuApprovalNumber
}
```

vuManufacturerName är namnet på tillverkaren av fordonsenheten.

vuManufacturerAddress är adressen till tillverkaren av fordonsenheten.

vuPartNumber är fordonsenhetens delnummer.

vuSerialNumber är fordonsenhetens serienummer.

vuSoftwareIdentification identifierar den programvara som används i fordonsenheten.

vuManufacturingDate är fordonsenhetens tillverkningsdatum.

vuApprovalNumber är fordonsenhetens typgodkännandenummer.

2.136 **VuManufacturerAddress**

Adress till tillverkaren av fordonsenheten.

```
VuManufacturerAddress ::= Address
```

Värdetilldelning: Ospecificerad.

2.137 **VuManufacturerName**

Namn på tillverkaren av fordonsenheten.

```
VuManufacturerName ::= Name
```

Värdetilldelning: Ospecificerad.

2.138 **VuManufacturingDate**

Fordonsenhetens tillverkningsdatum.

```
VuManufacturingDate ::= TimeReal
```

Värdetilldelning: Ospecificerad.

2.139 **VuOverSpeedingControlData**

Information som finns lagrad i en fordonsenhet om händelser av typen hastighetsöverträdelse sedan den senaste kontrollen av hastighetsöverträdelse (krav 095).

```
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.

2.140 **VuOverSpeedingEventData**

Information som finns lagrad i en fordonsenhet om händelser av typen hastighetsöverträdelse (krav 094).

```
VuOverSpeedingEventData ::= SEQUENCE {
   noOfVuOverSpeedingEvents                INTEGER(0..255),
   vuOverSpeedingEventRecords              SET SIZE(noOfVuOverSpeedingEvents) OF
                                           VuOverSpeedingEventRecord
}
```

noOfVuOverSpeedingEvents är det antal händelser som finns förtecknade i mängden vuOverSpeedingEventRecords.

vuOverSpeedingEventRecords är en mängd poster för händelser av typen hastighetsöverträdelse.

2.141 **VuOverSpeedingEventRecord**

Information som finns lagrad i en fordonsenhet om händelser av typen hastighetsöverträdelse (krav 094).

```
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.

cardNumberDriverSlotBegin identifierar det kort som sattes i förarens kortplats vid händelsens början.

similarEventsNumber är antalet liknande händelser samma dag.

2.142 **VuPartNumber**

Fordonsenhetens delnummer.

```
VuPartNumber ::= IA5String(SIZE(16))
```

Värdetilldelning: Specifik för tillverkaren av fordonsenheter.

2.143 **VuPlaceDailyWorkPeriodData**

Information som finns lagrad i en fordonsenhet om de platser där förarna påbörjar eller avslutar dagens arbetspass (krav 087).

```
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.

2.144 **VuPlaceDailyWorkPeriodRecord**

Information som finns lagrad i en fordonsenhet om en plats där en förare påbörjar eller avslutar dagens arbetspass (krav 087).

```
VuPlaceDailyWorkPeriodRecord ::= SEQUENCE {

   fullCardNumber                            FullCardNumber,

   placeRecord                               PlaceRecord

}
```

fullCardNumber är förarens korttyp, utfärdande medlemsstat och kortnummer.

placeRecord innehåller information om den plats som angivits.

2.145 **VuPrivateKey**

En fordonsenhets privata nyckel.

```
VuPrivateKey ::= RSAKeyPrivateExponent
```

2.146 **VuPublicKey**

En fordonsenhets öppna nyckel.

```
VuPublicKey ::= PublicKey
```

2.147 **VuSerialNumber**

Fordonsenhetens serienummer (krav 075).

```
VuSerialNumber ::= ExtendedSerialNumber
```

2.148 **VuSoftInstallationDate**

Datum för installation av fordonsenhetens programvaruversion.

```
VuSoftInstallationDate ::= TimeReal
```

Värdetilldelning: Ospecificerad.

2.149 **VuSoftwareIdentification**

Information som finns 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.

2.150 **VuSoftwareVersion**

Nummer på programvaruversionen i fordonsenheten.

```
VuSoftwareVersion ::= IA5String(SIZE(4))
```

Värdetilldelning: Ospecificerad.

2.151 **VuSpecificConditionData**

Information som finns 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 för särskilda omständigheter.

2.152 **VuTimeAdjustmentData**

Information som finns lagrad i en fordonsenhet om tidsinställningar som inte utförts vid en normal kalibrering (krav 101).

```
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.

2.153 **VuTimeAdjustmentRecord**

Information som finns lagrad i en fordonsenhet om en tidsinställning som inte utförts vid en normal kalibrering (krav 101).

```
VuTimeAdjustmentRecord ::= SEQUENCE {
   oldTimeValue                              TimeReal,
   oldTimeValue                              TimeReal,
   newTimeValue                              TimeReal,
   workshopName                              Name,
   workshopAddress                           Address,
   workshopCardNumber                        FullCardNumber
}
```

oldTimeValue, newTimeValue är de gamla och nya värdena för datum och tid.

workshopName, workshopAddress är verkstadens namn och adress.

workshopCardNumber identifierar det verkstadskort som används för att utföra tidsinställningen.

2.154 **W-VehicleCharacteristicConstant**

Fordonets karakteristiska koefficient (definition k)).

```
W-VehicleCharacteristicConstant ::= INTEGER(0..2^16-1))
```

Värdetilldelning: Impulser per kilometer i området 0 till 64 255 impulser/km.

2.155 **WorkshopCardApplicationIdentification**

Information som finns lagrad på ett verkstadskort om identifiering av tillämpningen av kortet (krav 190).

```
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 poster för aktiviteter.

noOfCardVehicleRecords är antal platser som kortet kan registrera.

noOfCardPlaceRecords är det antal kalibreringsposter som kortet kan lagra.

noOfCalibrationRecords är det antal fordonsposter som kortet kan lagra.

2.156 **WorkshopCardCalibrationData**

Information som finns lagrad på ett verkstadskort om verkstadsaktivitet som utförts med kortet (krav 227).

```
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.

2.157 **WorkshopCardCalibrationRecord**

Information som finns lagrad på ett verkstadskort om en kalibrering som utförts med kortet (krav 227).

```
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 chassinummer (VIN).

vehicleRegistration 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 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 tid.

nextCalibrationDate är datum för nästa kalibrering av den typ som anges i CalibrationPurpose och som skall utföras av den auktoriserade besiktningsmyndigheten.

vuPartNumber, vuSerialNumber och **sensorSerialNumber** är dataelementen för identifiering av färdskrivare.

2.158 **WorkshopCardHolderIdentification**

Information som finns lagrad på ett verkstadskort om identifiering av kortinnehavaren (krav 216).

```
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.

2.159 **WorkshopCardPIN**

Verkstadskortets personliga identifieringsnummer (krav 213).

```
WorkshopCardPIN ::= IA5String(SIZE(8))
```

Värdetilldelning: Den PIN-kod som kortinnehavaren har, högerutfylld med 'FF'-byte upp till 8 byte.

3. DEFINITIONER AV STORLEKS- OCH VÄRDEOMRÅDEN

Definition av variabler som används för definitioner i punkt 2.

`TimeRealRange ::= 2^32-1`

3.1 **Definitioner för förarkortet:**

Variabelns namn	Min	Max
`CardActivityLengthRange`	5 544 bytes (28 dagar 93 aktivitetsändringar per dag)	13 776 bytes (28 dagar 240 aktivitetsändringar per dag)
`NoOfCardPlaceRecords`	84	112
`NoOfCardVehicleRecords`	84	200
`NoOfEventsPerType`	6	12
`NoOfFaultsPerType`	12	24

3.2 **Definitioner för verkstadskortet:**

Variabelns namn	Min	Max
`CardActivityLengthRange`	198 bytes (1 dag 93 aktivitetsändringar)	492 bytes (1 dag 240 aktivitetsändringar)
`NoOfCardPlaceRecords`	6	8
`NoOfCardVehicleRecords`	4	8
`NoOfEventsPerType`	3	3
`NoOfFaultsPerType`	6	6
`NoOfCalibrationRecords`	88	255

3.3 **Definitioner för kontrollkortet:**

Variabelns namn	Min	Max
`NoOfControlActivityRecords`	230	520

3.4 **Definitioner för företagskortet:**

Variabelns namn	Min	Max
`NoOfCompanyActivityRecords`	230	520

4. TECKENMÄNGDER

IA5Strings använder ASCII-tecken enligt ISO/IEC 8824-1. För läsbarhet och för enkel referering ges värdetilldelningen nedan. ISO/IEC 8824-1 ersätter denna anmärkning vid bristande överensstämmelse.

```
! " # $ % & ' ( ) * + , - . / 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 och 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 och z { | } ~
```

Andra teckensträngar (Address, Name, VehicleRegistrationNumber) använder dessutom de tecken som definieras genom koderna 192 till 255 i ISO/IEC 8859-1 (teckenmängden Latin1) eller ISO/IEC 8859-7 (grekisk teckenmängd).

5. KODNING

När alla definierade datafält är kodade med kodningsreglerna ASN.1 skall de kodas enligt ISO/IEC 8825-2, anpassad (aligned) variant.

Tillägg 2

SPECIFICERING AV FÄRDSKRIVARKORT

INNEHÅLL

1. INLEDNING

1.1 **Förkortningar**

Följande förkortningar används i detta tillägg:

AC	Access conditions – Tillträdesvillkor
AID	Application Identifier – Tillämpningsidentifierare
ALW	Always – Alltid
APDU	Application Protocol Data Unit – Tillämpningsprotokolls dataenhet (ett kommandos struktur)
ATR	Answer To Reset – Återställningssignal
AUT	Authenticated – Autentiserad
C6, C7	Kontakt nr 6 och 7 på kortet enligt ISO/IEC 7816-2
cc	clock cycles – klockcykler
CHV	Card holder Verification Information – Information om verifiering av kortinnehavaren
CLA	Class byte of an APDU command – Klass-byte i ett APDU-kommando
DF	Dedicated File – Katalog. En katalog kan innehålla andra filer (EF or DF)
EF	Elementary File – Datafil
ENC	Encrypted – Krypterad: Tillträde endast möjligt genom kodningsdata
etu	elementary time unit – grundläggande tidsenhet
IC	Integrated Circuit – Integrerad krets
ICC	Integrated Circuit Card – IC-kort, kort med integrerade kretsar
ID	Identifier – Identifierare
IFD	Interface Device – Kortläsare
IFS	Information Field Size – Informationsfältstorlek
IFSC	Information Field Size for the card – Fältstorlek för kortet
IFSD	Information Field Size Device – Fältstorleksanordning (för terminalen)
INS	Instruction byte of an APDU command – Instruktions-byte i ett APDU-kommando
Lc	Längd på indata för ett APDU-kommando
Le	Längd på förväntade data (expected data) (utdata för ett kommando)
MF	Master File (root DF) – Huvudfil (rot-katalog)
P1-P2	Parameter bytes – Parameter-byte
NAD	Node Address used in T=1 protocol – Nodadress som används i T=1-protokoll
NEV	Never – Aldrig
PIN	Personal Identification Number – Personligt identifieringsnummer
PRO SM	Protected with secure messaging – Skyddas med säker meddelandehantering (secure messaging)
PTS	Protocol Transmission Selection – Val av protokollöverföring
RFU	Reserved for Future Use – Reserverat för framtida användning

RST	Reset (of the card) – Återställning (av kortet)
SM	Secure Messaging – Säker meddelandehantering
SW1-SW2	Status bytes – Status-byte
TS	Initial ATR character – Initialt ATR-tecken
VPP	Programming Voltage – Programmeringsspänning
XXh	Värde XX med hexadecimal beteckning
||	Concatenation symbol 03||04=0304 – Sammansättningssymbol 03||04=0304

1.2 **Referenser**

Följande referenser används i detta tillägg:

EN 726-3	Transaktionskort – Aktiva kort och terminaler vid telekommunikation – Tillämpningsoberoende kortkrav. December 1994.
ISO/IEC 7816-2	Transaktionskort – Aktivt kort – Kontaktdon. Första utgåvan: 1999.
ISO/IEC 7816-3	Transaktionskort – Aktivt kort – Signaler och protokoll. Utgåva 2: 1997.
ISO/IEC 7816-4	Transaktionskort – Aktivt kort – Gemensamma kommandon för datautbyte. Första utgåvan: 1995 + Ändring 1: 1997.
ISO/IEC 7816-6	Identifikationskort – Aktivt – Gemensamma dataelement. Första utgåvan: 1996 + Cor 1: 1998.
ISO/IEC 7816-8	Information technology – Identification cards – Integrated circuit(s) cards with contacts – Part 8: Security related interindustry commands. Första utgåvan: 1999.
ISO/IEC 9797	Dataskydd – Dataintegritet genom kryptografisk kontrollfunktion med blockchifferalgoritm. Utgåva 2: 1994.

2. ELEKTRISKA OCH FYSISKA EGENSKAPER

TCS_200 Alla elektroniska signaler skall överensstämma med ISO/IEC 7816-3 om inte annat anges.

TCS_201 Kortkontakternas placering och dimensioner skall överensstämma med ISO/IEC 7816-2.

2.1 **Strömspänning och aktuell förbrukning**

TCS_202 Kortet skall fungera enligt specifikationer inom de begränsningar av förbrukningen som anges i ISO/IEC 7816-3.

TCS_203 Kortet skall fungera med V_{cc} = 3 V (+/- 0,3 V) eller med V_{cc} = 5 V (+/- 0,5 V).

Spänningen skall väljas enligt ISO/IEC 7816-3.

2.2 **Programmeringsspänning V_{pp}**

TCS_204 Kortet skall inte kräva programmeringsspänning vid stift C6. Det förväntas att stift C6 inte är anslutet i en IFD. Kontakt C6 får anslutas till V_{cc} på kortet men skall inte anslutas till jord. Denna spänning bör inte tolkas i något fall.

2.3 **Klockgenerering och -frekvens**

TCS_205 Kortet skall fungera inom ett frekvensomfång av 1 till 5 MHz. Inom en kortsession får klockfrekvensen variera med ± 2 %. Klockfrekvensen genereras av fordonsenheten och inte kortet självt. 'Duty cycle' får variera mellan 40 och 60 %.

TCS_206 Den externa klockan kan stoppas på villkor som finns i kortfilen EF_{ICC}. Första byte i EF_{ICC} filmeddelande kodar villkoren för klockstoppläget (se EN 726-3):

Låg	Hög		
Bit 3	Bit 2	Bit 1	
0	0	1	Klockstopp tillåtet, ingen nivå föredras
0	1	1	Klockstopp tillåtet, hög nivå föredras
1	0	1	Klockstopp tillåtet, låg nivå föredras
0	0	0	Klockstopp ej tillåtet
0	1	0	Klockstopp endast tillåtet på hög nivå
1	0	0	Klockstopp endast tillåtet på låg nivå

Bitarna 4 till 8 används inte.

2.4 **I/O-kontakt**

TCS_207 I/O-kontakt C7 används för att ta emot data från och överföra data till IFD. Antingen kortet eller IFD enbart skall vara i överföringsläge vid drift. Kortet skall inte ta skada om båda enheterna är i överföringsläge. När kortet inte överför skall det övergå till mottagningsläge.

2.5 **Kortets tillstånd**

TCS_208 Kortet fungerar i två lägen när matarspänningen används:

— Driftläge när kommandon utförs eller interaktion sker med den digitala enheten.

— Friläge vid alla övriga tillfällen, i detta läge skall 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 driften och kompatibiliteten skall kunna säkerställas.

Färdskrivarkort skall överensstämma så långt som möjligt med tillgängliga tillämpliga normer i ISO/IEC (i synnerhet ISO/IEC 7816). Kommandon och protokoll beskrivs dock fullständigt för att viss begränsad användning eller vissa skillnader skall specificeras om de existerar. Specificerade kommandon överensstämmer till fullo med referensnormerna om inte annat anges.

3.2 **Överföringsprotokoll**

TCS_300 Överföringsprotokollet skall överensstämma med ISO/IEC 7816-3. I synnerhet skall fordonsenheten identifiera de förlängningar av väntetider som kortet sänder.

3.2.1 ***Protokoll***

TCS_301 Kortet skall tillhandahålla både protokoll T=0 och protokoll T=1.

TCS_302 T=0 är default-protokoll, och ett PTS-kommando behövs därför för att ändra protokollet till T=1.

TCS_303 Anordningarna skall stödja direkt kommunikation (direct convention) i båda protokollen. Direkt kommunikation (direct convention) är således obligatorisk för kortet.

TCS_304 Byte för Information Field Size Card skall presenteras vid ATR med TA3-tecken. Detta värde skall vara minst 'F0h' (= 240 byte).

Följande begränsningar

TCS_305 T=0

— Kortläsaren skall stödja ett svar på I/O efter den stigande kanten (rising edge) i signalen på RST från 400 cc.

— Kortläsaren skall kunna läsa tecken som är åtskilda med 12 etu.

— Kortläsaren skall läsa ett felaktigt tecken och upprepning av det 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 skall stödja en försening på 1 etu.

— Kortläsaren skall godta en ATR på 33 byte (TS+32).

— Om TC1 är närvarande i ATR, skall Extra Guard Time (extra vakttid) 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 utsänds av kortläsaren.

— Kortläsaren skall beakta ett NUL-tecken som utsänds av kortet.

— Kortläsaren skall godta komplementläge (complementary mode) för ACK.

— Kommandot GET-RESPONSE (hämta svar) kan inte användas i kedjeläge (chaining mode) för att få data vars längd skulle kunna överstiga 255 byte.

TCS_306 T=1

— NAD byte: ej använt (NAD skall sättas till '00').

— S-block ABORT: ej använt.

— S-block VPP state error: ej använt.

— Den sammanlagda kedjelängden för ett datafält kommer inte att överstiga 255 byte (vilket skall säkerställas av IFD).

— IFSD skall anges av IFD omedelbart efter ATR: IFD skall överföra S-Block IFS-begäran efter ATR och kortet skall sända tillbaka S-Block IFS. Det rekommenderade värdet på IFSD är 254 byte.

— Kortet kommer inte att fråga efter en återjustering av IFS.

3.2.2 ***ATR***

TCS_307 Anordningen kontrollerar ATR-byte, enligt ISO/IEC 7816-3. Ingen verifiering skall 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 skall användas
TD2	'11h'	TA3 närvarande, T=1 skall användas
TA3	'XXh' (at least 'F0h')	Information Field Size Card (IFSC)
TH1 till TH5	'XXh'	Historiska tecken
TCK	'XXh'	Kontrollera tecken (endast OR)

TCS_308 Efter Answer To Reset (ATR), väljs Master File (MF – huvudfilen) indirekt och blir Current Directory (aktuell mapp).

3.2.3 ***PTS***

TCS_309 Default-protokollet är T=0. För att sätta protokollet T=1, måste en PTS (även kallad PPS) sändas till kortet av anordningen.

TCS_310 Eftersom både protokoll T=0 och protokoll T=1 är obligatoriska för kortet är grund-PTS för protokollväxling obligatorisk för kortet.

Som anges i ISO/IEC 7816-3, kan PTS användas för att byta till högre baud-nivåer än den förvalda nivå som föreslås av kortet i ATR i förekommande fall (TA(1) byte).

Högre baud-nivåer är valfria för kortet.

TCS_311 Om ingen annan baud-nivå än den förvalda nivån stöds (eller om den valda baud-nivån inte stöds), skall kortet svara på PTS korrekt 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 är inte närvarande; '00h' för att välja T0, '01h' för att välja T1
PK	'XXh'	Kontrollera tecken: 'XXh' = 'FFh' om PPS0 = '00h' 'XXh' = 'FEh' om PPS0 = '01h'

3.3 **Tillträdesvillkor (AC)**

Tillträdesvillkor (Access conditions – (AC)) för kommandona UPDATE_BINARY (uppdatera binär) och READ_BINARY (läs binär) fastställs för varje datafil.

TCS_312 Tillträdesvillkoren för den aktuella filen måste uppfyllas innan filen kan tillgås via dessa kommandon.

Definitionerna av tillgängliga tillträdesvillkor är följande:

— ALW: Åtgärden är alltid möjlig och kan utföras utan någon begränsning.

— NEV: Åtgärden är aldrig möjlig.

— AUT: Den rätt som motsvarar en lyckad extern autentisering måste öppnas (vilket görs genom kommandot EXTERNAL-AUTHENTICATE (extern autentisera).

— PRO SM: Kommandot måste överföras med en kryptografisk kontrollsumma med hjälp av säker meddelandehantering (se tillägg 11).

— AUT und PRO SM (kombinerat).

När det gäller systemkommandona (UPDATE_BINARY och READ_BINARY), kan följande tillträdesvillkor sättas på kortet:

	UPDATE_BINARY	READ_BINARY
ALW	Ja	Ja
NEV	Ja	Ja
AUT	Ja	Ja
PRO SM	Ja	Nej
AUT och PRO SM	Ja	Nej

Tillträdesvillkoret PRO SM finns inte tillgängligt för kommandot READ_BINARY. Det innebär att närvaron av en kryptografisk kontrollsumma för ett READ-kommando aldrig är obligatorisk. Genom att använda värdet 'OC' för klassen är det dock möjligt att använda kommandot READ_BINARY med säker meddelandehantering (secure messaging), i enlighet med punkt 3.6.2.

3.4 **Datakryptering**

När sekretessen hos data som skall läsas från en fil behöver skyddas är filen markerad 'Encrypted' (krypterad). Kryptering utförs med hjälp av säker meddelandehantering (se tillägg 11).

3.5 **Översikt av kommandon och felkoder**

Kommandon och filorganisering härleds från och överensstämmer med ISO/IEC 7816-4.

TCS_313 Denna del innehåller en beskrivning av följande svarspar på APDU-kommandon:

Kommando	INS
SELECT FILE (välj fil)	A4
READ BINARY (läs binär)	B0
UPDATE BINARY (uppdatera binär)	D6
GET CHALLENGE (hämta utmaning)	84
VERIFY (verifiera)	20
GET RESPONSE (hämta svar)	C0
PERFORM SECURITY OPERATION (utför säkerhetsoperation): VERIFY CERTIFICATE (verifiera certifikat) COMPUTE DIGITAL SIGNATURE (beräkna digital signatur) VERIFY DIGITAL SIGNATURE (verifiera digital signatur) HASH	2A
INTERNAL AUTHENTICATE (intern autentisera)	88
EXTERNAL AUTHENTICATE (extern autentisera)	82
MANAGE SECURITY ENVIRONMENT (förvalta säkerhetsmiljö): SETTING A KEY (sätta en nyckel)	22
PERFORM HASH OF FILE (utför hashning av filen)	2A

TCS_314 Statusregistret SW1 SW2 återsänds i alla svarsmeddelanden och anger bearbetningstillstånd för kommandot.

SW1	SW2	Innebörd
90	00	Normal behandling
61	XX	Normal behandling XX = antal svars-byte som finns tillgängliga
62	81	Varningsbehandling. En del av de återsända data kan vara korrupta
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)
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 datafil)
69	87	Förväntade dataobjekt för säker meddelandehantering saknas
69	88	Inkorrekta dataobjekt för säker meddelandehantering
6A	82	Filen ej funnen
6A	86	Felaktiga parametrar P1-P2
6A	88	Referensdata ej funna
6B	00	Felaktiga parametrar (förskjutning utanför datafilen)

SW1	SW2	Innebörd
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

3.6 **Beskrivning av kommandon**

Detta kapitel innehåller en beskrivning av obligatoriska kommandon för färdskrivarkort.

Närmare relevanta uppgifter i samband med relevant kryptering återfinns i tillägg 11 (Gemensamma säkerhetsmekanismer).

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 associerad längd, associerat värde och associerad beskrivning tomma.

TCS_315 Om båda längd-byte (Lc och Le) begärs måste det kommando som beskrivs delas i två delar om IFD använder protokollet T=0. IFD sänder det kommando som beskrivs med P3=Lc + data och sänder sedan ett GET-RESPONSE-kommando (se punkt 3.6.6) med P3=Le.

TCS_316 Om båda längd-byte begärs och Le=0 (säker meddelandehantering):

— När protokollet T=1 används, skall kortet svara på Le=0 genom att sända alla tillgängliga utgående data.

— När protokollet T=0 används, skall IFD sända det första kommandot med P3=Lc + data, och kortet skall svara (på detta indirekta Le=0) genom status-byte ′61La′, där La är antal tillgängliga svars-byte. IFD skall sedan generera ett GET RESPONSE-kommando med P3 = La för att läsa data.

3.6.1 ***Select File (välj fil)***

Detta kommando överensstämmer med ISO/IEC 7816-4, men det har en begränsad användning jämfört med det kommando som definieras i normen.

Kommandot SELECT FILE används

— för att välja en tillämpningskatalog (val av namn krävs),

— för att välja en datafil som motsvarar det fil-ID som inlämnats.

3.6.1.1 *Selection by name (val med hjälp av namn) (AID)*

Detta kommando gör det möjligt att välja en tillämpningskatalog på kortet.

TCS_317 Detta kommando kan utföras från vilken plats som helst i filstrukturen (efter ATR eller när som helst).

TCS_318 Vid valet av tillämpning återställs befintlig säkerhetsmiljö. Efter det att tillämpning valts, väljs inte längre någon befintlig öppen nyckel och den tidigare sessionsnyckeln finns inte längre tillgänglig för säker meddelandehantering. AUT-tillträdesvillkoret förloras också.

TCS_319 Kommandomeddelande

Byte	Längd	Värde	Beskrivning
CLA	1	′00h′	
INS	1	′A4h′	
P1	1	′04h′	Val av namn (AID – tillämpningsidentifierare)
P2	1	′0Ch′	Inget svar förväntas
Lc	1	′NNh′	Antal byte som sänds till det andra kortet (längd på AID): ′06h′ för färdskrivartillämpningen
#6–#(5+NN)	NN	′XX..XXh′	AID: ′FF 54 41 43 48 4F′ för färdskrivartillämpningen

Inget svar på kommandot SELECT FILE behövs (Le frånvarande i T=1, eller inget svar efterfrågas i T=0).

TCS_320 Svarsmeddelande (inget svar efterfrågas)

Byte	Längd	Värde	Beskrivning
SW	2	'XXXXh'	Statusregister (SW1, SW2)

— Om kommandot lyckas återsänder kortet '9000'.

— Om den tillämpning som passar ihop med AID inte kan hittas, återsänds bearbetningstillstånd (process state) '6A82'.

— I T=1, om byte Le är närvarande, återsänds tillstånd '6700'.

— I T=0, om ett svar efterfrågas efter kommandot SELECT FILE, återsänds tillstånd '6900'.

— Om den valda tillämpningen anses korrupt (integritetsfel upptäcks i filattributen), återsänds bearbetningstillstånd '6400' eller '6581'.

3.6.1.2 *Selection of an Elementary File using its File Identifier (val av datafil med hjälp av dess filidentifierare)*

TCS_321 Kommandomeddelande

Byte	Längd	Värde	Beskrivning
CLA	1	'00h'	
INS	1	'A4h'	
P1	1	'02h'	Val av en datafil under aktuell katalog
P2	1	'0Ch'	Inget svar förväntas
Lc	1	'02h'	Antal byte som sänts till kortet
#6–#7	2	'XXXXh'	Filidentifierare

Inget svar på kommandot SELECT FILE behövs (Le frånvarande i T=1, eller inget svar efterfrågas i T=0).

TCS_322 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 bearbetningstillstånd '6A82'.

— I T=1, om byte Le är närvarande, återsänds tillstånd '6700'.

— I T=0, om ett svar efterfrågas efter kommandot SELECT FILE, återsänds tillstånd '6900'.

— Om den valda filen anses korrupt (integritetsfel upptäcks i filattributen), återsänds bearbetningstillstånd '6400' eller '6581'.

3.6.2 ***Read Binary (läs binär)***

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.

TCS_323 Kommandot kan utföras endast om säkerhetsstatusen överensstämmer med de säkerhetsattribut som definieras för datafilen med avseende på READ-funktionen.

3.6.2.1 *Kommando utan säker meddelandehantering*

Detta kommando gör det möjligt för IFD att läsa data från den datafil som för närvarande är vald, utan säker meddelandehantering.

TCS_324 Det skall inte vara möjligt att läsa data från en fil som är märkt 'Encrypted' (krypterad) genom detta kommando.

TCS_325 Kommandomeddelande

Byte	Längd	Värde	Beskrivning
CLA	1	'00h'	Ingen säker meddelandehantering efterfrågad
INS	1	'B0h'	
P1	1	'XXh'	Förskjutning i byte från början av filen: Mest signifikanta byte
P2	1	'XXh'	Förskjutning i byte från början av filen: Minst signifikanta byte
Le	1	'XXh'	Längd på förväntade data. Antal byte som skall läsas

Obs: bit 8 av P1 måste sättas till 0.

TCS_326 Svarsmeddelande

Byte	Längd	Värde	Beskrivning
#1-#X	X	'XX..XXh'	Läs data
SW	2	'XXXXh'	Statusregister (SW1, SW2)

— Om kommandot lyckas återsänder kortet '9000'.

— Om ingen datafil väljs återsänds bearbetningstillstånd '6986'.

— Om tillträdeskontrollen för den valda filen inte klaras avbryts kommandot med '6982'.

— Om förskjutningen inte överensstämmer med storleken på datafilen (Offset > EF size), återsänds bearbetningstillstånd '6B00'.

— Om storleken på de data som skall läsas inte överensstämmer med storleken på datafilen (Offset + Le > EF size) återsänds bearbetningstillstånd '6700' eller '6Cxx', där 'xx' avser den exakta längden.

— Om ett integritetsfel upptäcks i filattributen, skall kortet anse filen vara skadad och omöjlig att återställa, och bearbetningstillstånd '6400' eller '6581' skall återsändas.

— Om ett integritetsfel upptäcks inom de lagrade data, skall kortet återsända de begärda data, och bearbetningstillstånd '6281' skall återsändas.

3.6.2.2 *Kommando med säker meddelandehantering*

Detta kommando gör det möjligt för IFD att läsa data från den datafil 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 datafilen är märkt 'Encrypted' (krypterad).

TCS_327 Kommandomeddelande

Byte	Längd	Värde	Beskrivning
CLA	1	'0Ch'	Säker meddelandehantering efterfrågad
INS	1	'B0h'	INS
P1	1	'XXh'	P1 (förskjutning i byte från början av filen): Mest signifikanta byte
P2	1	'XXh'	P2 (förskjutning i byte från början av filen): Minst signifikanta byte
Lc	1	'09h'	Längd på ingående data 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 (original Le): Antal byte som skall läsas

Byte	Längd	Värde	Beskrivning
#9	1	'8Eh'	T_{CC}: Tagg för kryptografisk kontrollsumma
#10	1	'04h'	L_{CC}: Längd på efterföljande kryptografiska kontrollsumma
#11-#14	4	'XX..XXh'	Kryptografisk kontrollsumma (4 mest signifikanta byte)
Le	1	'00h'	Enligt ISO/IEC 7816-4

TCS_328 Svarsmeddelande om datafilen inte är märkt 'Encrypted' (krypterad) och det ingående formatet för säker meddelandehantering är korrekt:

Byte	Längd	Värde	Beskrivning
#1	1	'81h'	T_{PV}: Tagg för data med verkliga värden
#2	L	'NNh' or '81 NNh'	L_{PV}: längd på återsända data (=ursprunglig Le) L är 2 byte om LPV>127 byte
#(2+L)-#(1+L+NN)	NN	'XX..XXh'	Verkligt datavärde
#(2+L+NN)	1	'8Eh'	T_{CC}: Tagg för kryptografisk kontrollsumma
#(3+L+NN)	1	'04h'	L_{CC}: Längd på efterföljande kryptografiska kontrollsumma
#(4+L+NN)-#(7+L+NN)	4	'XX..XXh'	Kryptografisk kontrollsumma (4 mest signifikanta byte)
SW	2	'XXXXh'	Statusregister (SW1, SW2)

TCS_329 Svarsmeddelande om datafilen är märkt 'Encrypted' (krypterad) och det ingående formatet för säker meddelandehantering är korrekt:

Byte	Längd	Värde	Beskrivning
#1	1	'87h'	$T_{PI\ CG}$: Tagg för krypterade data (kryptogram)
#2	L	'MMh' or '81 MMh'	$L_{LPI\ CG}$: 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	'8Eh'	T_{CC}: Tagg för kryptografisk kontrollsumma
#(3+L+MM)	1	'04h'	L_{CC}: Längd på efterföljande kryptografiska kontrollsumma
#(4+L+MM)-#(7+L+MM)	4	'XX..XXh'	Kryptografisk kontrollsumma (4 mest signifikanta byte)
SW	2	'XXXXh'	Statusregister (SW1, SW2)

Återsända krypterade data innehåller en första byte som anger använt utfyllnads-läge (padding mode). För färdskrivartillämpningen tar utfyllnadsindikatorn alltid värdet '01h', vilket innebär att det använda utfyllnads-läget är det som specificeras i ISO/IEC 7816-4 (en byte med värdet '80h' följd av några noll-byte: ISO/IEC 9797 metod 2).

De 'sedvanliga' bearbetningstillstånden, som beskrivs för kommandot READ BINARY utan säker meddelandehantering (se punkt 3.6.2.1), kan återsändas med hjälp av de strukturer för svarsmeddelanden som beskrivs ovan.

Vissa fel, som specifikt hänförs till säker meddelandehantering, kan inträffa. I så fall återsänds helt enkelt bearbetningstillståndet utan någon struktur för säker meddelandehantering:

TCS_330 Svarsmeddelande om det ingående formatet för säker meddelandehantering är inkorrekt

Byte	Längd	Värde	Beskrivning
SW	2	'XXXXh'	Statusregister (SW1, SW2)

— Om ingen aktuell sessionsnyckel finns tillgänglig återsänds bearbetningstillstånd '6A88'. Detta inträffar antingen om sessionsnyckeln ännu inte har genererats eller om giltigheten för sessionsnyckeln har utgått (i detta fall måste IFD köra om en ömsesidig autentiseringsprocess för att sätta en ny sessionsnyckel).

— Om några förväntade dataobjekt (enligt specifikation ovan) saknas i formatet för säker meddelandehantering, återsänds bearbetningstillstånd '6987'. Detta fel inträffar om en förväntad tagg saknas eller om kommandomeddelandet inte är korrekt konstruerat.

— Om några dataobjekt är inkorrekta, återsänds bearbetningstillstånd '6988'. Detta fel inträffar om alla begärda taggar finns närvarande men vissa längder skiljer sig från dem som förväntas.

— Om verifieringen av den kryptografiska kontrollsumman misslyckas, återsänds bearbetningstillstånd '6688'.

3.6.3 ***Update Binary (uppdatera binär)***

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 (ta bort + skriv)) av de bitar som redan finns närvarande i en binär datafil med bitar givna i kommando-APDU.

TCS_331 Kommandot kan utföras endast om säkerhetsstatusen överensstämmer med de säkerhetsegenskaper som fastställts för datafilen när det gäller UPDATE-funktionen. (Om tillträdeskontrollen av UPDATE-funktionen inbegriper PRO SM, måste säker meddelandehantering läggas till i kommandot).

3.6.3.1 *Kommando utan säker meddelandehantering*

Detta kommando gör det möjligt för IFD att skriva data i den datafil som för närvarande är vald, utan att kortet verifierar integriteten hos de data som tas emot. Detta 'klarläge' (plain mode) tillåts endast om den berörda filen inte är märkt 'Encrypted' (krypterad).

TCS_332 Kommandomeddelande

Byte	Längd	Värde	Beskrivning
CLA	1	'00h'	Ingen säker meddelandehantering efterfrågas
INS	1	'D6h'	
P1	1	'XXh'	Förskjutning i byte från början av filen: Mest signifikanta byte
P2	1	'XXh'	Förskjutning i byte från början av filen: Minst signifikanta byte
Lc	1	'NNh'	Lc Längd på data som skall uppdateras. Antal byte som skall skrivas
#6-#(5+NN)	NN	'XX..XXh'	Data som skall skrivas

Obs: bit 8 av P1 måste sättas till 0.

TCS_333 Svarsmeddelande

Byte	Längd	Värde	Beskrivning
SW	2	'XXXXh'	Statusregister (SW1, SW2)

— Om kommandot lyckas återsänder kortet '9000'.

— Om ingen datafil väljs återsänds bearbetningstillstånd '6986'.

— Om tillträdeskontrollen för den valda filen inte klaras avbryts kommandot med '6982'.

— Om förskjutningen inte överensstämmer med storleken på datafilen (Offset > EF size), återsänds bearbetningstillstånd '6B00'.

— Om storleken på de data som skall skrivas inte överensstämmer med storleken på datafilen (Offset + Le > EF size) återsänds bearbetningstillstånd '6700'.

— Om ett integritetsfel upptäcks i filattributen, skall kortet anse filen vara skadad och omöjlig att återställa, och bearbetningstillstånd '6400' eller '6500' skall återsändas.

— Om det inte går att skriva data, återsänds bearbetningstillstånd '6581'.

3.6.3.2 *Kommando med säker meddelandehantering*

Detta kommando gör det möjligt för IFD att skriva data i den datafil som för närvarande är vald, varigenom kortet verifierar integriteten hos mottagna data. Eftersom ingen sekretess krävs skall dessa data inte krypteras.

TCS_334 Kommandomeddelande

Byte	Längd	Värde	Beskrivning
CLA	1	'0Ch'	Säker meddelandehantering efterfrågas
INS	1	'D6h'	INS
P1	1	'XXh'	Förskjutning i byte från början av filen: Mest signifikanta byte
P2	1	'XXh'	Förskjutning i byte från början av filen: Minst signifikanta byte
Lc	1	'XXh'	Längd på säkerhetsfält
#6	1	'81h'	T_{PV}: Tagg för data med verkliga värden
#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'	Verkligt datavärde (data som skall skrivas)
#(7+L+NN)	1	'8Eh'	T_{CC}: Tagg för kryptografisk kontrollsumma
#(8+L+NN)	1	'04h'	L_{CC}: Längd på efterföljande kryptografiska kontrollsumma
#(9+L+NN)-#(12+L+NN)	4	'XX..XXh'	Kryptografisk kontrollsumma (4 mest signifikanta byte)
Le	1	'00h'	Enligt ISO/IEC 7816-4

TCS_335 Svarsmeddelande om det ingående formatet för säker meddelandehantering är korrekt

Byte	Längd	Värde	Beskrivning
#1	1	'99h'	T_{SW}: Tagg för statusregister (skall skyddas av CC)
#2	1	'02h'	L_{SW}: Längd på återsända statusregister
#3-#4	2	'XXXXh'	Statusregister (SW1, SW2)
#5	1	'8Eh'	T_{CC}: Tagg för kryptografisk kontrollsumma
#6	1	'04h'	L_{CC}: Längd på efterföljande kryptografiska kontrollsumma
#7-#10	4	'XX..XXh'	Kryptografisk kontrollsumma (4 mest signifikanta byte)
SW	2	'XXXXh'	Statusregister (SW1, SW2)

De 'sedvanliga' bearbetningstillstånden, som beskrivs för kommandot UPDATE BINARY utan säker meddelandehantering (se punkt 3.6.3.1), kan återsändas med hjälp av den struktur för svarsmeddelanden som beskrivs ovan.

Några fel, som specifikt kan hänföras till säker meddelandehantering, kan inträffa. I så fall återsänds helt enkelt bearbetningstillståndet utan någon struktur för säker meddelandehantering:

TCS_336 Svarsmeddelande vid fel i den säkra meddelandehanteringen

Byte	Längd	Värde	Beskrivning
SW	2	'XXXXh'	Statusregister (SW1, SW2)

— Om ingen aktuell sessionsnyckel finns tillgänglig återsänds bearbetningstillstånd '6A88'.

— Om några förväntade dataobjekt (enligt specifikation ovan) saknas i formatet för säker meddelandehantering, återsänds bearbetningstillstånd '6987'. Detta fel inträffar om en förväntad tagg saknas eller om kommandomeddelandet inte är rätt konstruerat.

— Om några dataobjekt är inkorrekta, återsänds bearbetningstillstånd '6988'. Detta fel inträffar om alla nödvändiga taggar finns närvarande men vissa längder skiljer sig från dem som förväntas.

— Om verifieringen av den kryptografiska kontrollsumman misslyckas, återsänds bearbetningstillstånd '6688'.

3.6.4 ***Get Challenge (hämta utmaning)***

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 för att använda den i ett säkerhetsförfarande i vilket ett kryptogram eller några chiffrerade data sänds till kortet.

TCS_337 Den utmaning som utfärdas av kortet är endast giltig för nästa kommando som använder en utmaning som sänds till kortet.

TCS_338 Kommandomeddelande

Byte	Längd	Värde	Beskrivning
CLA	1	'00h'	CLA
INS	1	'84h'	INS
P1	1	'00h'	P1
P2	1	'00h'	P2
Le	1	'08h'	Le (Längd på den utmaning som förväntas)

TCS_339 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 bearbetningstillståndet '6700'.

— Om parametrarna P1-P2 är inkorrekta är bearbetningstillståndet '6A86'.

3.6.5 ***Verify (verifiera)***

Detta kommando överensstämmer med ISO/IEC 7816-4, men det har en begränsad användning jämfört med det kommando som definieras i normen.

Kommandot Verify initierar jämförelsen på kortet av CHV (PIN)-data som sänds från kommandot med referensen CHV lagrad på kortet.

Obs: Den PIN-kod som anges av användaren måste vara utfylld till höger av IFD med 'FFh'-byte upp till en längd av 8 byte.

TCS_340 Om kommandot lyckas öppnas rättigheterna som motsvarar CHV-presentationen och räknaren av återstående CHV-försök initieras igen.

TCS_341 En misslyckad jämförelse registreras på kortet för att begränsa antalet ytterligare försök att använda referens-CHV.

TCS_342 Kommandomeddelande

Byte	Längd	Värde	Beskrivning
CLA	1	'00h'	CLA
INS	1	'20h'	INS
P1	1	'00h'	P1
P2	1	'00h'	P2 (den verifierade CHV är indirekt känd)
Lc	1	'08h'	Längd på CHV-koden överförd
#6-#13	8	'XX..XXh'	CHV

TCS_343 Svarsmeddelande

Byte	Längd	Värde	Beskrivning
SW	2	'XXXXh'	Statusregister (SW1, SW2)

— Om kommandot lyckas återsänder kortet '9000'.

— Om referens-CHV inte hittas, återsänds bearbetningstillstånd '6A88'.

— Om CHV blockeras (räknaren av återstående CHV-försök står på noll) är det processtilllstånd som återsänds '6983'. När CHV väl är i detta tillstånd kan den aldrig presenteras med gott resultat igen.

— Om jämförelsen misslyckas minskas värdet på räknaren för återstående försök och status '63CX' återsänds (X > 0 och X = räknare av återstående CHV-försök. Om X = 'F', är värdet på räknaren av CHV-försök större än 'F').

— Om referens-CHV anses korrupt, återsänds bearbetningstillstånd '6400' eller '6581'.

3.6.6 ***Get Response (hämta svar)***

Detta kommando överensstämmer med ISO/IEC 7816-4.

Detta kommando (som bara behövs och finns för T=0-protokoll) används för att överföra förberedda data från kortet till kortläsaren (fall där ett kommando inbegriper både Lc och Le).

Kommandot GET-RESPONSE måste utfärdas 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_344 Kommandomeddelande

Byte	Längd	Värde	Beskrivning
CLA	1	'00h'	
INS	1	'C0h'	
P1	1	'00h'	
P2	1	'00h'	
Le	1	'XXh'	Antal förväntade byte

TCS_345 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 bearbetningstillstånd '6900' eller '6F00'.

— Om Le överstiger antal tillgängliga byte eller om Le är noll återsänds bearbetningstillstånd '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 bearbetningstillstånd '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'.

3.6.7 ***PSO: Verify Certificate (verifiera certifikat)***

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 validitet.

TCS_346 När ett VERIFY CERTIFICATE-kommando lyckas lagras den öppna nyckeln i säkerhetsmiljön för framtida användning. Denna nyckel skall indirekt sättas för användning i säkerhetsrelaterade kommandon (INTERNAL AUTHENTICATE, EXTERNAL AUTHENTICATE eller VERIFY CERTIFICATE) av MSE-kommandot (se punkt 3.6.10) med hjälp av dess nyckelidentifierare.

TCS_347 I alla händelser använder kommandot VERIFY CERTIFICATE den öppna nyckel som MSE-kommandot tidigare valt för att öppna certifikatet. Denna öppna nyckel skall tillhöra antingen en medlemsstat eller Europa.

TCS_348 Kommandomeddelande

Byte	Längd	Värde	Beskrivning
CLA	1	'00h'	CLA
INS	1	'2Ah'	Utför Security Operation (säkerhetsoperation)
P1	1	'00h'	P1
P2	1	'AEh'	P2: icke BER-TLV-kodade data (sammansättning av dataelement)
Lc	1	'CEh'	Lc: Certifikatets längd, 194 byte
#6-#199	194	'XX..XXh'	Certifikat: Sammansättning av dataelement (enligt tillägg 11)

TCS_349 Svarsmeddelande

Byte	Längd	Värde	Beskrivning
SW	2	'XXXXh'	Statusregister (SW1, SW2)

— Om kommandot lyckas återsänder kortet '9000'.

— Om verifieringen av certifikat misslyckas, återsänds bearbetningstillstånd '6688'. Verifiering och uppackning av certifikat beskrivs i tillägg 11.

— 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 korrupt återsänds bearbetningstillstånd '6400' eller '6581'.

— 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 bearbetningstillstånd '6985'.

3.6.8 ***Internal Authenticate (intern autentisera)***

Detta kommando överensstämmer med ISO/IEC 7816-4.

Med hjälp av kommandot INTERNAL AUTHENTICATE kan IFD autentisera kortet.

Autentiseringen beskrivs i tillägg 11. Den inbegriper följande programsatser:

TCS_350 Kommandot INTERNAL AUTHENTICATE använder den hemliga kortnyckeln (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_351 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_352 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 Security Environment (säkerhetsmiljön) återsänds bearbetningstillstånd '6A88'.

— Om ingen hemlig nyckel är närvarande i Security Environment (säkerhetsmiljön) återsänds bearbetningstillstånd '6A88'.

— Om VU.CHR inte överensstämmer med aktuell identifierare av öppen nyckel återsänds bearbetningstillstånd '6A88'.

— Om den valda öppna nyckeln anses korrupt, återsänds bearbetningstillstånd '6400' eller '6581'.

TCS_353 Om kommandot INTERNAL-AUTHENTICATE lyckas tas aktuell sessionsnyckel i förekommande fall bort och den upphör att vara tillgänglig. För att göra en ny sessionsnyckel tillgänglig måste kommandot EXTERNAL-AUTHENTICATE (extern autentisera) utföras med gott resultat.

3.6.9 ***External Authenticate (extern autentisera)***

Detta kommando överensstämmer med ISO/IEC 7816-4.

Med hjälp av kommandot EXTERNAL AUTHENTICATE kan kortet autentisera IFD.

Autentiseringen beskrivs i tillägg 11. Det inbegriper följande programsatser:

TCS_354 Kommandot GET CHALLENGE (hämta utmaning) måste omedelbart föregå kommandot EXTERNAL-AUTHENTICATE. Kortet utfärdar en utmaning till utsidan (RND3).

TCS_355 Vid verifieringen av kryptogrammet används RND3 (utmaning utfärdad av kortet), privat kortnyckel (indirekt vald) och den öppna nyckel som tidigare valts av MSE-kommandot.

TCS_356 Kortet verifierar kryptogrammet och om det är korrekt öppnas AUT-tillträdesvillkor.

TCS_357 Det ingående kryptogrammet överför det andra elementet för K2-överenskommelse om sessionsnycklar.

TCS_358 Kommandomeddelande

Byte	Längd	Värde	Beskrivning
CLA	1	'00h'	CLA
INS	1	'82h'	INS
P1	1	'00h'	P1
P2	1	'00h'	P2 (den öppna nyckel som skall användas är indirekt känd och har satts tidigare av MSE-kommandot)
Lc	1	'80h'	Lc (längd på de data som sänds till kortet)
#6-#133	128	'XX..XXh'	Kryptogram (se tillägg 11)

TCS_359 Svarsmeddelande

Byte	Längd	Värde	Beskrivning
SW	2	'XXXXh'	Statusregister (SW1, SW2)

— Om kommandot lyckas återsänder kortet '9000'.

— Om ingen öppen nyckel är närvarande i Security Environment (säkerhetsmiljön) återsänds '6A88'.

— Om CHA för den för närvarande satta öppna nyckeln inte är en sammansättning av färdskrivartillämpningens AID (tillämpningsidentifierare) och av en typ av fordonsenhetsutrustning, återsänds bearbetningstillstånd '6F00' (se tillägg 11).

— Om ingen privat nyckel är närvarande i Security Environment (säkerhetsmiljön) återsänds bearbetningstillstånd '6A88'.

— Om verifieringen av kryptogrammet misslyckas, återsänds bearbetningstillstånd '6688'.

— Om kommandot inte omedelbart föregås av kommandot GET CHALLENGE återsänds bearbetningstillstånd '6985'.

— Om den valda öppna nyckeln anses korrupt, återsänds bearbetningstillstånd '6400' eller '6581'.

TCS_360 Om kommandot EXTERNAL AUTHENTICATE lyckas, och om första delen av sessionsnyckeln är tillgänglig från en lyckad INTERNAL AUTHENTICATE som utförts nyligen, sätts sessionsnyckeln för framtida kommandon med hjälp av säker meddelandehantering.

TCS_361 Om den första sessionsnyckeldelen inte är tillgänglig från ett tidigare INTERNAL AUTHENTICATE-kommando, lagras den andra delen av sessionsnyckeln, som sänds av IFD, inte på kortet. Denna mekanism säkerställer att den ömsesidiga autentiseringen görs i den ordning som anges i tillägg 11.

3.6.10 ***Manage Security Environment (förvalta säkerhetsmiljö)***

Detta kommando används för att sätta en öppen nyckel i autentiseringssyfte.

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

TCS_362 Den nyckel som det refereras till i MSE-fältet är giltig för varje fil i färdskrivarkatalogen.

TCS_363 Den nyckel som det refereras till i MSE-fältet förblir befintlig öppen nyckel till nästa korrekta MSE-kommando.

TCS_364 Om den nyckel som det refereras till inte (redan) är närvarande i kortet, förblir säkerhetsmiljön oförändrad.

TCS_365 Kommandomeddelande

Byte	Längd	Värde	Beskrivning
CLA	1	'00h'	CLA
INS	1	'22h'	INS
P1	1	'C1h'	P1: Refererad nyckel som är giltig för all kryptografisk verksamhet
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 nyckel-referensen (nyckelidentifierare)
#8-#15	08h	'XX..XXh'	Nyckelidentifierare enligt tillägg 11

TCS_366 Svarsmeddelande

Byte	Längd	Värde	Beskrivning
SW	2	'XXXXh'	Statusregister (SW1, SW2)

— Om kommandot lyckas återsänder kortet '9000'.

— Om referensnyckeln inte är närvarande på kortet återsänds bearbetningstillstånd '6A88'.

— Om några förväntade dataobjekt saknas i formatet för säker meddelandehantering, återsänds bearbetningstillstånd '6987'. Detta kan inträffa om taggen '83h' saknas.

— Om några dataobjekt är inkorrekta, återsänds bearbetningstillstånd '6988'. Detta kan inträffa om längden på nyckelidentifieraren inte är '08h'.

— Om den valda nyckeln anses korrupt, återsänds bearbetningstillstånd '6400' eller '6581'.

3.6.11 ***PSO: Hash***

Detta kommando används för att till kortet överföra resultatet från en hash-beräkning på vissa data. Detta kommando används för att verifiera digitala signaturer. Hash-värdet lagras i EEPROM för det efterföljande kommandot verifiera digital signatur.

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

TCS_367 Kommandomeddelande

Byte	Längd	Värde	Beskrivning
CLA	1	'00h'	CLA
INS	1	'2Ah'	Utför Security Operation (säkerhetsoperation)
P1	1	'90h'	Återsänd hash-kod
P2	1	'A0h'	Tagg: Datafältet innehåller dataobjekt som är relevanta vid hashing
Lc	1	'16h'	Längd Lc på efterföljande datafält
#6	1	'90h'	Tagg för hash-koden
#7	1	'14h'	Längd på hash-koden
#8-#27	20	'XX..XXh'	Hash-kod

TCS_368 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 bearbetningstillstånd '6987'. Detta kan inträffa om en av taggarna '90h' saknas.

— Om några dataobjekt är inkorrekta, återsänds bearbetningstillstånd '6988'. Detta fel inträffar om den nödvändiga taggen är närvarande, men med en längd som skiljer sig från '14h'.

3.6.12 ***Perform Hash of File (utför hashning av fil)***

Detta kommando överensstämmer inte med ISO/IEC 7816-8. CLA-byte i detta kommando anger sålunda att det finns en proprietär användning av PERFORM SECURITY OPERATION/HASH.

TCS_369 Kommandot perform hash of file används för att hasha dataarean hos den för närvarande valda transparenta datafilen.

TCS_370 Resultatet från hashningen lagras på kortet. Det kan därefter användas för att få en digital signatur av filen, med hjälp av kommandot PSO-COMPUTE_DIGITAL_SIGNATURE. Detta resultat förblir tillgängligt för kommandot COMPUTE DIGITAL SIGNATURE tills nästa PERFORM HASH of FILE-kommando lyckas.

TCS_371 Kommandomeddelande

Byte	Längd	Värde	Beskrivning
CLA	1	'80h'	CLA
INS	1	'2Ah'	Utför Security Operation (säkerhetsoperation)
P1	1	'90h'	Tagg: Hash
P2	1	'00h'	P2: Hasha data från den för närvarande valda transparenta filen

TCS_372 Svarsmeddelande

Byte	Längd	Värde	Beskrivning
SW	2	'XXXXh'	Statusregister (SW1, SW2)

— Om kommandot lyckas återsänder kortet '9000'.

— Om ingen tillämpning väljs återsänds bearbetningstillstånd '6985'.

— Om den valda datafilen anses korrupt (integritetsfel i filattributen eller de lagrade data), återsänds bearbetningstillstånd '6400' eller '6581'.

— Om den valda filen inte är en transparent fil, återsänds bearbetningstillstånd '6986'.

3.6.13 ***PSO: Compute Digital Signature (beräkna digital signatur)***

Detta kommando används för att beräkna digital signatur hos tidigare beräknad hash-kod (se PERFORM HASH of FILE, punkt 3.6.12).

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

TCS_373 Den privata kortnyckeln används för att beräkna den digitala signaturen och är indirekt känd av kortet.

TCS_374 Kortet utför en digital signatur med hjälp av en utfyllnadsmetod som överensstämmer med PKCS1 (se tillägg 11).

TCS_375 Kommandomeddelande

Byte	Längd	Värde	Beskrivning
CLA	1	'00h'	CLA
INS	1	'2Ah'	Utför Security Operation (säkerhetsoperation)
P1	1	'9Eh'	Digital signatur som återsänds
P2	1	'9Ah'	Tagg: Datafältet innehåller data som skall signeras. Eftersom inget datafält inbegrips är det meningen att data redan skall finnas på kortet (filens hash)
Le	1	'80h'	Längd på förväntad signatur

TCS_376 Svarsmeddelande

Byte	Längd	Värde	Beskrivning
#1-#128	128	'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 korrupt, återsänds bearbetningstillstånd '6400' eller '6581'.

3.6.14 ***PSO: Verify Digital Signature (verifiera digital signatur)***

Detta kommando används för att verifiera den digitala signaturen, som tillhandahålls som indata, i överensstämmelse med PKCS1 i ett meddelande 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.

TCS_377 Kommandot Verify Digital Signatur (verifiera digital signatur) använder alltid den öppna nyckel som valts av tidigare Manage Security Environment-kommando, och den tidigare hash-kod som angivits genom ett PSO: Hash-kommando.

TCS_378 Kommandomeddelande

Byte	Längd	Värde	Beskrivning
CLA	1	'00h'	CLA
INS	1	'2Ah'	Utför Security Operation (säkerhetsoperation)
P1	1	'00h'	
P2	1	'A8h'	Tagg: Datafältet innehåller dataobjekt som är relevanta vid verifiering
Lc	1	'83h'	Längd Lc på efterföljande datafält
#28	1	'9Eh'	Tagg för digital signatur
#29-#30	2	'8180h'	Längd på den digitala signaturen (128 byte, kodade i överensstämmelse med ISO/IEC 7816-6)
#31-#158	128	'XX..XXh'	Innehåll i digital signatur

TCS_379 Svarsmeddelande

Byte	Längd	Värde	Beskrivning
SW	2	'XXXXh'	Statusregister (SW1, SW2)

— Om kommandot lyckas återsänder kortet '9000'.

— Om verifieringen av signaturen misslyckas, återsänds bearbetningstillstånd '6688'. Verifieringen beskrivs i tillägg 11.

— Om ingen öppen nyckel har valts återsänds bearbetningstillstånd '6A88'.

— Om några förväntade dataobjekt (enligt specifikation ovan) saknas återsänds bearbetningstillstånd '6987': Detta kan inträffa om en av de nödvändiga taggarna saknas.

— Om ingen hash-kod finns tillgänglig för att behandla kommandot (på grund av tidigare PSO: hash-kommando) återsänds bearbetningstillstånd '6985'.

— Om vissa dataobjekt är inkorrekta, återsänds bearbetningstillstånd '6988'. Detta kan inträffa om en av de begärda dataobjektlängderna är inkorrekt.

— Om den valda öppna nyckeln anses korrupt, återsänds bearbetningstillstånd '6400' eller '6581'.

4. FÄRDSKRIVARKORTENS STRUKTUR

I denna punkt specificeras filstrukturerna i färdskrivarkort för lagring av tillgängliga data. (Se definitioner av datatyper i tillägg 1).

Här specificeras varken interna strukturer som är beroende av korttillverkare, exempelvis etikett för filbörjan, eller lagring och hantering av dataelement som endast behövs för intern användning, exempelvis `EuropeanPublicKey`, `CardPrivateKey`, `TDesSessionKey` eller `WorkshopCardPin`.

Den användbara lagringskapaciteten på färdskrivarkort skall sättas till minst 11 Kbyte. Större kapacitet får användas. I så fall skall kortets struktur vara den samma, men antal poster för vissa element i strukturen ökas. I denna punkt specificeras minsta och största värden på dessa postnummer.

4.1 **Förarkortets struktur**

TCS_400 Efter det att kortet har användaranpassats skall det ha följande permanenta filstruktur och filtillträdesvillkor:

Fil	Fil-ID	Tillträdesvillkor		
		Läs (Read)	Uppdatering	Krypterad
MF	3F00			
├─EF ICC	0002	ALW	NEV	No
├─EF IC	0005	ALW	NEV	No
└─DF Tachograph	0500			
├─EF Application_Identification	0501	ALW	NEV	No
├─EF Card_Certificate	C100	ALW	NEV	No
├─EF CA_Certificate	C108	ALW	NEV	No
├─EF Identification	0520	ALW	NEV	No
├─EF Card_Download	050E	ALW	ALW	No
├─EF Driving_Licence_Info	0521	ALW	NEV	No
├─EF Events_Data	0502	ALW	PRO SM / AUT	No
├─EF Faults_Data	0503	ALW	PRO SM / AUT	No
├─EF Driver_Activity_Data	0504	ALW	PRO SM / AUT	No
├─EF Vehicles_Used	0505	ALW	PRO SM / AUT	No
├─EF Places	0506	ALW	PRO SM / AUT	No
├─EF Current_Usage	0507	ALW	PRO SM / AUT	No
├─EF Control_Activity_Data	0508	ALW	PRO SM / AUT	No
└─EF Specific_Conditions	0522	ALW	PRO SM / AUT	No

TCS_401 Alla datafilstrukturer skall vara transparenta.

TCS_402 Läs (Read) med säker meddelandehantering skall vara möjlig för alla filer under katalogen färdskrivare (DF Tachograph).

TCS_403 Förarkortet skall ha följande datastruktur:

Fil/dataelement	Antal poster	Storlek (byte)		Förvalda värden
		Min	Max	
MF		*11411*	*24959*	
╠═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}
╚═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				
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}

TCS_404 Nedanstående värden, som används för att tillhandahålla storlekar i tabellen ovan, är de minsta och största postnummervärden som förarkortets datastruktur måste använda.

		Min	Max
n_1	NoOfEventsPerType	6	12
n_2	NoOfFaultsPerType	12	24
n_3	NoOfCardVehicleRecords	84	200
n_4	NoOfCardPlaceRecords	84	112
n_6	CardActivityLengthRange	5 544 bytes (28 dagar * 93 aktivitetsändringar)	13 776 byte (28 dagar * 240 aktivitetsändringar)

4.2 **Verkstadskortets struktur**

TCS_405 Efter det att verkstadskortet har användaranpassats skall det ha följande permanenta filstruktur och filtillträdesvillkor:

		Tillträdesvillkor		
Fil	Fil-ID	Läs (Read)	Uppdatering	Krypterad
MF	3F00			
├─EF ICC	0002	ALW	NEV	No
├─EF IC	0005	ALW	NEV	No
└─DF Tachograph	0500			
├─EF Application_Identification	0501	ALW	NEV	No
├─EF Card_Certificate	C100	ALW	NEV	No
├─EF CA_Certificate	C108	ALW	NEV	No
├─EF Identification	0520	ALW	NEV	No
├─EF Card_Download	0509	ALW	ALW	No
├─EF Calibration	050A	ALW	PRO SM / AUT	No
├─EF Sensor_Installation_Data	050B	ALW	NEV	Yes
├─EF Events_Data	0502	ALW	PRO SM / AUT	No
├─EF Faults_Data	0503	ALW	PRO SM / AUT	No
├─EF Driver_Activity_Data	0504	ALW	PRO SM / AUT	No
├─EF Vehicles_Used	0505	ALW	PRO SM / AUT	No
├─EF Places	0506	ALW	PRO SM / AUT	No
├─EF Current_Usage	0507	ALW	PRO SM / AUT	No
├─EF Control_Activity_Data	0508	ALW	PRO SM / AUT	No
└─EF Specific_Conditions	0522	ALW	PRO SM / AUT	No

TCS_406 Alla datafilstrukturer skall vara transparenta.

TCS_407 Läs (Read) med säker meddelandehantering skall vara möjlig för alla filer under katalogen färdskrivare (DF Tachograph).

TCS_408 Verkstadskortet skall ha följande datastruktur:

Fil/dataelement	Antal poster	Storlek (byte) Min	Storlek (byte) Max	Förvalda värden
MF	*11088*	*29061*		
╠═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}	
╚═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}
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}
═EF Control_Activity_Data		*46*	*46*	
└─CardControlActivityDataRecord		*46*	*46*	
├─controlType		1	1	{00}
├─controlTime		4	4	{00..00}
├─controlCardNumber				
│ ├─cardType		1	1	{00}
│ ├─cardIssuingMemberState		1	1	{00}
│ └─cardNumber		16	16	{20..20}
├─controlVehicleRegistration				
│ ├─vehicleRegistrationNation		1	1	{00}
│ └─vehicleRegistrationNumber		14	14	{00, 20..20}
├─controlDownloadPeriodBegin		4	4	{00..00}
└─controlDownloadPeriodEnd		4	4	{00..00}
═EF Specific_Conditions		*10*	*10*	
└─SpecificConditionRecord	2	*5*	*5*	
├─entryTime		4	4	{00..00}
└─SpecificConditionType		1	1	{00}

TCS_409 Nedanstående värden, som används för att tillhandahålla storlekar i tabellen ovan, är de minsta och största postnummervärden som verkstadskortets datastruktur måste använda.

		Min	Max
n_1	NoOfEventsPerType	3	3
n_2	NoOfFaultsPerType	6	6
n_3	NoOfCardVehicleRecords	4	8
n_4	NoOfCardPlaceRecords	6	8
n_6	CardActivityLengthRange	88	255
n_5	NoOfCalibrationRecords	198 byte (1 dag * 93 aktivitetsändringar)	492 byte (1 dag * 240 aktivitetsändringar)

4.3 **Kontrollkortets struktur**

TCS_410 Efter det att kontrollkortet har användaranpassats skall det ha följande permanenta filstruktur och filtillträdesvillkor:

		Tillträdesvillkor		
Fil	Fil-ID	Läs (Read)	Uppdatering	Krypterad
MF	3F00			
├─EF ICC	0002	ALW	NEV	No
├─EF IC	0005	ALW	NEV	No
└─DF Tachograph	0500			
├─EF Application_Identification	0501	ALW	NEV	No
├─EF Card_Certificate	C100	ALW	NEV	No
├─EF CA_Certificate	C108	ALW	NEV	No
├─EF Identification	0520	AUT	NEV	No
└─EF Controller_Activity_Data	050C	ALW	PRO SM / AUT	No

TCS_411 Alla datafilstrukturer skall vara transparenta.

TCS_412 Läs (Read) med säker meddelandehantering skall vara möjlig för filer under katalogen färdskrivare (DF Tachograph).

TCS_413 Kontrollkortet skall ha följande datastruktur:

Fil/dataelement	Antal poster	Storlek (byte) Min	Storlek (byte) Max	Förvalda värden
MF		*11219*	*24559*	
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}
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_414 Nedanstående värden, som används för att tillhandahålla storlekar i tabellen ovan, är de minsta och största postnummervärden som kontrollkortets datastruktur måste använda.

		Min.	Max.
n_7	NoOfControlActivityRecords	230	520

4.4 **Företagskortets struktur**

TCS_415 Efter det att företagskortet har användaranpassats skall det ha följande permanenta filstruktur och filtillträdesvillkor:

Fil	Fil-ID	Tillträdesvillkor		
		Läs (Read)	Uppdatering	Krypterad
MF	3F00			
├─EF ICC	0002	ALW	NEV	No
├─EF IC	0005	ALW	NEV	No
└─DF Tachograph	0500			
├─EF Application_Identification	0501	ALW	NEV	No
├─EF Card_Certificate	C100	ALW	NEV	No
├─EF CA_Certificate	C108	ALW	NEV	No
├─EF Identification	0520	AUT	NEV	No
└─EF Company_Activity_Data	050D	ALW	PRO SM / AUT	No

TCS_416 Alla datafilstrukturer skall vara transparenta.

TCS_417 Läs (Read) med säker meddelandehantering skall vara möjlig för alla filer under katalogen färdskrivare.

TCS_418 Företagskortet skall ha följande datastruktur:

Fil/dataelement	Antal poster	Storlek (byte) Min	Storlek (byte) Max	Förvalda värden
MF		*11147*	*24487*	
╠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}
╚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}

├─cardNumberInformation			
│ ├─cardType	1	1	{00}
│ ├─cardIssuingMemberState	1	1	{00}
│ └─cardNumber	16	16	{20..20}
├─downloadPeriodBegin	4	4	{00..00}
└─downloadPeriodEnd	4	4	{00..00}

TCS_419 Nedanstående värden, som används för att tillhandahålla storlekar i tabellen ovan, är de minsta och största postnummervärden som företagskortets datastruktur måste använda.

		Min.	Max.
n_8	NoOfCompanyActivityRecords	230	520

Tillägg 3

PIKTOGRAM

PIC_001Färdskrivaren får använda sig av följande piktogram och kombinationer av piktogram:

1. GRUNDLÄGGANDE PIKTOGRAM

	Personer	**Åtgärder**	**Driftlägen**
	Företag		Företagsläge
	Kontrollant	Kontroll	Kontrolläge
	Förare	Körning	Driftläge
	Verkstad/provningsstation	Besiktning/kalibrering	Kalibreringsläge
	Tillverkare		

	Aktiviteter	**Varaktighet**
	Tillgänglighet	Innevarande tillgänglighetsperiod
	Körning	Sammanhängande körtid
	Vila	Innevarande viloperiod
	Arbete	Innevarande arbetsperiod
	Rast	Sammanlagd avbrottstid
?	Okänd	

	Utrustning	**Funktioner**
1	Förarens kortplats	
2	Medförarens kortplats	
	Kort	
	Klocka	
	Display	Visning
	Extern lagring	Överföring
	Strömtillförsel	
	Skrivare/utskrift	Utskrift
	Sensor	
	Däcksdimension	
	Fordon/fordonsenhet	

	Särskilda omständigheter
OUT	Omfattas ej
	Transport med färja/tåg

	Övrigt		
!	Händelser	×	Fel
	Påbörjande av dagens arbetspass		Avslutande av dagens arbetspass
	Plats	M	Manuell angivelse av föraraktiviteter
	Säkerhet		Hastighet
	Tid	Σ	Totalt/sammanfattning

	Precisering
24h	Dagligen
|	Varje vecka
||	Två veckor
	Från eller till

2. Kombinationer av piktogram

	Övrigt		
	Kontrollplats		
	Plats där dagens arbetspass påbörjas		Plats där dagens arbetspass avslutas
	Från tidpunkt		Till tidpunkt
	Från fordon		
OUT	Perioden ’omfattas ej’ börjar	OUT	Perioden ’omfattas ej’ slutar

Kort

Förarkort
Företagskort
Kontrollkort
Provningskort
Inget kort

Körning

Körning med flera förare (crew)
Körningstid under en vecka
Körningstid under två veckor

Utskrifter

Daglig utskrift från kort av föraraktiviteter
Daglig utskrift 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

Isättning av ogiltigt kort
Kortkonflikt
Överlappning av tider
Körning utan korrekt kort
Isättning av kort under körning
Senaste kortanvändning ej korrekt avslutad
Hastighetsöverträdelse
Avbrott av strömtillförseln
Fel i rörelsedata
Säkerhetsöverträdelse
Tidsinställning (av verkstad)
Kontroll av hastighetsöverträdelse

Fel

Kortfel (förarens kortplats)
Kortfel (medförarens kortplats)
Displayfel
Överföringsfel
Skrivarfel
Sensorfel
Internt fel i fordonsenheten (VU)

Manuella angivelser

Dagens arbetspass fortfarande det samma?
Avslutande av föregående arbetspass?
Bekräfta eller ange plats för avslutande av arbetspass
Ange tid för påbörjande
Ange plats för påbörjande av arbetspass

Obs: Ytterligare kombinationer av piktogram för identifierare av utskriftsblock eller av register definieras i tillägg 4.

Tillägg 4

UTSKRIFTER

INNEHÅLL

1. ALLMÄNT

Varje utskrift byggs upp genom sammankedjning av olika datamängder, som eventuellt identifieras genom en blockidentifierare.

En datamängd innehåller en eller flera registreringar, som eventuellt identifieras genom en registeridentifierare.

PRT_001 När en blockidentifierare omedelbart föregår en registeridentifierare, skrivs registeridentifieraren inte ut.

PRT_002 Om en datapost inte är känd, eller måste 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 skall skrivas ut, utelämnas hela raden.

PRT_004 Numeriska datafält skrivs ut högerjusterade, med blanksteg för tusental och miljontal, och utan ledande nollor.

PRT_005 Strängdatafält skrivs ut vänsterjusterade och fylls med blanksteg till fältlängd, eller trunkeras vid behov till fältlängd (namn och adresser).

2. SPECIFICERING AV DATAMÄNGD

I detta kapitel används följande formatbeteckningar:

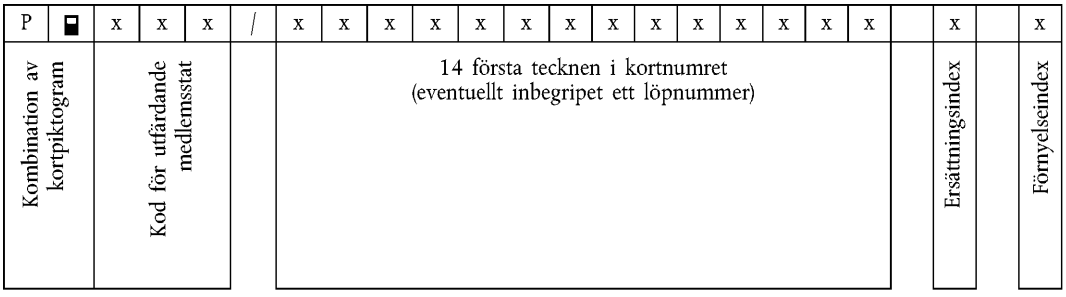
— Tecken i *fetstil* betyder att vanlig text skall skrivas ut (utskriften sker med vanliga tecken).

— Vanliga tecken betyder att variabler (piktogram eller data) skall ersättas med sina värden vid utskrift.

— Variabelnamn har strukits under för att visa den fältlängd som finns tillgänglig för variabeln.

— Data specificeras i formatet 'dd/mm/åååå' (dag, månad, år). Formatet 'dd.mm.åååå' 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.



PRT_006 Vid utskrift skall följande datamängd och/eller dataregistreringar användas, med följande betydelser och format:

Nummer på block eller registrering Betydelse	Data Format
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 ställning (endast utskrift av hastighetsöverträdelse)

```
-----------T ------------
Picto xxx  km/h
```

3 **Identifiering av kortinnehavare**

Blockidentifierare = personpiktogram

Kortinnehavarens efternamn

Kortinnehavarens förnamn (i förekommande fall)

Kortidentifiering

Kortets sista giltighetsdag (i förekommande fall)

Om kortet är opersonligt och inte innehåller något efternamn på innehavaren, skall företagets, verkstadens eller kontrollorganets namn skrivas i stället.

```
-----------P-------------
P Last_Name _______________
  First_Name _____________
Card_Identification _______
  dd/mm/yyyy
```

4 **Fordonsidentifiering**

Blockidentifierare

Fordonets identifieringsnummer (VIN)

Registrerande medlemsstat och fordonets registreringsnummer (VRN)

```
------------ -----------
 VIN _____________________
  Nat/VRN _______________
```

5 **Identifiering av fordonsenhet**

Blockidentifierare

Namn på tillverkaren av fordonsenheten

Fordonsenhetens delnummer

```
------------------------
 VU_Manufacturer _________
  VU_Part_Number __________
```

6 **Senaste kalibrering av färdskrivaren**

Blockidentifierare

Verkstadens namn

Identifiering av verkstadskort

Datum för kalibrering

```
------------T-----------
T Last_Name _______________
Card_Identification _______
T  dd/mm/yyyy
```

7 **Senaste kontroll (av en kontrollant)**

Blockidentifierare

Identifiering av kontrollantens kort

Datum och tidpunkt för kontroll samt typ av kontroll

Typ av kontroll: Upp till fyra piktogram. Kontrolltypen kan vara (en kombination av) följande:
: Överföring av data från kort. : Överföring av data från fordonsenhet. T: Utskrift. : Visning.

```
------------------------
Card_Identification _______
  dd/mm/yyyy hh:mm pppp
```

8 **Föraraktiviteter som finns lagrade på ett kort i den ordning de inträffat**

Blockidentifierare

Datum för förfrågan (kalenderdag för utskriften) + Närvaroräknare för kortet

```
------------------------
       dd/mm/yyyy xxx
```

8.1 *Period då kortet inte var isatt*

8.1a Registeridentifierare (periodens början)

8.1b *Okänd period*. Tid för påbörjande och avslutande, varaktighet

8.1c *Manuellt angiven aktivitet*

Aktivitetspiktogram, tid för påbörjande och avslutande (inbegripet), varaktighet, viloperioder på minst en timme är märkta med en stjärna.

```
   --------------------
?  hh:mm hh:mm hhhmm
A  hh:mm hh:mm hhhmm          *
```

8.2 *Isättning av kort i kortplats S*

Registeridentifierare, S = Öppningspiktogram

Medlemsstat där fordonet är registrerat och fordonets registreringsnummer

Fordonets vägmätare vid isättning

```
----------S----------
Nat/VRN _______________

x xxx xxx km
```

8.3 *Aktivitet (medan kortet var isatt)*

Aktivitetspiktogram, tid för påbörjande och avslutande (inbegripet), varaktighet, status för antal förare (piktogram med flera förare vid CREW (flera förare)), tomt vid SINGLE (ensam), viloperioder på minst en timme är märkta med en stjärna.

```
A hh:mm hh:mm hhhmm 00      *
```

8.3a *Särskild omständighet*. Tidpunkt för angivelse, piktogram för särskilda omständigheter (eller kombination av piktogram).

```
hh:mm ----- pppp -----
```

8.4 *Urtagning av kort*

Fordonets vägmätarvärde och tillryggalagd sträcka sedan senaste isättning för vilken vägmätarvärdet är känt

```
x xxx xxx km; x xxx km
```

9 **Föraraktiviteter som finns lagrade i en fordonsenhet per kortplats i kronologisk följd**

Blockidentifierare

Datum för förfrågan (kalenderdag för utskriften)

Fordonets vägmätarvärde klockan 00:00 och 24:00

```
-----------0-----------
        dd/mm/yyyy
x xxx xxx - x xxx xxx km
```

10 **Aktiviteter i kortplats S**

Blockidentifierare

```
---------- S ---------
```

10.1 *Period då inget kort är isatt i kortplats S*

Registeridentifierare

Inget kort isatt

Fordonets vägmätarvärde i början av perioden

```
--------------------
0 ---
  x xxx xxx km
```

10.2 *Kortisättning*

Registreringsidentifierare för isättning av kort

Förarens namn

Förarens förnamn

Identifiering av förarkort

Förarkortets sista giltighetsdag

Registrerande medlemsstat och registreringsnummer för föregående fordon som använts

Datum och tidpunkt för urtagning av kort från föregående fordon

Tom rad

Fordonets vägmätarvärde vid isättning av kortet, manuell angivelse av föraraktivitetsmarkering (M för ja, tom för nej).

```
--------------------
0 Last_Name _____________
  First_Name ____________
Card_Identification _______
   dd/mm/yyyy
Nat/VRN _______________

   dd/mm/yyyy hh:mm


   x xxx xxx km          M
```

10.3 *Aktivitet*

Aktivitetspiktogram, tid för påbörjande och avslutande (inbegripet), varaktighet, status för antal förare (piktogram med flera förare vid CREW (flera förare), tomt vid SINGLE (ensam)), viloperioder på minst en timme är märkta med en stjärna.

```
A hh:mm hh:mm hhhmm 00      *
```

10.3a *Särskild omständighet*. Tidpunkt för angivelse, piktogram för särskilda omständigheter (eller kombination av piktogram).

```
hh:mm ----- pppp -----
```

10.4 *Urtagning av kort eller slut på period med 'inget kort'*

Fordonets vägmätarvärde vid urtagning av kort eller i slutet av period med 'inget kort' och sträcka som tillryggalagts sedan isättning, eller sedan början av period med 'inget kort'.

```
x xxx xxx km; x xxx km
```

11 **Daglig sammanfattning**

Blockidentifierare

```
----------Σ ----------
```

11.1 *Sammanfattning för fordonsenhet av perioder utan kort i förarens kortplats*

Blockidentifierare

```
10■ - - -
```

11.2 *Sammanfattning för fordonsenhet av perioder utan kort i medförarens kortplats*

Blockidentifierare

```
20■ - - -
```

11.3 *Daglig sammanfattning för fordonsenheten per förare*

Registeridentifierare

Förarens efternamn

Förarens förnamn

Identifiering av förarkort

```
  --------------------
0 Last_Name _____________
  First_Name _____________
Card_Identification _______
```

11.4 *Angivelse av plats där dagens arbetspass påbörjas och/eller avslutas*

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

Vägmätarvärde

```
pihh:mm  Cou  Reg
  x xxx  xxx  km
```

11.5 *Aktivitetssammanfattning (från ett kort)*

Sammanlagd varaktighet för körning, tillryggalagd sträcka

Total varaktighet för arbete och närvaro

Total varaktighet för vila och okänd aktivitet

Total varaktighet för förarnas (crew) aktiviteter

```
  0 hhhmm x xxx km
  ⚒ hhhmm ◘ hhhmm
  ⊢ hhhmm ? hhhmm
00 hhhmm
```

11.6 *Aktivitetssammanfattning (perioder utan kort, förarens kortplats)*

Sammanlagd varaktighet för körning, tillryggalagd sträcka

Total varaktighet för arbete och närvaro

Total varaktighet för vila

```
  0 hhhmm x xxx km
  ⚒ hhhmm ◘ hhhmm
  ⊢ hhhmm
```

11.7 *Aktivitetssammanfattning (perioder utan kort, medförarens kortplats)*

Total varaktighet för arbete och närvaro

Total varaktighet för vila

```
  ⚒ hhhmm ◘ hhhmm
  ⊢ hhhmm
```

11.8 *Aktivitetssammanfattning (per förare, båda kortplatserna medtagna)*

Sammanlagd varaktighet för körning, tillryggalagd sträcka

Total varaktighet för arbete och närvaro

Total varaktighet för vila

Total varaktighet för förarnas (crew) aktiviteter

När en daglig utskrift begärs för innevarande dag beräknas informationen i sammanfattningen för dagen med hjälp av de data som finns tillgängliga vid tidpunkten för utskriften.

```
hhhmm x xxx km
hhhmm hhhmm
hhhmm
hhhmm
```

12 **Händelser och/eller fel som finns lagrade på ett kort**

12.1 Blockidentifierare senaste fem 'händelser och fel' från ett kort

```
-------- !x -------
```

12.2 Blockidentifierare alla registrerade 'händelser' på ett kort

```
--------- ! ---------
```

12.3 Blockidentifierare alla registrerade 'fel' på ett kort

```
--------- x ---------
```

12.4 *Registrering av händelser och/eller fel*

Registeridentifierare

Piktogram för händelse/fel, syfte med registreringen, datum och tidpunkt för påbörjande

Kod för ytterligare händelse/fel (i förekommande fall), varaktighet

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

```
--------------------
Pic (p)     dd/mm/yyyy hh:mm

!xxx                   hhhmm

Nat/VRN _____
```

13 **Händelser och/eller fel som finns lagrade eller håller på att registreras i en fordonsenhet**

13.1 Blockidentifierare senaste fem 'händelser och fel' från en fordonsenhet

```
-------- !x -------
```

13.2 Blockidentifierare alla registrerade 'händelser' som finns lagrade eller håller på att registreras i en fordonsenhet

```
--------- ! ---------
```

13.3 Blockidentifierare alla registrerade 'fel' som finns lagrade eller håller på att registreras i en fordonsenhet

```
--------- x ---------
```

13.4 *Registrering av händelse och/eller fel*

Registeridentifierare

Piktogram för händelse/fel, syfte med registreringen, datum och tidpunkt för påbörjande

Ytterligare kod för händelse/fel (i förekommande fall), antal liknande händelser samma dag, varaktighet

Identifiering av isatta kort vid händelsens eller felets början eller slut (högst fyra rader utan repetition av kortnummer)

Om inget kort var isatt

Registreringssyftet (p) är en numerisk kod som förklarar varför händelsen eller felet registrerades, som kodas i enlighet med dataelementet `EventFaultRecordPurpose`.

```
--------------------
Pic  (p)  dd/mm/yyyy  hh:mm

!xxx                  hhhmm

Card_Identification _______
Card_Identification _______
Card_Identification _______
Card_Identification _______
---
```

14 **Identifiering av fordonsenhet**

Blockidentifierare
Namn på tillverkaren av fordonsenheten
Adress till tillverkaren av fordonsenheten
Fordonsenhetens delnummer
Fordonsenhetens typgodkännandenummer
Fordonsenhetens serienummer
Fordonsenhetens tillverkningsår
Fordonsenhetens programvaruversion och datum för installation

```
----------⊟----------
⊟ Name _____________________
  Address _________________
  PartNumber _______
  Apprv _____________
  S/N _______
  yyyy
  v    xx.xx.xx   dd/mm/yyyy
```

15 **Identifiering av sensor**

Blockidentifierare
Sensorns serienummer
Sensorns typgodkännandenummer
Datum för första installation av sensorn

```
----------Л----------
Л S/N _______
  Apprv _____________
  dd/mm/yyyy
```

16 **Kalibreringsdata**

Blockidentifierare

```
----------T ---------
```

16.1 *Registrering av kalibrering*

Registeridentifierare
Verkstad som utfört kalibreringen
Verkstadens adress
Identifiering av verkstadskort
Verkstadskortets sista giltighetsdatum
Tom rad
Datum för + syfte med kalibrering
Fordonets identifieringsnummer
Registrerande medlemsstat och fordonets registreringsnummer
Fordonets karakteristiska koefficient
Färdskrivarens konstant:
Bildäckens effektiva omkrets
Dimensioner på monterade däck
Värde på hastighetsbegränsande anordning
Gamla och nya vägmätarvärden
Kalibreringssyftet (p) är en numerisk kod som förklarar varför dessa kalibreringsparametrar registrerades, och som kodas i enlighet med dataelementet `CalibrationPurpose`

```
  --------------------
T Workshop_name _____________
  Workshop_address _________
Card-Identification _______
  dd/mm/yyyy

T dd/mm/yyyy   (p)
Д VIN ________________________
  Nat/VRN __________

w  xx xxx Imp/km
k  xx xxx Imp/km
l  xx xxx mm
o  TyreSize __________
›  xxx km/h
x xxx xxx km; x xxx km
```

17 **Tidsinställning**

Blockidentifierare

```
----------◷ ---------
```

17.1 *Registrering av tidsinställning*

Registeridentifierare
Gammalt datum och gammal tidpunkt
Nytt datum och ny tidpunkt
Verkstad som utfört tidsinställningen
Verkstadens adress
Identifiering av verkstadskort
Verkstadskortets sista giltighetsdatum

```
  --------------------
! ◷ dd/mm/yyyy hh:mm
  ◷ dd/mm/yyyy hh:mm
T Workshop_name __________
  Workshop_address _______
Card_Identification ______
  dd/mm/yyyy
```

18 **Senaste händelse och fel som registrerats i fordonsenheten**

Blockidentifierare

Senaste datum och tidpunkt för händelse

Senaste datum och tidpunkt för fel

```
---------- !x ----------
!  dd/mm/yyyy  hh:mm
x  dd/mm/yyyy  hh:mm
```

19 **Information om kontroll av hastighetsöverträdelse**

Blockidentifierare

Datum och tidpunkt för senaste kontroll av hastighetsöverträdelse (OVER SPEEDING CONTROL)

Datum/tidpunkt för första hastighetsöverträdelse och antal hastighetsöverträdelsehändelser sedan dess

```
-----------›› ----------
›  dd/mm/yyyy  hh:mm
››xx dd/mm/yyyy hh:mm(UTC)
```

20 **Registrering av hastighetsöverträdelse**

20.1 Blockidentifierare 'första hastighetsöverträdelse sedan senaste kalibrering'

```
-------- ››T --------
```

20.2 Blockidentifierare 'de fem allvarligaste under de senaste 365 dygnen'

```
------- ››(365)-------
```

20.3 Blockidentifierare 'den allvarligaste under vart och ett av de senaste tio dygn de inträffat'

```
------- ››(10) -------
```

20.4 Registeridentifierare

Datum, tidpunkt och varaktighet

Högsta och genomsnittliga hastighet, antal liknande händelser samma dag

Förarens efternamn

Förarens förnamn

Identifiering av förarkort

```
   ------------------
›› dd/mm/yyyy hh:mm
   xxx km/h xxx km/h (xxx)

   Last_Name _____________
   First_Name _____________
Card_Identification _______
```

20.5 Om ingen registrering av hastighetsöverträdelse finns i ett block

```
›› - - -
```

21 **Handskriven information**

Blockidentifierare

21.1 Kontrollplats

21.2 Kontrollantens namnteckning

21.3 Från tidpunkt

21.4 Till tidpunkt

21.5 Förarens namnteckning

'Handskriven information', mata in ett tillräckligt antal tomma rader ovanför det som skall vara handskrivet, så att man verkligen kan skriva erforderlig information eller skriva under

```
------------------------
 ● .....
   .....
 ✚ .....
 ✚ .....
   .....
```

3. SPECIFIKATIONER FÖR UTSKRIFTER

I detta kapitel används följande formatbeteckningar:

N	Nummer N på registrering eller utskriftsblock
N	Nummer N på registrering eller utskriftsblock repeterat så många gånger som det behövs
X/Y	Utskriftsblock eller registreringar X och/eller Y efter behov, och repeterat så många gånger som det behövs

3.1 **Daglig utskrift från kort av föraraktiviteter**

PRT_007 Den dagliga utskriften från kort av föraraktiviteter skall ske i följande format:

1	Datum och tidpunkt för utskrift av dokumentet
2	Typ av utskrift
3	Identifiering av kontrollant (om ett kontrollkort har satts i fordonsenheten)
3	Identifiering av förare (från det kort som utskriften avser)
4	Identifiering av fordonet (fordon från vilket utskrift görs)
5	Identifiering av fordonsenhet (från vilken utskrift görs)
6	Senaste kalibrering av denna fordonsenhet
7	Senaste kontroll av föraren
8	Gränstecken för föraraktiviteter
8.1a / 8.1b / 8.1c / 8.2 / 8.3 / 8.3a / 8.4	Förarens aktiviteter i den ordning de inträffar
11	Gränstecken för daglig sammanfattning
11.4	Angivna platser i kronologisk ordning
11.5	Aktivitetssammanfattning
12.1	Händelser eller fel från gränstecken för kort
12.4	Registreringar av händelser/fel (de fem senaste händelser eller fel som finns lagrade på kortet)
13.1	Händelser eller fel från gränstecken för fordonsenhet
13.4	Registreringar av händelser/fel (de fem senaste händelser eller fel som finns lagrade eller håller på att registreras i fordonsenheten)
21.1	Kontrollplats
21.2	Kontrollantens namnteckning
21.5	Förarens namnteckning

3.2 **Daglig utskrift från fordonsenhet av föraraktiviteter**

PRT_008 Den dagliga utskriften från en fordonsenhet av föraraktiviteter skall ske i följande format:

1	Datum och tidpunkt för utskrift av dokumentet
2	Typ av utskrift
3	Identifiering av kortinnehavare (för alla kort som har satts i fordonsenheten)
4	Identifiering av fordonet (från vilket utskrift görs)
5	Identifiering av fordonsenhet (från vilken utskrift görs)
6	Senaste kalibrering av denna fordonsenhet
7	Senaste kontroll på denna färdskrivare
9	Gränstecken för föraraktiviteter
10	Gränstecken för förarens kortplats (kortplats 1)
10.1 / 10.2 / 10.3 /10.3a / 10.4	Aktiviteter i kronologisk ordning (förarens kortplats)
10	Gränstecken för medförarens kortplats (kortplats 2)
10.1 / 10.2 / 10.3 /10.3a / 10.4	Aktiviteter i kronologisk ordning (medförarens kortplats)
11	Gränstecken för daglig sammanfattning
11.1	Sammanfattning av perioder utan kort i förarens kortplats
11.4	Angivna platser i kronologisk ordning
11.6	Aktivitetssammanfattning

11.2	Sammanfattning av perioder utan kort i medförarens kortplats
11.4	Angivna platser i kronologisk ordning
11.7	Aktivitetssammanfattning
11.3	Sammanfattning av aktiviteter för en förare, båda kortplatser
11.4	Platser som denna förare angivit i kronologisk ordning
11.7	Aktivitetssammanfattning för denna förare
13.1	Gränstecken för händelser/fel
13.4	Registreringar av händelser/fel (de fem senaste händelser eller fel som finns lagrade eller håller på att registreras i fordonsenheten)
21.1	Kontrollplats
21.2	Kontrollantens namnteckning
21.3	Från tidpunkt (utrymme där en förare utan kort kan ange relevanta perioder)
21.4	Till tidpunkt
21.5	Förarens namnteckning

3.3 **Utskrift från kort av händelser och fel**

PRT_009 Den dagliga utskriften från kort av händelser och fel skall ske i följande format:

1	Datum och tidpunkt för utskrift av dokumentet
2	Typ av utskrift
3	Identifiering av kontrollant (om ett kontrollkort har satts i fordonsenheten)
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	Registrering av händelser (alla händelser som finns lagrade på kortet)
12.3	Gränstecken för fel
12.4	Registrering av fel (alla fel som finns lagrade på kortet)
21.1	Kontrollplats
21.2	Kontrollantens namnteckning
21.5	Förarens namnteckning

3.4 **Utskrift från fordonsenhet av händelser och fel**

PRT_010 Den dagliga utskriften från fordonsenheten av händelser och fel skall ske i följande format:

1	Datum och tidpunkt för utskrift av dokumentet
2	Typ av utskrift
3	Identifiering av kortinnehavare (för alla kortsom har satts i fordonsenheten)
4	Identifiering av fordonet (från vilket utskrift görs)
13.2	Gränstecken för händelser
13.4	Registrering av händelser (alla händelser som lagrats eller håller på att registreras i fordonsenheten)
13.3	Gränstecken för fel
13.4	Registrering av fel (alla fel som lagrats eller håller på att registreras i fordonsenheten)
21.1	Kontrollplats
21.2	Kontrollantens namnteckning
21.5	Förarens namnteckning

3.5 **Utskrift av tekniska data**

PRT_011 Utskrift av tekniska data skall ske i följande format:

1	Datum och tidpunkt för utskrift av dokumentet
2	Typ av utskrift
3	Identifiering av kortinnehavare (för alla kort som har satts i fordonsenheten)
4	Identifiering av fordonet (från vilket utskrift görs)
14	Identifiering av fordonsenhet
15	Identifiering av sensor
16	Gränstecken för kalibreringsdata
16.1	Kalibreringsregistreringar (alla tillgängliga registreringar i kronologisk ordning)
17	Gränstecken för tidsinställning
17.1	Registreringar av tidsinställningar (alla tillgängliga registreringar från register över tidsinställningar och kalibreringsdata)
18	Senaste händelse/fel som registrerats i fordonsenheten

3.6 **Utskrift av hastighetsöverträdelse**

PRT_012 Utskriften av hastighetsöverträdelser skall ske i följande format:

1	Datum och tidpunkt för utskrift av dokumentet
2	Typ av utskrift
3	Identifiering av kortinnehavare (för alla kort som har satts i fordonsenheten)
4	Identifiering av fordonet (från vilket utskrift görs)
19	Information om kontroll av hastighetsöverträdelse
20.1	Identifiering av data om hastighetsöverträdelser
20.4 / 20.5	Första hastighetsöverträdelse efter senaste kalibrering
20.2	Identifiering av data om hastighetsöverträdelser
20.4 / 20.5	De fem mest allvarliga hastighetsöverträdelserna under de senaste 365 dygnen
20.3	Identifiering av data om hastighetsöverträdelser
20.4 / 20.5	Den allvarligaste hastighetsöverträdelsen under vart och ett av de senaste tio dygn de inträffat
21.1	Kontrollplats
21.2	Kontrollantens namnteckning
21.5	Förarens namnteckning

Tillägg 5

DISPLAY

I detta tillägg används följande formatbeteckningar:

— Tecken i **fetstil** betyder att vanlig text skall visas (visningen sker med vanliga tecken).

— Vanliga tecken betyder att variabler (piktogram eller data) skall ersättas med sina värden vid visning:

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 driftläge

DIS_001 Färdskrivaren skall visa data i följande format:

Data	Format
Uppgifter som visas automatiskt	
Lokaltid	hh:mm
Driftläge	O
Information om föraren	1 Dhh**h**mm ▮▮hh**h**mm
Information om medföraren	2 Dhh**h**mm
Omständigheten 'omfattas ej' öppnad	OUT
Visade varningar	
Sammanhängande körtid överskrids	10 hh**h**mm ▮▮hh**h**mm
Händelse eller fel	EF
Övrig visad information	
UTC-datum	UTC dd/mm/aaaa or UTC dd.mm.aaaa
Tid	hh:mm
Förarens sammanhängande körtid och sammanlagda avbrottstid	10 hh**h**mm ▮▮hh**h**mm
Medförarens sammanhängande körtid och sammanlagda avbrottstid	20 hh**h**mm ▮▮hh**h**mm
Förarens sammanlagda körtid för föregående och innevarande vecka	10 ‖ hhh**h**mm
Medförarens sammanlagda körtid för föregående och innevarande vecka	20 ‖ hhh**h**mm

Tillägg 6

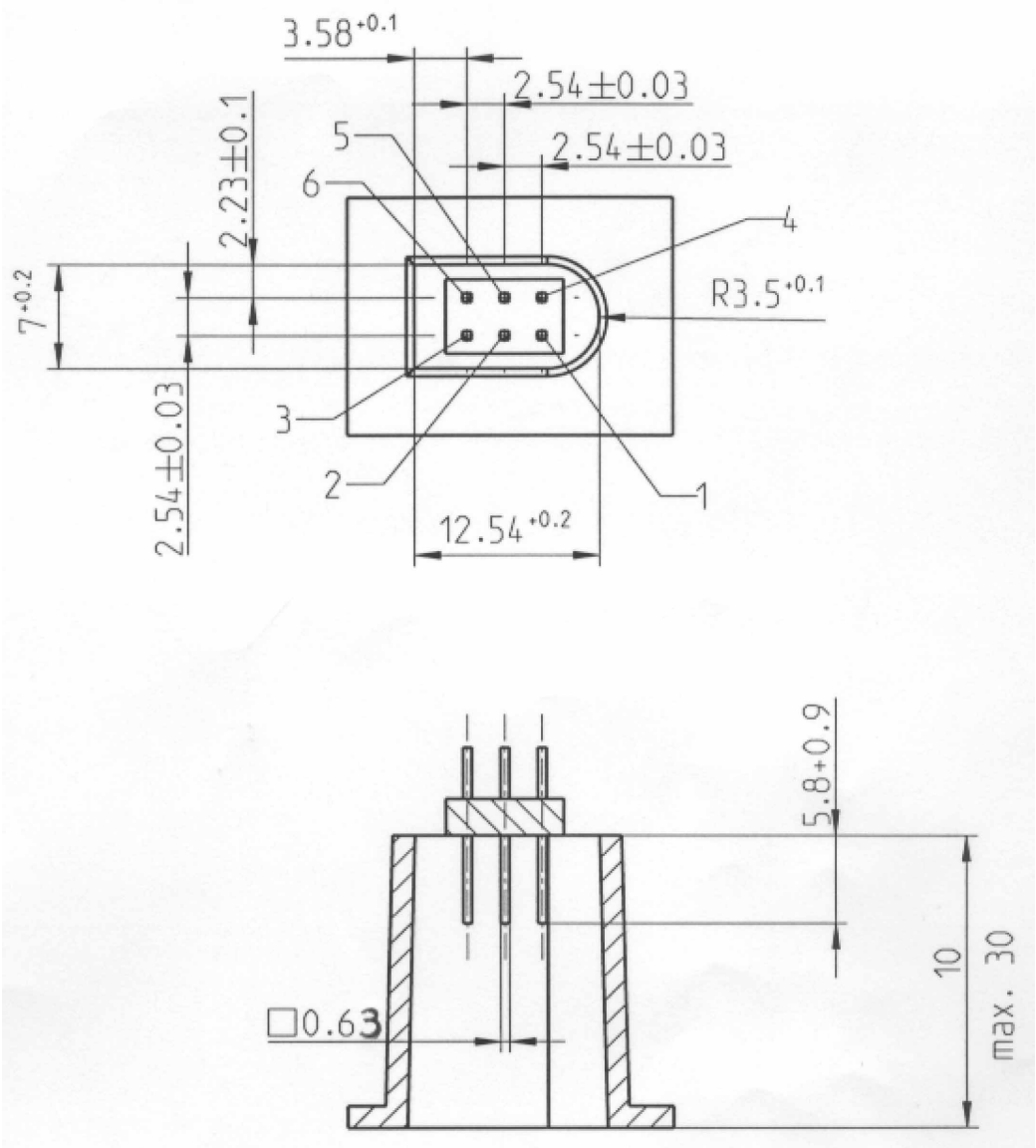
EXTERNA GRÄNSSNITT

INNEHÅLL

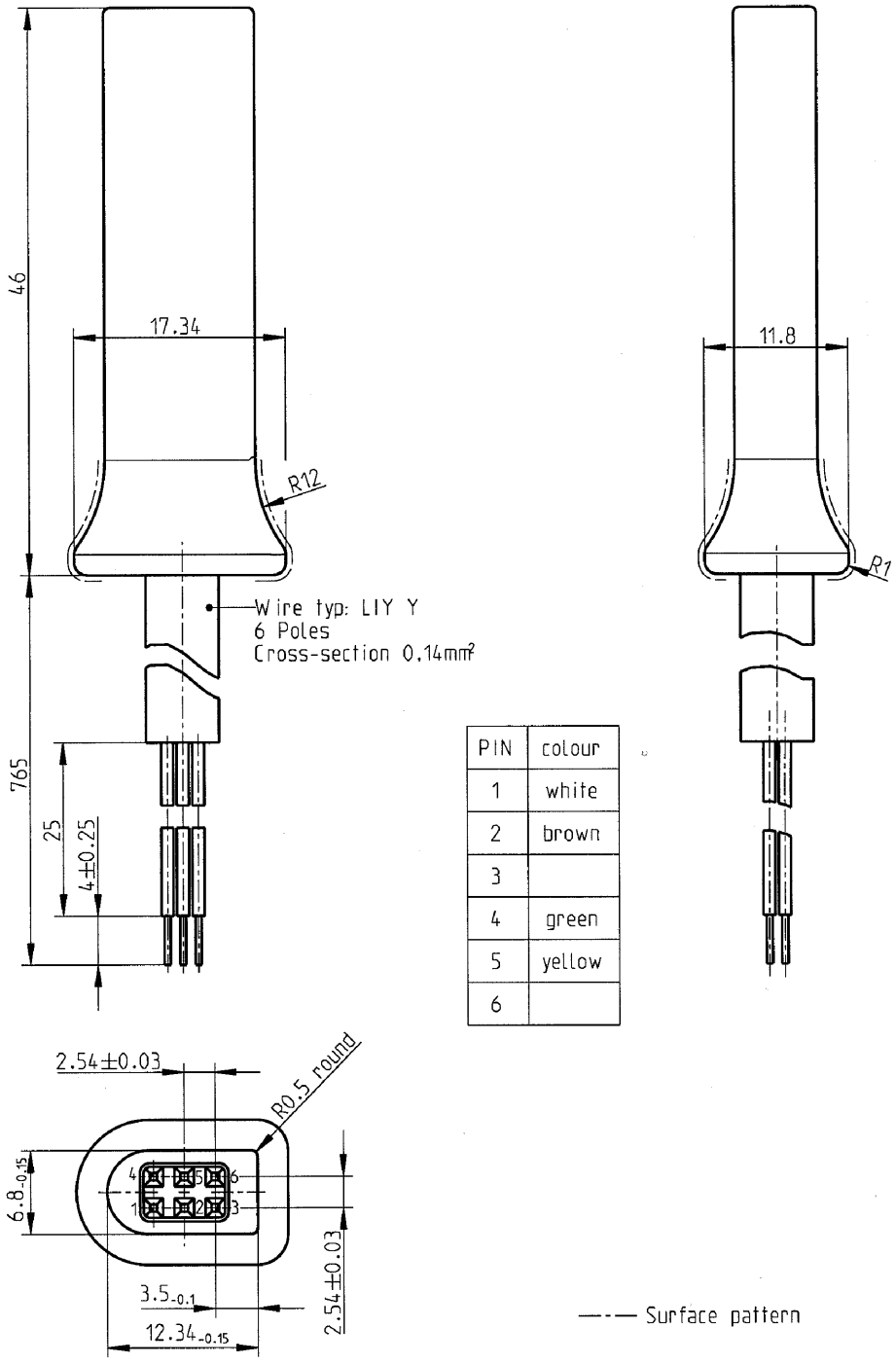
1. MASKINVARA

1.1 **Anslutning**

INT_001 Kalibrerings-/överföringsanslutningen skall vara en 6-stiftsanslutning, som är tillgänglig på frontplattan utan att man behöver koppla ur någon del av färdskrivaren, och den skall överensstämma med följande ritning (alla mått i millimeter).



I följande diagram visas en typisk matchande kontakt (mating plug) med 6 stift:



PIN	colour
1	white
2	brown
3	
4	green
5	yellow
6	

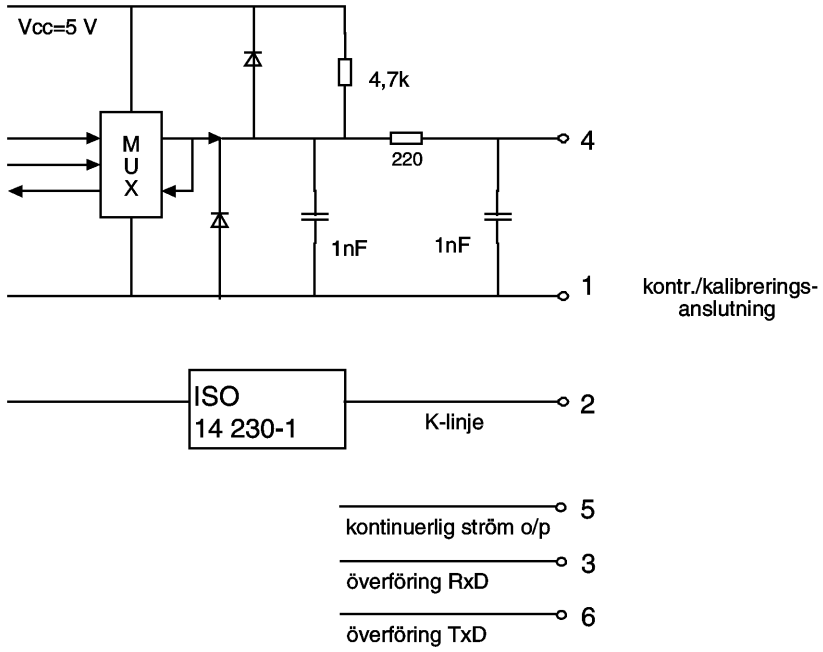
1.2 **Fördelning av kontakter**

INT_002 Kontakterna skall fördelas enligt följande tabell:

Stift	Beskrivning	Anmärkning
1	Batteriminus	Ansluten till fordonets batteriminus
2	Datakommunikation	K-linje (ISO 14230-1)
3	RxD – överföring	Ingående data till färdskrivaren
4	Ingående/utgående signal	Kalibrering
5	Permanent utgående ström	Spänningsomfånget specificeras till fordonets ström-minus 3V för att möjliggöra spänningsfall över den skyddande strömkretsanordningen Utgående ström 40 mA
6	TxD – överföring	Utgående data från färdskrivaren

1.3. **Blockdiagram**

INT_003 Blockdiagrammet skall överensstämma med följande:



2. GRÄNSSNITT FÖR ÖVERFÖRING

INT_004 Gränssnittet för överföring skall överensstämma med RS232-specifikationerna.

INT_005 Gränssnittet för överföring skall använda en start-bit, 8 data-bitar LSB först, en jämn paritets-bit och en stopp-bit.

Organisering av data-byte

Start-bit: en bit med logisk nivå 0

Data-bitar: överförs med LSB-först.

Paritets-bit: jämn paritet

Stopp-bit: en 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 Baud-nivåerna för överföringen skall vara justerbara från 9 600 bps till 115 200 bps. Överföringen skall ske med största möjliga överföringshastighet, med en inledande baud-nivå efter kommunikationsstart satt till 9 600 bps.

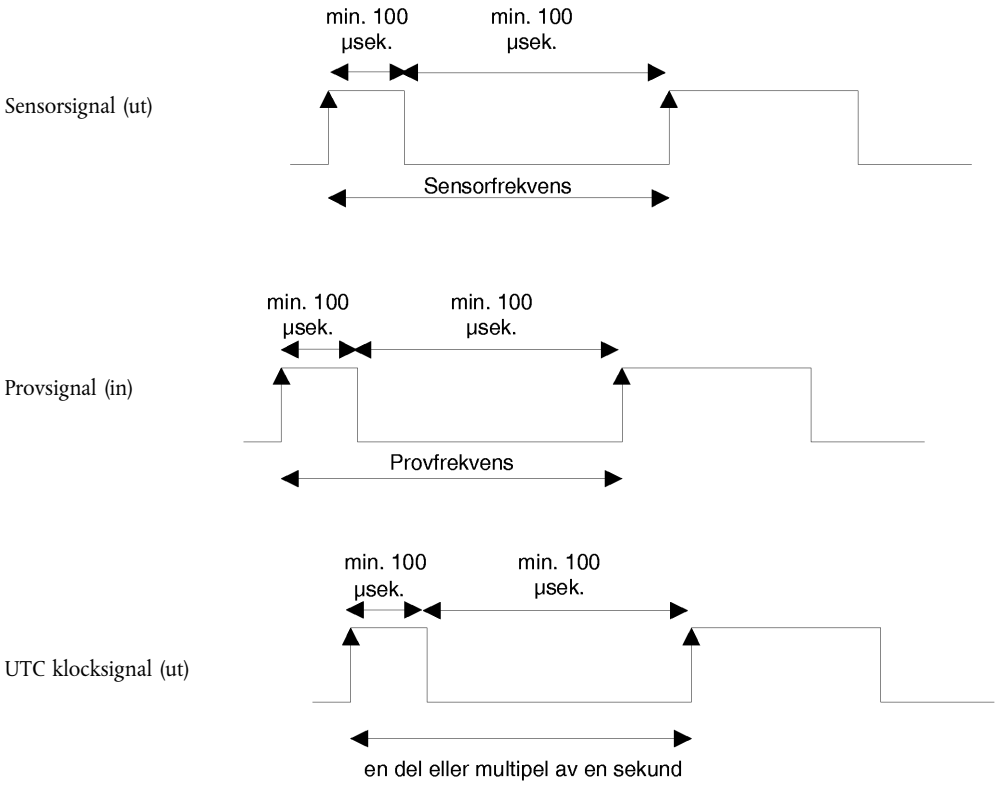
3. GRÄNSSNITT FÖR KALIBRERING

INT_007 Datakommunikationen skall överensstämma med ISO 14230-1 Vägfordon – Keyword Protocol 2000 för diagnostiksystem – Del 1: Fysiskt skikt, första utgåvan: 1999.

INT_008 Ingående/utgående signal skall överensstämma med följande elektriska specifikationer:

Parameter	Min	Typisk	Max	Anmärkning
U_{low} (in)			1,0 V	I = 750 µA
$U_{U\ high}$ (out)	4 V			I = 200 µA
Frekvens			4 kHz	
U_{low} (out)			1,0 V	I = 1 mA
U_{high} (out)	4 V			I = 1 mA

INT_009 Ingående/utgående signal skall överensstämma med följande tidsdiagram:



Tillägg 7

PROTOKOLL FÖR DATAÖVERFÖRING

INNEHÅLL

1. INLEDNING

I detta tillägg specificeras de förfaranden som måste följas för att man skall kunna utföra de olika typerna av dataöverföring till ett externt lagringsmedium (External Storage Medium – ESM), och de protokoll som man måste använda för att säkerställa korrekt dataöverföring och full kompatibilitet hos överfört dataformat så att alla kontrollanter skall kunna besiktiga dessa data och kontrollera deras autenticitet och integritet innan de analyserar dem.

1.1 **Räckvidd**

Data kan överföras till ett externt lagringsmedium på följande sätt:

— Från en fordonsenhet, av en IDE (Intelligent Dedicated Equipment) som är ansluten till fordonsenheten.

— Från ett färdskrivarkort, av en IDE utrustad med en kortläsare (Interface Device – IFD).

— Från ett färdskrivarkort via en fordonsenhet, av en IDE 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 (Gemensamma säkerhetsmekanismer). Identifiering av källutrustning (fordonsenhet eller kort) och dess säkerhetscertifikat (medlemsstat och utrustning) överförs också. Den som verifierar dessa data måste oberoende ha en betrodd europeisk öppen nyckel.

DDP_001 Data som överförs under en överföringssession måste lagras på det externa lagringsmediet inom en fil.

1.2 **Förkortningar och beteckningar**

Följande förkortningar används i detta tillägg:

AID	Application Identifier – Tillämpningsidentifierare
ATR	Answer To Reset – Återställningssignal
CS	Checksum byte – Kontrollsumme-byte
DF	Dedicated File – Katalog
DS	Diagnostic Session – Diagnossession
EF	Elementary File – Datafil
ESM	External Storage Medium – Externt lagringsmedium
FID	File Identifier (File ID) – Filidentifierare
FMT	Format Byte (first byte of a message header) – Format-byte (första byte i ett meddelandehuvud (message header))
ICC	Integrated Circuit Card – IC-kort, kort med integrerade kretsar
IDE	Intelligent Dedicated Equipment – Intelligent tilldelad utrustning: Utrustning för att överföra data till ett externt lagringsmedium (exempelvis en persondator)
IFD	Interface Device – Kortläsare
KWP	Keyword Protocol 2000
LEN	Length Byte – Längd-byte (första byte i meddelandehuvud)
PPS	Protocol Parameter Selection – Val av protokollparameter
PSO	Perform Security Operation – Utför Security Operation (säkerhetsoperation)
SID	Service Identifier – Tjänste-identifierare
SRC	Source byte – Käll-byte
TGT	Target Byte – Mål-byte
TLV	Tag Length Value – Tagglängdsvärde
TREP	Transfer Response Parameter – Parameter för överföringssvar
TRTP	Transfer Request Parameter – Parameter för begäran om överföring
VU	Vechicle Unit – Fordonsenhet

2. ÖVERFÖRING AV FORDONSENHETSDATA

2.1 **Överföring**

För att överföra fordonsenhetsdata, måste operatören göra följande:

— Sätta i sitt färdskrivarkort i en kortplats i fordonsenheten ([1]).

— Ansluta IDE till fordonsenhetens överföringsanslutning.

— Upprätta en anslutning mellan IDE och fordonsenhet.

— På IDE välja de data som skall överföras och sända begäran till fordonsenheten.

— Avsluta överföringssessionen.

2.2 **Protokoll för dataöverföring**

Protokollet är uppbyggt enligt modellen 'master-slave', med IDE som 'master' och fordonsenheten som 'slave'.

Meddelandestruktur, meddelandetyper och meddelandeflöden bygger huvudsakligen på Keyword Protocol 2000 (KWP) (ISO 14230-2 Vägfordon – Keyword Protocol 2000 för diagnostiksystem – Del 2: Länkskikt).

Tillämpningsskiktet grundas i princip på det gällande utkastet till ISO 14229-1 (Vägfordon – Diagnostikssystem – Del 1: Diagnostiska tjänster, version 6 av den 22 februari 2001).

2.2.1 ***Meddelandestruktur***

DDP_002 Alla de meddelanden som utbyts mellan IDE och fordonsenhet formateras med en struktur som består av följande tre delar:

— Huvud bestående av en format-byte (Format byte – FMT), en mål-byte (Target byte – TGT), en käll-byte (Source byte – SRC) och eventuellt en längd-byte (Length byte – LEN).

— Datafält bestående av tjänsteidentifierar-byte (Service Identifier Byte – SID) och ett varierande antal databyte, som kan inbegripa en byte för diagnossession (DS) eller en byte för en överföringsparameter (TREP eller TRTP).

— Kontrollsumma (checksum) bestående av en kontrollsummebyte (Checksum byte – CS).

Huvud				Datafält					Kontroll-summa
FMT	TGT	SRC	LEN	SID	DATA	…	…	…	CS
4 byte				Max 255 byte					1 byte

TGT- och SRC-byte representerar den fysiska adressen till meddelandets mottagare och avsändare. Värdena är F0 Hex för IDE och EE Hex för fordonsenheten.

LEN-byte är längden på datafältsdelen.

Kontrollsumme-byte är 8 bits-summorna modulo 256 av alla byte i meddelandet utom CS själv.

FMT-, SID-, DS-, TRTP- och TREP-byte definieras nedan i detta dokument.

([1]) Det kort som satts i kommer att utlösa lämpliga tillträdesrättigheter till överföringsfunktion och till data.

DDP_003 I de fall där de data som skall överföras i meddelandet är längre än det utrymme som finns tillgängligt i datafältsdelen sänds meddelandet i själva verket i flera undermeddelanden. Varje undermeddelande har ett huvud, samma SID, TREP och en undermeddelanderäknare på 2 byte som anger undermeddelandenummer inom hela meddelandet. IDE kvitterar varje undermeddelande för att möjliggöra felkontroll och för att avbryta. IDE 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 (utom SID TREP och undermeddelanderäknare) datafält tillfogas för att visa slutet på meddelandet.

Exempel:

Huvud	SID	TREP	Meddelande	CS
4 byte	Längre än 255 byte			

Kommer att överföras som

Huvud	SID	TREP	00	01	Undermeddelande 1	CS
4 byte	255 byte					

Huvud	SID	TREP	00	02	Undermeddelande 2	CS
4 byte	255 byte					

…

Huvud	SID	TREP	xx	yy	Undermeddelande n	CS
4 byte	Mindre än 255 byte					

eller som

Huvud	SID	TREP	00	01	Undermeddelande 1	CS
4 byte	255 byte					

Huvud	SID	TREP	00	02	Undermeddelande 2	CS
4 byte	255 byte					

…

Huvud	SID	TREP	xx	yy	Undermeddelande n	CS
4 byte	255 byte					

Huvud	SID	TREP	xx	yy+1	CS
4 byte	4 byte				

2.2.2 ***Meddelandetyper***

Kommunikationsprotokollet för dataöverföring mellan fordonsenhet och IDE förutsätter utbyte av 8 olika meddelandetyper.

Dessa meddelanden sammanfattas i följande tabell.

Meddelandestruktur	Max 4 byte Huvud				Max 255 byte Data			1 byte Kontroll-summa
IDE -> <- FE	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		8F,EA	9B
Start Diagnostic Session Request	80	EE	F0	02	10	81		F1
Positive Response Start Diagnostic	80	F0	EE	02	50	81		31
Link Control Service (länkkontrolltjänst)								
Verify Baud Rate (stage 1) (kontrollera baud-nivån, 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	ED
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 (positivt svar kontrollera baud-nivån)	80	F0	EE	02	C7		01	28
Transition Baud Rate (stage 2) (övergång baud-nivån, steg 2)	80	EE	F0	03	87		02,03	ED
Request Upload	80	EE	F0	0A	35		00,00,00,0-0,00,FF,FF,-FF,FF	99
Positive Response Request Upload	80	F0	EE	03	75		00,FF	D5
Transfer Data Request								
Översikt	80	EE	F0	02	36	01		97
Activities	80	EE	F0	06	36	02	Date	CS
Events & Faults	80	EE	F0	02	36	03		99
Detailed Speed	80	EE	F0	02	36	04		9A
Technical Data	80	EE	F0	02	36	05		9B
Card download	80	EE	F0	02	36	06		9C
Positive Response Transfer Data	80	F0	EE	Len	76	TREP	Data	CS
Request Transfer Exit	80	EE	F0	01	37			96
Positive Response Request Transfer Exit	80	F0	EE	01	77			D6
Stop Communication Request	80	EE	F0	01	82			E1
Positive Response Stop Communication	80	F0	EE	01	C2			21
Acknowledge sub message	80	EE	F0	Len	83		Data	CS
Negative responses								
General reject	80	F0	EE	03	7F	Sid Req	10	CS
Service not supported	80	F0	EE	03	7F	Sid Req	11	CS
Sub function not supported	80	F0	EE	03	7F	Sid Req	12	CS
Incorrect Message Length (inkorrekt meddelande-längd)	80	F0	EE	03	7F	Sid Req	13	CS
Conditions not correct or Request sequence error (villkoren är inkorrekta eller begäran sekvensfel)	80	F0	EE	03	7F	Sid Req	22	CS
Request out of range (begäran utom räckhåll)	80	F0	EE	03	7F	Sid Req	31	CS
Upload not accepted	80	F0	EE	03	7F	Sid Req	50	CS
Response pending	80	F0	EE	03	7F	Sid Req	78	CS
Data not available	80	F0	EE	03	7F	Sid Req	FA	CS

Anmärkningar:
— Sid Req = Sid för motsvarande begäran
— TREP = TRTP för motsvarande begäran.
— Mörka fält betecknar att inget har överförts.
— Termen uppläggning (upload) (sett från IDE) används för kompatibilitet med ISO 14229. Det betyder samma sak som överföring (download) (sett från fordonsenheten).
— Möjliga 2-byte undermeddelanderäknare visas inte i tabellen.

2.2.2.1 *Start Communication Request (SID 81)*

DDP_005 IDE utfärdar detta meddelande för att upprätta kommunikationslänken med fordonsenheten. De första meddelandena utväxlas alltid med 9 600 baud (tills överföringshastigheten så småningom ändras med hjälp av lämpliga länkkontrolltjänster (Link control services)).

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 2 nyckel-byte ′8F′ ′EA′ som anger att enheten stödjer protokoll med huvud inbegripet information om målkälla (target source) och längd.

2.2.2.3 *Start Diagnostic Session Request (SID 10)*

DDP_007 IDE utfärdar meddelandet med begäran Start Diagnostic Session (starta diagnossession) för att begära en ny diagnossession med fordonsenheten. Underfunktionen 'default session' (81 Hex) anger att en standard diagnossession skall öppnas.

2.2.2.4 *Positive Response Start Diagnostic (SID 50)*

DDP_008 Fordonsenheten sänder meddelandet Positive Response Start Diagnostic (positivt svar start diagnos) för att svara positivt på begäran om diagnossession (Diagnostic Session Request)

2.2.2.5 *Link Control Service (SID 87)*

DDP_052 IDE använder Link Control Service (länkkontrolltjänsten) för att inleda ändringen av överföringshastigheten (baud-nivån), vilket sker i följande två steg: I steg ett föreslår IDE ändringen av baud-nivån. Vid mottagandet av ett positivt svar från fordonsenheten utfärdar IDE en bekräftelse av ändringen av baud-nivån till fordonsenheten (steg två). Därefter ändrar IDE till den nya baud-nivån. Efter mottagandet av bekräftelsen ändrar fordonsenheten till den nya baud-nivån.

2.2.2.6 *Link Control Positive Response (SID C7)*

DDP_053 Fordonsenheten utfärdar Link Control Positive response (positivt svar för länkkontrollen) för att svara positivt på begäran om länkkontrolltjänst (Link Control Service request) (steg ett). Det bör noteras att inget svar lämnas på begäran om bekräftelse (steg två).

2.2.2.7 *Request Upload (SID 35)*

DDP_009 IDE utfärdar meddelandet Request Upload (begäran uppläggning) för att specificera för fordonsenheten att en överföring har begärts. För att uppfylla kraven i ISO14229 ingår uppgifter som omfattar adress, storlek och format för de uppgifter som begärs. Eftersom dessa inte är kända av IDE 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 (positivt svar begäran uppläggning) för att ange för IDE att fordonsenheten är beredd att överföra data. För att uppfylla kraven i ISO14229 ingår uppgifter i detta meddelande som anger för IDE att ytterligare meddelanden om Positive Response Transfer Data (positivt svar överföring data) kommer att omfatta högst 00FF byte (hex).

2.2.2.9 *Transfer Data Request (SID 36)*

DDP_011 IDE sänder begäran Transfer Data Request (överföring data begäran) för att för fordonsenheten specificera typen av data som skall överföras. En Transfer Request Parameter (TRTP, parameter för begäran om överföring) på en byte anger överföringstypen.

Det finns sex typer av dataöverföring:

— Översikt (TRTP 01),

— Aktiviteter med avseende på ett särskilt datum (TRTP 02),

— Händelser och fel (TRTP 03),

— Detaljerad hastighet (TRTP 04),

— Tekniska data (TRTP 05),

— Kortöverföring (TRTP 06).

DDP_054 IDE måste begära översiktsdataöveföringen (TRTP 01) under en överföringssession, eftersom det är det enda sättet att se till 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 (överföring data begäran) angivelse av den kalenderdag (formatet `TimeReal`) som skall överföras.

2.2.2.10 *Positive Response Transfer Data (SID 76)*

DDP_012 Fordonsenheten sänder meddelandet Positive Response Transfer Data (positivt svar överföring data) som svar på Transfer Data Request (överföring data begäran). Meddelandet innehåller begärda data, med en Transfer Response Parameter (TREP,parameter för överföringssvar) som motsvarar TRTP i begäran.

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

— Säkerhetscertifikat.

— Fordonsidentifiering.

— Fordonsenhetens aktuella datum och tid.

— Min och Max överföringsbart datum (fordonsenhetsdata).

— Angivelse av korts närvaro i fordonsenheten.

— Tidigare överföring till ett företag.

— Företagslås.

— Tidigare kontroller.

2.2.2.11 *Request Transfer Exit (SID 37)*

DDP_013 IDE sänder meddelandet Request Transfer Exit (begäran om avslutning av överföring) för att informera fordonsenheten om att överföringssessionen har avslutats.

2.2.2.12 *Positive Response Request Transfer Exit (SID 77)*

DDP_014 Fordonsenheten sänder meddelandet Positive Response Request Transfer Exit – positivt svar begäran om avslutning av överföring för att kvittera Request Transfer Exit (begäran om avslutning av överföring).

2.2.2.13 *Stop Communication Request (SID 82)*

DDP_015 IDE sänder meddelandet Stop Communication Request (avslutad kommunikation begäran) för att koppla ur kommunikationslänken med fordonsenheten.

2.2.2.14 *Positive Response Stop Communication (SID C2)*

DDP_016 Fordonsenheten sänder meddelandet Positive Response Stop Communication (positivt svar avslutning kommunikation) för att kvittera Stop Communication Request (avslutning kommunikation begäran).

2.2.2.15 *Acknowledge Sub Message (SID 83)*

DDP_017 IDE sänder meddelandet Acknowledge Sub Message (kvittera undermeddelande) för att bekräfta mottagandet av varje del av ett meddelande som överförs som flera undermeddelanden. Datafältet innehåller SID som mottagits från fordonsenheten och en 2 byte-kod enligt följande:

— MsgC +1 kvitterar korrekt mottagande av undermeddelande nummer MsgC.

Begäran från IDE till fordonsenheten att sända nästa undermeddelande.

— MsgC anger att ett problem uppstått med mottagande av undermeddelande nummer MsgC.

Begäran från IDE till fordonsenheten att sända undermeddelandet igen.

— FFFF begär att meddelandet avslutas.

Detta kan användas av IDE för att avsluta överföringen av fordonsenhetens meddelande av vilken orsak som helst.

Det sista undermeddelandet i ett meddelande (LEN byte < 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 (positivt svar överföring data) (SID 76).

2.2.2.16 *Negative Response (SID 7F)*

DDP_018 Fordonsenheten sänder meddelandet Negative Response (negativt svar) som svar på ovan nämnda meddelande med 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 general reject (allmänt avslag).

Åtgärden kan inte utföras av en anledning som inte omfattas nedan.

— 11 service not supported (tjänsten stöds ej)

SID för begäran ej förstådd.

— 12 sub function not supported (underfunktion stöds ej)

DS eller TRTP för begäran är inte förstådd, eller det finns inga ytterligare undermeddelanden som skall överföras.

— 13 incorrect message length (felaktig meddelandelängd)

Längden på det mottagna meddelandet är felaktig.

— 22 conditions not correct or request sequence error (villkoren är felaktiga eller sekvensfel i begäran)

Den begärda tjänsten är inte aktiv eller sekvensen i ett meddelande med begäran är felaktig.

— 31 Request out of range (ogiltigt värde på begäran)

Parameterregistret för begäran (datafält) är inte giltigt.

— 50 upload not accepted (uppläggning ej godtagen).

Begäran kan inte utföras (fordonsenheten i olämpligt driftläge eller internt fel i fordonsenheten).

— 78 response pending (svar ej avslutat).

Begärd åtgärd kan inte avslutas 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 (till exempel: inget kort har satts i, …).

2.2.3 ***Meddelandeflöde***

Nedan visas ett typiskt meddelandeflöde under en normal dataöverföring:

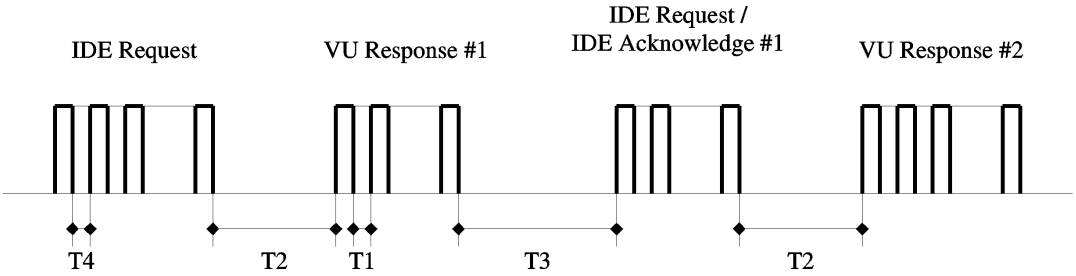
IDE		VU
Start Communication Request	⇨	
	⇦	Positive Response
Start Diagnostic Service Request	⇨	
	⇦	Positive Response
Request Upload	⇨	
	⇦	Positive Response
Transfer Data Request Overview	⇨	
	⇦	Positive Response
Transfer Data Request #2	⇨	
	⇦	Positive Response #1
Acknowledge Sub Message #1	⇨	
	⇦	Positive Response #2
Acknowledge Sub Message #2	⇨	
	⇦	Positive Response #m
Acknowledge Sub Message #m	⇨	
	⇦	Positive Response (Data Field < 255 Bytes)
Acknowledge Sub Message (optional)	⇨	
	…	
Transfer Data Request #n	⇨	
	⇦	Positive Response
Request Transfer Exit	⇨	
	⇦	Positive Response
Stop Communication Request	⇨	
	⇦	Positive Response

2.2.4 ***Tidsavpassning***

DDP_019 Vid normal drift är de tidsparametrar som visas i följande figur relevanta:

Figur 1

Meddelandeflöde, tidsavpassning



där

P1 = Interbyte-tid för fordonsenhetens svar.

P2 = Tid mellan slut på IDE-begäran och början på fordonsenhets svar, eller mellan slut på IDE-kvittering och början på nästa svar från fordonsenhet.

P3 = Tid mellan slut på svar från fordonsenhet och början på ny IDE-begäran, eller mellan slut på fordonsenhets svar och början på IDE-kvittering, eller mellan slut på IDE-begäran och början på ny IDE-begäran om fordonsenheten inte svarar.

P4 = Interbyte-tid för IDE-begäran.

P5 = Utökat värde för P3 för överföring från kort.

Tillåtna värden för tidsparametrar visas i följande tabell (KWP utökade tidsparametrar satta, används vid fysisk adressering för snabbare kommunikation).

Parameter	Nedre gräns Värde (ms)	Övre gräns Värde (ms)
P1	0	20
P2	20	1 000 (*)
P3	10	5 000
P4	5	20
P5	10	20 minuter

(*) Om fordonsenheten svarar med ett Negative Response (negativt svar) som innehåller en kod som betyder 'begäran korrekt mottagen, svar kommer', utökas detta värde till samma övre gränsvärde som 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 förfarandena för felhantering med avseende på fordonsenhet respektive IDE.

2.2.5.1 *Fasen Start Communication*

DDP_020 Om IDE upptäcker ett fel under Start Communication-fasen, 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, skall den inte sända något svar utan vänta på ett till Start Communication Request-meddelande inom en period P3max.

2.2.5.2 *Fasen Communication*

Följande två typer av felhantering kan definieras:

1. Fordonsenheten upptäcker ett fel vid IDE-överföring

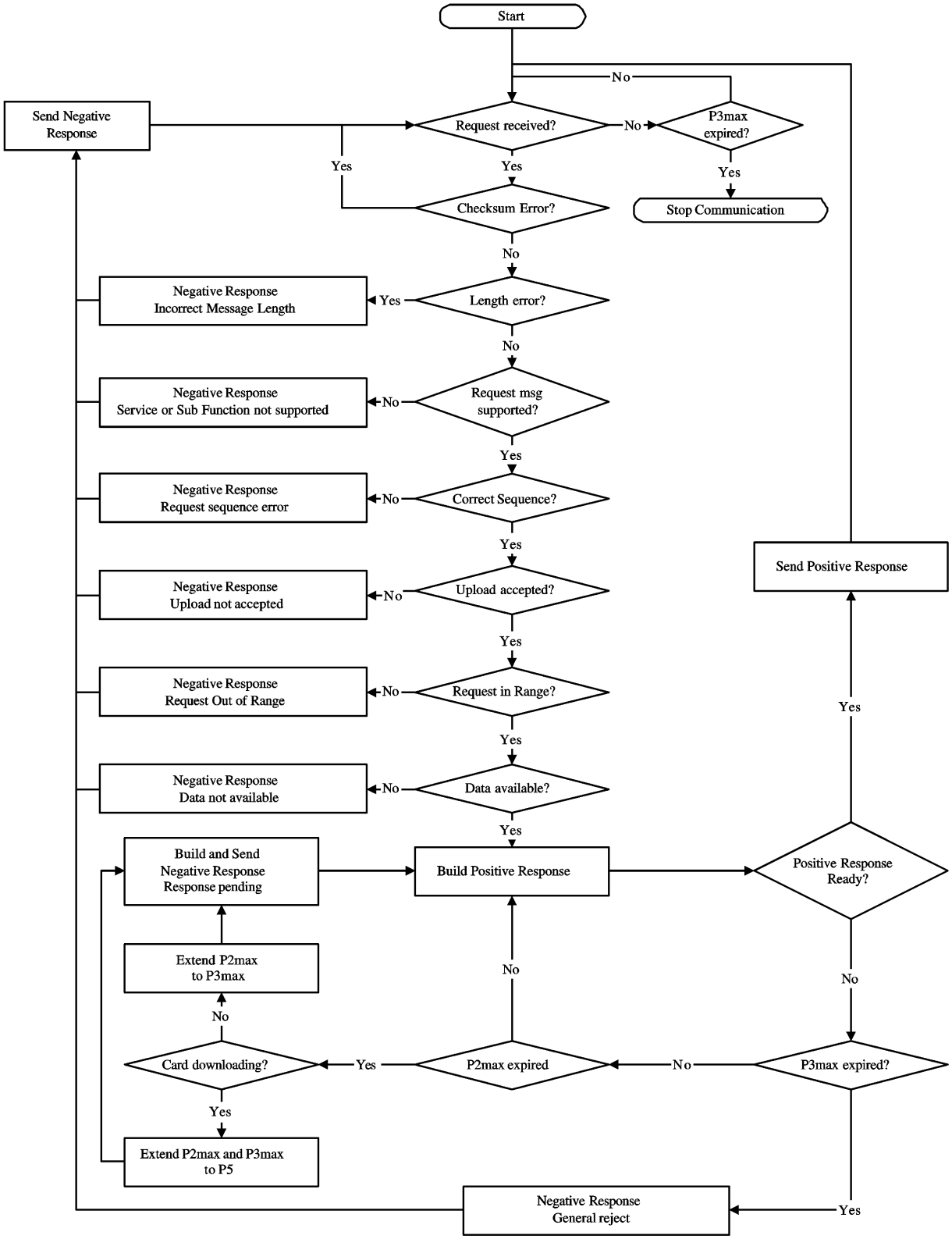
DDP_022 För varje mottaget meddelande skall fordonsenheten upptäcka tidsfel, byte-formatfel (exempelvis överträdelser med avseende på start- och stopp-bitar) och ramfel (fel antal mottagna byte, fel kontrollsumme-byte).

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 (exempelvis meddelandet stöds ej) även om meddelandet uppfyller kraven med avseende på längd och kontrollsumma. I så fall skall fordonsenheten svara IDE med ett Negative Response-meddelande (negativt svarsmeddelande) som specificerar felets natur.

Figur 2

Hantering av fordonsenhetsfel



2. IDE upptäcker ett fel vid överföring från fordonsenhet

DDP_025 För varje mottaget meddelande skall IDE upptäcka tidsfel, byte-formatfel (exempelvis överträdelser med avseende på start- och stopp-bitar) och ramfel (fel antal mottagna byte, fel kontrollsumme-byte).

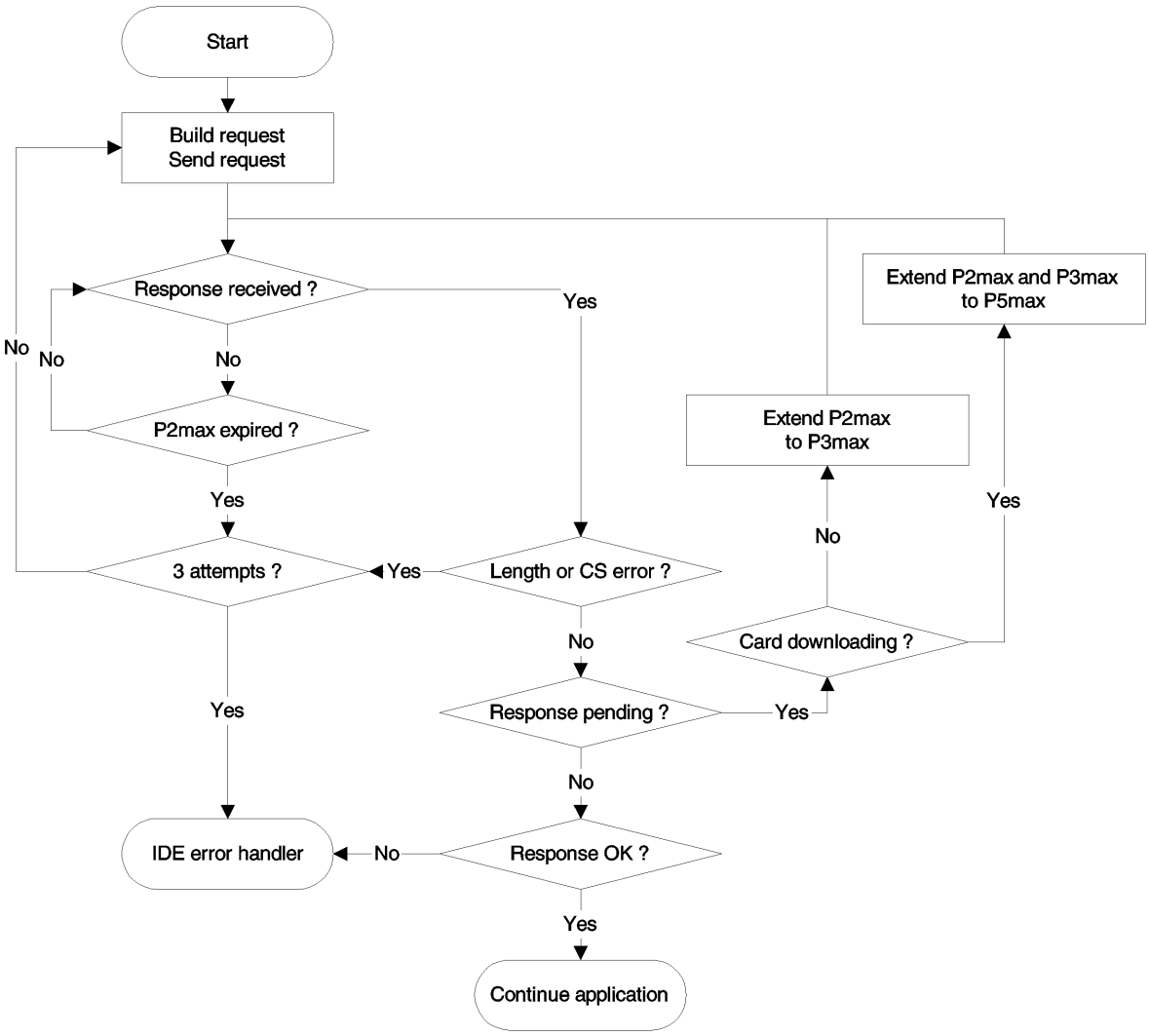
DDP_026 IDE skall upptäcka sekvensfel, exempelvis inkorrekta steg i räknaren av undermeddelanden i mottagna meddelanden som följer på varandra.

DDP_027 Om IDE upptäcker ett fel eller om det inte kom något svar från fordonsenheten inom perioden P2max, skall meddelandet med begäran sändas igen under sammanlagt högst tre överföringar. För att bidra till upptäckt av dessa fel kommer en kvittering av undermeddelanden att betraktas som en begäran till fordonsenheten.

DDP_028 IDE skall vänta åtminstone under en period P3min innan den påbörjar varje överföring. Vänteperioden skall mätas från senast beräknade förekomst av en stopp-bit efter det att felet upptäcktes.

Figur 3

Hantering av IDE-fel



2.2.6 ***Innehåll i Response Message***

I denna punkt specificeras innehållet i datafälten i de olika positiva svarsmeddelandena.

Dataelement definieras i tillägg 1 (Dataordlista).

2.2.6.1 *Positive Response Transfer Data Overview*

DDP_029 Datafältet i meddelandet 'Positive Response Transfer Data Overview' skall tillhandahålla följande data i följande ordning under SID 76 Hex, TREP 01 Hex och passande delning och räkning av undermeddelanden:

Dataelement	Längd (byte)	Kommentar
MemberStateCertificate	194	Fordonsenhets säkerhetscertifikat
VUCertificate	194	
VehicleIdentificationNumber	17	Fordonsidentifiering
VehicleRegistrationIdentification		
vehicleRegistrationNation	1	
vehicleRegistrationNumber	14	
CurrentDateTime	4	Fordonsenhetens aktuella datum och tid
VuDownloadablePeriod		Överföringsbar period
minDownloadableTime	4	
maxDownloadableTime	4	
CardSlotsStatus	1	Typ av kort som satts i fordonsenheten
VuDownloadActivityData		Tidigare överföring från fordonsenhet
downloadingTime	4	
fullCardNumber	18	
companyOrWorkshopName	36	
VuCompanyLocksData		Alla lagrade företagslås. Om sektionen är tom sänds endast noOfLocks = 0.
noOfLocks	1	
...	(98)	
VuCompanyLocksRecord		
lockInTime	4	
lockOutTime	4	
companyName	36	
companyAddress	36	
companyCardNumber	18	
...		
VuControlActivityData		Alla kontrollposter som finns lagrade i fordonsenheten. Om sektionen är tom sänds endast noOfControls = 0.
noOfControls	1	
...	(31)	
VuControlActivityRecord		
controlType	1	
controlTime	4	
controlCardNumber	18	
downloadPeriodBeginTime	4	
downloadPeriodEndTime	4	
...		
Signature	128	RSA-signatur för alla data (utom certifikat) med start från VehicleIdentificationNumber ned till sista byte i sista VuControlActivityRecord.

2.2.6.2 *Positive Response Transfer Data Activities*

DDP_030 Datafältet i meddelandet 'Positive Response Transfer Data Activities' skall tillhandahålla följande data i följande ordning under SID 76 Hex, TREP 02 Hex och passande delning och räkning av undermeddelanden:

Dataelement	Längd (byte)	Kommentar
TimeReal	4	Datum för överförd dag
OdometerValueMidnight	3	Vägmätarställning i slutet av överförd dag
VuCardIWData		Data om cykler med isättning och urtagning av kort. — Om denna sektion inte innehåller några tillgängliga data, sänds endast noOfVuCardIWRecords = 0. — När en VuCardIWRecord sträcker sig över 00.00 (kortisättning dagen innan) eller över 24.00 (korturtagning följande dag) skall den visas fullständigt inom de två berörda dygnen.
noOfVuCardIWRecords	2	
...	(129)	
VuCardIWRecord		
cardHolderName		
holderSurname	36	
holderFirstNames	36	
fullCardNumber	18	
cardExpiryDate	4	
cardInsertionTime	4	
vehicleOdometerValueAtInsertion	3	
cardSlotNumber	1	
cardWithdrawalTime	4	
vehicleOdometerValueAtWithdrawal	3	
previousVehicleInfo		
vehicleRegistrationIdentification		
vehicleRegistrationNation	1	
vehicleRegistrationNumber	14	
cardWithdrawalTime	4	
manualInputFlag	1	
...		
VuActivityDailyData		Öppningsstatus kl 00.00 och aktivitetsändringar som registrerats för den dag som överförts.
noOfActivityChanges	2	
...		
ActivityChangeInfo	2	
...		
VuPlaceDailyWorkPeriodData		Data om platser som registrerats för den dag som överförts. Om sektionen är tom sänds endast noOfPlaceRecords = 0.
noOfPlaceRecords	1	
...	(28)	
VuPlaceDailyWorkPeriodRecord		
fullCardNumber	18	
placeRecord		
entryTime	4	
entryTypeDailyWorkPeriod	1	
dailyWorkPeriodCountry	1	
dailyWorkPeriodRegion	1	
vehicleOdometerValue	3	
...		
VuSpecificConditionData		Data om särskilda omständigheter som registrerats för den dag som överförts. Om avsnittet är tomt sänds endast noOfSpecificConditionRecords = 0.
noOfSpecificConditionRecords	2	
...	(5)	
SpecificConditionRecord		
EntryTime	4	
specificConditionType	1	
...		
Signature	128	RSA-signatur för alla data med början från TimeReal ned till sista byte i sista post för särskild omständighet.

2.2.6.3 *Positive Response Transfer Data Events and Faults*

DDP_031 Datafältet i meddelandet 'Positive Response Transfer Data Events and Faults' skall tillhandahålla följande data i följande ordning under SID 76 Hex, TREP 03 Hex och passande delning och räkning av undermeddelanden:

Dataelement	Längd (byte)	Kommentar
VuFaultData		Alla fel som finns lagrade eller håller på att registreras i fordonsenheten. Om sektionen är tom sänds endast noOfVuFaults = 0.
NoOfVuFaults	1	
...	(82)	
VuFaultRecord: FaultType	1	
VuFaultRecord: FaultRecordPurpose	1	
VuFaultRecord: FaultBeginTime	4	
VuFaultRecord: FaultEndTime	4	
VuFaultRecord: CardNumberDriverSlotBegin	18	
VuFaultRecord: CardNumberCodriverSlotBegin	18	
VuFaultRecord: CardNumberDriverSlotEnd	18	
VuFaultRecord: CardNumberCodriverSlotEnd	18	
...		
VuEventData		Alla händelser (utom hastighetsöverträdelse) som finns lagrade eller håller på att registreras i fordonsenheten. Om sektionen är tom sänds endast noOfVuEvents = 0.
NoOfVuEvents	1	
...	(83)	
VuEventRecord: EventType	1	
VuEventRecord: EventRecordPurpose	1	
VuEventRecord: EventBeginTime	4	
VuEventRecord: EventEndTime	4	
VuEventRecord: CardNumberDriverSlotBegin	18	
VuEventRecord: CardNumberCodriverSlotBegin	18	
VuEventRecord: CardNumberDriverSlotEnd	18	
VuEventRecord: CardNumberCodriverSlotEnd	18	
VuEventRecord: SimilarEventsNumber	1	
...		
VuOverSpeedingControlData		Data om senaste kontroll av hastighetsöverträdelse (förvalt värde om data inte finns).
LastOverspeedControlTime	4	
FirstOverspeedSince	4	
NumberOfOverspeedSince	1	
VuOverSpeedingEventData		Alla händelser av typen hastighetsöverträdelse som finns lagrade i fordonsenheten. Om sektionen är tom sänds endast noOfVuOverSpeedingEvents = 0.
NoOfVuOverSpeedingEvents	1	
...	(31)	
VuOverSpeedingEventRecord: EventType	1	
VuOverSpeedingEventRecord: EventRecordPurpose	1	
VuOverSpeedingEventRecord: EventBeginTime	4	
VuOverSpeedingEventRecord: EventEndTime	4	
VuOverSpeedingEventRecord: MaxSpeedValue	1	
VuOverSpeedingEventRecord: AverageSpeedValue	1	
VuOverSpeedingEventRecord: CardNumberDriverSlotBegin	18	
VuOverSpeedingEventRecord: SimilarEventsNumber	1	
...		
VuTimeAdjustmentData		Alla händelser av typen tidsinställningar som finns lagrade i fordonsenheten (vid annat än fullständig kalibrering). Om sektionen är tom sänds endast noOfVuTimeAdjRecords = 0.
NoOfVuTimeAdjRecords	1	
...	(98)	
VuTimeAdjustmentRecord: OldTimeValue	4	
VuTimeAdjustmentRecord: NewTimeValue	4	
VuTimeAdjustmentRecord: WorkshopName	36	
VuTimeAdjustmentRecord: WorkshopAddress	36	
VuTimeAdjustmentRecord: WorkshopCardNumber	18	
...		
Signature	128	RSA-signatur för alla data med början från noOfVuFaults ned till sista byte i sista post för tidsinställning.

2.2.6.4 *Positive Response Transfer Data Detailed Speed*

DDP_032 'Positive Response Transfer Data Detailed Speed' skall tillhandahålla följande data i följande ordning under SID 76 Hex, TREP 04 Hex och passande delning och räkning av undermeddelanden:

Dataelement	Längd (byte)	Kommentar
VuDetailedSpeedData		
NoOfSpeedBlocks	2	All detaljerad hastighet som finns lagrad i fordonsenheten (ett hastighetsblock per minut då fordonet har varit i rörelse) 60 hastighetsvärden per minut (ett per sekund).
...		
VuDeatailedSpeedBlock		
SpeedBlockBeginDate	4	
speedsPerSecond	60	
...		
Signature	128	RSA-signatur för alla data med början från noOfSpeedBlocks ned till sista byte i sista hastighetsblocket.

2.2.6.5 *Positive Response Transfer Data Technical Data*

DDP_033 Datafältet i meddelandet 'Positive Response Transfer Data Technical Data' skall tillhandahålla följande data i följande ordning under SID 76 Hex, TREP 05 Hex och passande delning och räkning av undermeddelanden:

Dataelement	Längd (byte)	Kommentar
VuIdentification		
vuManufacturerName	36	
vuManufacturerAddress	36	
vuPartNumber	16	
vuSerialNumber	8	
vuSoftwareIdentification		
vuSoftwareVersion	4	
vuSoftInstallationDate	4	
vuManufacturingDate	4	
vuApprovalNumber	8	
SensorPaired		
sensorSerialNumber	8	
sensorApprovalNumber	8	
sensorPairingDateFirst	4	
VuCalibrationData		Alla kalibreringsposter som finns lagrade i fordonsenheten.
noOfVuCalibrationRecords	1	
...	(164)	
VuCalibrationRecord		
calibrationPurpose	1	
workshopName	36	
workshopAddress	36	
workshopCardNumber	18	
workshopCardExpiryDate	4	
vehicleIdentificationNumber	17	
vehicleRegistrationIdentification		
vehicleRegistrationNation	1	
vehicleRegistrationNumber	14	
wVehicleCharacteristicConstant	2	
kConstantOfRecordingEquipment	2	
lTyreCircumference	2	
tyreSize	15	
authorisedSpeed	1	
oldOdometerValue	3	
newOdometerValue	3	
oldTimeValue	4	
newTimeValue	4	
nextCalibrationDate	4	
...		
Signature	128	RSA-signatur för alla data med början från vuManufacturerName ned till sista byte i sista VuCalibrationRecord.

2.3 **Fillagring på Externa lagringsmedia**

DDP_034 När en överföringssession har inbegripit överföring av fordonsenhetsdata, skall IDE i en fysisk fil lagra alla de data som mottagits från fordonsenheten under överföringssessionen inom meddelandena 'Positive Response Transfer Data'. Lagrade data inbegriper ej meddelandehuvuden, 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 **Räckvidd**

I denna punkt beskrivs direkt överföring av kortdata från ett färdskrivarkort till IDE. IDE är inte en del av den säkra miljön. Följaktligen utförs ingen autentisering mellan kort och IDE.

3.2 **Definitioner**

Överföringssession: Varje gång en överföring av ICC-data (data på IC-kort) utförs. Sessionen omfattar ett fullständigt förfarande från återställning av IC-kortet av en IFD (kortläsare) till avaktivering av ICC (urtagning av kort eller nästa återställning).

Signerad datafil: En fil från IC-kortet. Filen överförs till kortläsaren i klartext. På IC-kortet hashas och signeras filen och signaturen överförs till kortläsaren.

3.3 **Överföring från kort**

DDP_035 Överföring från ett färdskrivarkort inbegriper följande steg:

— Överför basinformationen på kortet i datafilens `ICC` och `IC`. Denna information är valbar och säkras inte med en digital signatur.

— Överför datafilens `Card_Certificate` och `CA_Certificate`. Denna information säkras inte med en digital signatur.

Överföring av dessa filer vid varje överföringssession är obligatorisk.

— Överför övriga datafiler för tillämpningsdata (inom `Tachograph` DF), med undantag av datafilen `Card_Download`. Denna information säkras med en digital signatur.

  — Överföring av åtminstone datafilernas `Application_Identification` och `ID` vid varje överföringssession.

  — Vid överföring av förarkort är överföring av följande datafiler också obligatorisk:

    — `Events_Data` (händelsedata).

    — `Faults_Data` (feldata).

    — `Driver_Activity_Data` (data om föraraktiviteter).

    — `Vehicles_Used` (använda fordon).

    — `Places` (platser).

    — `Control_Activity_Data` (data om kontrollaktiviteter).

    — `Specific_Conditions` (särskilda omständigheter).

— Vid överföring av förarkort, uppdatera datumet för `LastCard_Download` i datafilen `Card_Download` (kortöverföring).

— Vid överföring från ett verkstadskort, återställ kalibreringsräknaren i datafilen `Card_Download` (kortöverföring).

3.3.1 ***Initieringssekvens***

DDP_036 IDE skall initiera sekvensen enligt följande:

Kort	Riktning	IDE/IFD	Betydelse/anmärkningar
	⇦	Maskinvaruåterställning	
ATR	⇨		

Man kan använda PPS (val av protokollparametrar) för att byta till en högre baud-nivå så länge IC-kortet stödjer det.

3.3.2 ***Sekvens för osignerade datafiler***

DDP_037 Sekvens för överföring av datafilernas `ICC`, `IC`, `Card_Certificate` och `CA_Certificate` är följande:

Kort	Riktning	IDE/IFD	Betydelse/anmärkningar
	⇦	Välj fil	Välj med hjälp av filidentifierare
OK	⇨		
	⇦	Read Binary (Läs binär)	Om filen innehåller mer data än buffertstorleken hos läsaren eller kortet måste kommandot upprepas tills den fulllständiga filen har lästs
Fildata OK	⇨	Lagra data till ESM	Enligt punkt 3.4. Format för lagring av data

Obs: Innan datafilen `Card_Certificate` väljs, måste färdskrivartillämpning väljas (val genom AID (tillämpningsidentifierare))

3.3.3 ***Sekvens för signerade datafiler***

DDP_038 Följande sekvens skall användas för var och en av följande filer som måste överföras med sin signatur.

Kort	Riktning	IDE/IFD	Betydelse/anmärkningar
	⇦	Select File (välj fil)	
OK	⇨		
	⇦	Perform Hash of File (hasha filen)	Beräknar hashvärdet över datainnehållet i vald fil med hjälp av föreskriven hash-algoritm enligt tillägg 11. Detta kommando är inte ett ISO-kommando.
Calculate Hash of File and store Hash value temporarily (Beräkna filens hashvärde och lagra hashvärdet tillfälligt)			
OK	⇨		
	⇦	Read Binary (Läs binär)	Om filen innehåller mer data än bufferten hos läsaren eller kortet måste kommandot upprepas tills den fulllständiga filen har lästs.
Fildata OK	⇨	Lagra mottagna data till ESM	Enligt punkt 3.4. Format för lagring av datat
	⇦	PSO: Compute Digital Signature (beräkna digital signatur)	
Perform Security Operation (utför säkerhetsoperation) 'Compute Digital Signature' med hjälp av det tillfälligt lagrade hash-värdet			
Signature (signatur) OK	⇨	Foga data till tidigare lagrade data i ESM	Enligt punkt 3.4. Format för lagring av data

3.3.4 ***Sekvens för återställning av kalibreringsräknare***

DDP_039 Sekvensen för återställning av räknaren av `NoOfCalibrationsSinceDownload` i datafilen `Card_Download` på ett verkstadskort är följande:

Kort	Riktning	IDE/IFD	Betydelse/anmärkningar
OK	⇦ ⇨	Select File (välj datafil) `Card_Download`	Välj med hjälp av filidentifierare
	⇦	Update Binary (uppdatera binär) `NoOfCalibrationsSinceDownload` = '00 00'	
återställer kortöverföringsnummer			
OK	⇨		

3.4 **Format för lagring av data**

3.4.1 ***Inledning***

DDP_040 Överförda data måste lagras enligt följande villkor:

— Data skall lagras transparent. Detta innebär att byte-ordningen och bit-ordningen inuti de byte som överförs från kortet måste bevaras vid lagring.

— Alla de filer på ett kort som överförs vid en överföringssession lagras i en fil i ESM.

3.4.2 ***Filformat***

DDP_041 Filformatet är en sammansättning av flera TLV-objekt.

DDP_042 Taggen för en datafil skall vara FID (filidentifierare) plus tillägget '00'.

DDP_043 Taggen för en datafils signatur skall vara FID (filidentifierare) av filen plus tillägget '01'.

DDP_044 Längden är ett värde på två byte. Värdet definierar antalet byte i värdefältet. Värdet i längdfältet är reserverat för framtida användning.

DDP_045 Om en fil inte överförs skall inte något som förknippas med filen lagras (ingen tagg och ingen noll-längd).

DDP_046 En signatur skall 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 data i en överföringsfil i ett ESM:

Tagg	Längd	Värde
00 02 00	00 11	Data i EF `ICC`
C1 00 00	00 C2	Data i EF `Card_Certificate`
		…
05 05 00	0A 2E	Data i EF `Vehicles_Used`
05 05 01	00 80	Signatur för EF `Vehicles_Used`

4. ÖVERFÖRING FRÅN ETT FÄRDSKRIVARKORT VIA EN FORDONSENHET

DDP_047 Fordonsenheten måste möjliggöra överföring från ett förarkort som är isatt i en ansluten IDE.

DDP_048 IDE skall sända meddelandet 'Transfer Data Request Card Download' till fordonsenheten för att initiera detta läge (se 2.2.2.9).

DDP_049 Fordonsenheten skall sedan överföra hela kortet, fil efter fil, enligt det protokoll för kortöverföring som definieras i punkt 3, och vidaresända alla data som mottagits från kortet till IDE i lämpligt TIL-filformat (se punkt 3.4.2) och som inkapslats i meddelandet 'Positive Response Transfer Data'.

DDP_050 IDE skall hämta kortdata från meddelandet 'Positive Response Transfer Data' (och stryka alla huvuden, SID, TREP, undermeddelanderäknare och kontrollsummor) och lagra dem i en fysisk fil i enlighet med punkt 2.3.

DDP_051 Fordonsenheten skall därefter i förekommande fall uppdatera förarkortets datafil med kontrollaktiviteter `ControlActivityData` eller datafil med överföring av kort `Card_Download`.

Tillägg 8

KALIBRERINGSPROTOKOLL

INNEHÅLL

1. INLEDNING

I detta tillägg beskrivs hur data utbyts mellan en fordonsenhet och en provare (tester) via K-linjen (K-line), som utgör en del av det gränssnitt för kalibrering som beskrivs i tillägg 6. Dessutom beskrivs kontroll av linjen för ingående/utgående signal på kalibreringsanslutningen.

Upprättande av K-linjekommunikationer beskrivs i avsnitt 4 'Kommunikationstjänster'.

I denna bilaga används begreppet diagnossessioner (diagnostic sessions) för att avgöra räckvidden för K-linjekontroll under olika omständigheter. Den förvalda sessionen är 'StandardDiagnosticSession', där alla data kan läsas från en fordonsenhet men inga data kan skrivas till en fordonsenhet.

Val av diagnossession beskrivs i avsnitt 5 'Förvaltningstjänster'.

CPR_001 'ECUProgrammingSession' möjliggör ingång av data i fordonsenheten. När det gäller ingång av kalibreringsdata (krav 097 och 098), måste fordonsenheten dessutom vara i driftläge CALIBRATION (kalibrering).

Dataöverföring via K-linjen beskrivs i avsnitt 6 'Dataöverföringstjänster'. Formaten för data som överförs beskrivs närmare i avsnitt 8 'Format för dataRecords'.

CPR_002 'ECUAdjustmentSession' möjliggör val av in-/utläge på in-/ut- signallinjen (för kalibrering) via K-linjegränssnittet. Kontroll av in-/ut- signallinjen (för kalibrering) beskrivs i avsnitt 7 'Kontroll av provpulser – Funktionsenhet för kontroll av in-/utdata'.

CPR_003 I hela detta dokument betecknas provarens adress med 'tt'. Även om det kan finnas adresser som föredras för provare skall fordonsenheten svara korrekt på alla provaradresser. Fordonsenhetens fysiska adress är 0xEE.

2. TERMER, DEFINITIONER OCH REFERENSER

Protokollen, meddelandena och felkoderna bygger huvudsakligen på den aktuella versionen av ISO 14229-1 (Vägfordon – Diagnostiksystem – Del 1: Diagnostiktjänster, version 6 av den 22 februari 2001).

Lokala identifierare och dataformat definieras i ISO 16844-7.

Byte-kodning och hexadecimala värden används för identifierare av tjänster, begäran om tjänster och svar samt standardparametrar.

Termen 'provare' (tester) avser den utrustning som används för att mata in programmerings-/kalibreringsdata i fordonsenheten.

Termerna 'klient' (client) och 'server' (server) avser provare respektive fordonsenhet.

Termen ECU betyder 'Electronic Control Unit' (eletronisk styrenhet) och avser fordonsenheten.

Referenser:

ISO 14230-2: Vägfordon – Keyword Protocol 2000 för diagnostiksystem – Del 2: Länkskikt. Första utgåvan: 1999. Fordon – Diagnostiksystem.

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 inbegriper avsnittets nummer i detta tillägg där tjänsten definieras närmare.

— I den tredje kolumnen tilldelas tjänsteidentifierarnas värden för meddelanden med begäran.

— I den fjärde kolumnen specificeras de tjänster i 'StandardDiagnosticSession' (SD) som måste användas i varje fordonsenhet.

— I den femte kolumnen specificeras de tjänster i 'ECUAdjustmentSession' (ECUAS) (inställningssessionen) som måste användas för att möjliggöra kontroll av in-/ut- signallinjen i kalibreringsanslutningen på frontpanelen i fordonsenheten.

— I den sjätte kolumnen specificeras de tjänster i 'ECUProgrammingSession' (ECUPS) (programmeringssessionen) som måste användas för att det skall vara möjligt att programmera parametrar i fordonsenheten.

Tabell 1

Sammanfattande tabell över värden på tjänsteidentifierare

			Diagnossessioner		
Namn på diagnostjänst	Avsnitt nr	Tjänste-ID erforderligt värde	SD	ECUAS	ECUPS
StartCommunication	4.1	81	■	■	■
StopCommunication	4.2	82	■		
Testerpresent	4.3	3E	■	■	■
StartDiagnosticSession	5.1	10	■	■	■
SecurityAccess	5.2	27	■	■	■
ReadDataByIdentifier	6.1	22	■	■	■
WriteDataByIdentifier	6.2	2E			■
InputOutputControlByIdentifier	7.1	2F		■	

■ Denna symbol anger att tjänsten är obligatorisk under denna diagnossession.
Ingen symbol anger att denna tjänst inte är tillåten under denna diagnossession.

3.2 **Svarskoder**

Svarskoder (response codes) definieras för varje tjänst.

4. KOMMUNIKATIONSTJÄNSTER

Vissa tjänster behövs för att kommunikation skall kunna upprättas och upprätthållas. De finns inte på tillämpningsskiktet. Tillgängliga tjänster specificeras i nedanstående tabell.

Tabell 2

Kommunikationstjänster

Namn på tjänst	Beskrivning
StartCommunication	Klienten begär att få starta en kommunikationssession med en eller flera servrar
StopCommunication	Klienten begär att få avsluta pågående kommunikationssession
TesterPresent	Klienten meddelar servern att förbindelsen fortfarande är aktiv

CPR_005 Tjänsten StartCommunication används för att starta en kommunikation. För att man skall kunna utföra en tjänst måste kommunikationen initieras och kommunikationsparametrarna bör vara lämpliga för önskat läge (mode).

4.1 **Tjänsten StartCommunication (starta kommunikation)**

CPR_006 Vid mottagande av indikationsprimitiven StartCommunication skall fordonsenheten kontrollera om den begärda kommunikationslänken kan initieras under innevarande omständigheter. Giltiga omständigheter för initiering av en kommunikationslänk beskrivs i dokument ISO 14230-2.

CPR_007 Fordonsenheten skall därefter utföra alla de funktioner som krävs för att initiera kommunikationslänken och sända svarsprimitiven StartCommunication med de Positive Response parameters (positivt svar-parametrar) 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 starta kommunikation) (exempelvis på grund av felåterhämtning i provaren) skall begäran godtas och fordonsenheten skall återinitieras.

CPR_009 Om kommunikationslänken av någon anledning inte kan initieras, skall fordonsenheten fortsätta att fungera på samma sätt som den gjorde omedelbart före försöket att initiera kommunikationslänken.

CPR_010 Meddelandet med StartCommunication Request måste vara fysiskt adresserad.

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 tabell 5 enligt nyckel-byte (key bytes).

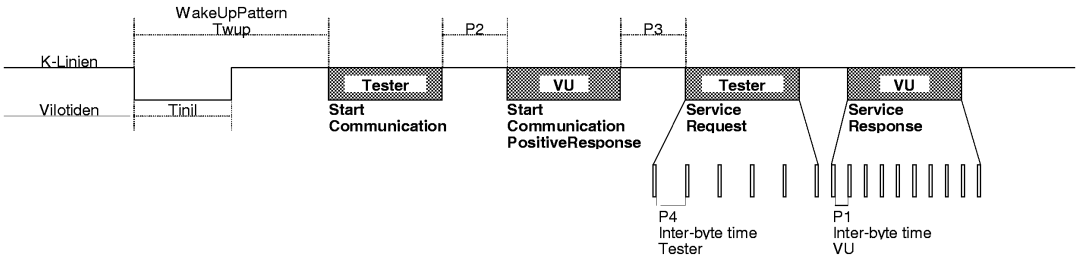
— Fordonsenheten väntar på provarens första begäran.

— Fordonsenheten är i förvalt diagnosläge, dvs. StandardDiagnosticSession.

— In-/ut- signallinjen (för kalibrering) är i förvalt läge, dvs. avaktiverat läge.

CPR_014 Dataöverföringshastigheten på K-linjen skall vara 10 400 baud.

CPR_016 Den snabba initieringen påbörjas av provaren, som överför ett Wake up-mönster (Wup) på K-linjen. Mönstret börjar efter vilotiden på K-linjen med en Tinil-lågtid (low time of Tinil). Provaren överför första bit i tjänsten StartCommunication efter en tid av Twup som följer på första fallande kant.



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, Tidle = 300 ms.

— Efter slutförande av en StopCommunication-tjänst, Tidle = P3 min.

— Efter det att kommunikationen avslutats genom time-out P3 max, Tidle = 0.

Tabell 3

Tidsvärden för snabb initiering

Parameter		lägsta värde	högsta värde
Tinil	25 ± 1 ms	24 ms	26 ms
Twup	50 ± 1 ms	49 ms	51 ms

Tabell 4

Tidsvärden vid kommunikation

Tids-Parameter	Parameterbeskrivning	Nedre gränsvärden (ms)	Övre gränsvärden (ms)
		Min	Max
P1	Inter byte-tid (inter byte time) för fordonsenhetens svar	0	20
P2	Tid mellan provarens begäran och fordonsenhetens svar eller två fordonsenhetssvar	25	250
P3	Tid mellan slut på fordonsenhets svar och start på ny begäran från provare	55	5000
P4	Inter byte-tid för provarens begäran	5	20

CPR_018 Meddelandeformat för snabb initiering anges i detalj i nedanstående tabeller.

Tabell 5

StartCommunication Request Message (meddelande med begäran om att starta kommunikation)

Byte #	Parameternamn	Hexvärde	Memo
#1	Format byte – physical addressing (format-byte – fysisk adressering)	81	FMT
#2	Target address byte (måladress-byte)	EE	TGT
#3	Source address byte (källadress-byte)	tt	SRC
#4	StartCommunication Request Service Id (starta kommunikation begäran tjänste-ID)	81	SCR
#5	Checksum (kontrollsumma)	00-FF	CS

Tabell 6

StartCommunication Positive Request Message (positivt svar på meddelande med begäran om att starta kommunikation)

Byte #	Parameternamn	Hexvärde	Memo
#1	Format byte – physical addressing (format-byte – fysisk adressering)	80	FMT
#2	Target address byte (måladress-byte)	tt	TGT
#3	Source address byte (källadress-byte)	EE	SRC
#4	Additional length byte (extra längd-byte)	03	LEN
#5	StartCommunication Positive Response Service Id (starta kommunikation positivt svar tjänste-ID)	C1	SCRPR
#6	Key byte 1 (nyckel-byte 1)	EA	KB1
#7	Key byte 2 (nyckel-byte 2)	8F	KB2
#8	Checksum (kontrollsumma)	00-FF	CS

CPR_019 Det finns inget negativt svar på meddelandet med StartCommunication Request, 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 (avsluta kommunikation)**

4.2.1 ***Meddelandebeskrivning***

Syftet med denna kommunikationsskiktstjänst är att avsluta en kommunikationssession.

CPR_020 När fordonsenheten tar emot indikationsprimitiven StopCommunication (avsluta kommunikation), skall den kontrollera om aktuella omständigheter tillåter att denna kommunikation avslutas. I detta fall skall fordonsenheten utföra alla de funktioner som behövs för att avsluta denna kommunikation.

CPR_021 Om det är möjligt att avsluta kommunikationen, skall fordonsenheten utfärda en StopCommunication svarsprimitiv med valda Positive response-parametrar (positivt svar-parametrar), innan kommunikationen avslutas.

CPR_022 Om kommunikationen inte kan avslutas av någon anledning, skall fordonsenheten utfärda en StopCommunication svarsprimitiv med vald Negative Response-parameter (negativt svar-parameter).

CPR_023 Om time-out av P3max upptäcks av fordonsenheten, skall kommunikationen avslutas utan att någon svarsprimitiv utfärdas.

4.2.2 ***Meddelandeformat***

CPR_024 Meddelandeformat för StopCommunication-primitiver anges i detalj i nedanstående tabeller.

Tabell 7

StopCommunication Request Message (meddelande med begäran om avsluta kommunikation)

Byte #	Parameternamn	Hexvärde	Memo
#1	Format byte – physical addressing (format-byte – fysisk adressering)	80	FMT
#2	Target address byte(måladress-byte)	EE	TGT
#3	Source address byte (källadress-byte)	tt	SRC
#4	Additional length byte (extra längd-byte)	01	LEN
#5	StopCommunication Request Service Id (avsluta kommunikation begäran tjänste-ID)	82	SPR
#6	Checksum (kontrollsumma)	00-FF	CS

Tabell 8

StopCommunication Positive Response Message (avsluta kommunikation positivt svarsmeddelande)

Byte #	Parameternamn	Hexvärde	Memo
#1	Format byte – physical addressing (format-byte – fysisk adressering)	80	FMT
#2	Target address byte (måladress-byte)	tt	TGT
#3	Source address byte (källadress-byte)	EE	SRC
#4	Additional length byte (extra längd-byte)	01	LEN
#5	StopCommunication Positive Response Service Id (avsluta kommunikation positivt svar tjänste-ID)	C2	SPRPR
#6	Checksum (kontrollsumma)	00-FF	CS

Tabell 9

StopCommunication Negative Response Message (avsluta kommunikation negativt svarsmeddelande)

Byte #	Parameternamn	Hexvärde	Memo
#1	Format byte – physical addressing (format-byte – fysisk adressering)	80	FMT
#2	Target address byte (måladress-byte)	tt	TGT
#3	Source address byte (källadress-byte)	EE	SRC
#4	Additional length byte (extra längd-byte)	03	LEN
#5	negative Response Service Id (negativt svar tjänste-ID)	7F	NR
#6	StopCommunication Request Service Identification (avsluta kommunikation begäran tjänste-ID)	82	SPR
#7	ResponseCode = generalReject (svarskod = allmänt avslag)	10	RC_GR
#8	Checksum (kontrollsumma)	00-FF	CS

4.2.3 ***Definition av parametrar***

Denna tjänst förutsätter inte någon definition av parametrar.

4.3 **Tjänsten TesterPresent**

4.3.1 ***Meddelandebeskrivning***

Tjänsten TesterPresent används av provaren ('tester') för att meddela servern att den fortfarande är aktiv i förbindelsen. Syftet är att hindra servern från att automatiskt återgå till normalt driftsläge 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 Meddelandeformaten före TesterPresent-primitiverna anges i detalj i nedanstående tabeller.

Tabell 10

TesterPresent Request Message

Byte #	Parameternamn	Hexvärde	Memo
#1	Format byte – physical addressing (format-byte – fysisk adressering)	80	FMT
#2	Target address byte (måladress-byte)	EE	TGT
#3	Source address byte (källadress-byte)	tt	SRC
#4	Additional length byte (extra längd-byte)	02	LEN
#5	TesterPresent Request Service Id	3E	TP
#6	Sub Function = responseRequired = [yes	01	RESPREQ_Y
	no]	02	RESPREQ_NO
#7	Checksum (kontrollsumma)	00-FF	CS

CPR_080 Om parametern responseRequired sätts till 'yes' skall servern svara med följande positiva svarsmeddelande. Om parametern sätts till 'no' skall inget svar skickas av servern.

Tabell 11

TesterPresent Positive Response Message

Byte #	Parameternamn	Hexvärde	Memo
#1	Format byte – physical addressing	80	FMT
#2	Target address byte	tt	TGT
#3	Source address byte	EE	SRC
#4	Additional length byte	01	LEN
#5	TesterPresent Positive Response Service Id	7E	TPPR
#6	Checksum	00-FF	CS

CPR_081 Tjänsten skall använda följande negativa svarskoder:

Tabell 12

TesterPresent Negative Response Message

Byte #	Parameternamn	Hexvärde	Memo
#1	Format byte – physical addressing	80	FMT
#2	Target address byte	tt	TGT
#3	Source address byte	EE	SRC
#4	Additional length byte	03	LEN
#5	Negative Response Service Id	7F	NR
#6	TesterPresent Request Service Identification	3E	TP
#7	ResponseCode = [SubFunctionNotSupported-InvalidFormat	12	RC_SFNS_IF
	incorrectMessageLength]	13	RC_IML
#8	Checksum	00-FF	CS

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(starta diagnossession)**

5.1.1 ***Meddelandebeskrivning***

CPR_025 Tjänsten StartDiagnosticSession används för att möjliggöra olika diagnossessioner i servern. En diagnossession möjliggör en specifik mängd tjänster enligt tabell 17. En session kan aktivera tjänster som är specifika för vissa fordonstillverkare och som inte beskrivs i detta dokument. Användningsreglerna skall överensstämma med följande krav:

— Det skall alltid vara exakt en diagnossession aktiv i fordonsenheten.

— När fordonsenheten kopplas in skall den alltid starta StandardDiagnosticSession. Om ingen annan diagnossession startas, skall StandardDiagnosticSession vara aktiv så länge fordonsheten får ström.

— Om en diagnossession som redan är aktiv har begärts av provaren ('tester'), skall fordonsenheten skicka ett positivt svarsmeddelande.

— Varje gång provaren ('tester') begär en ny diagnossession, skall fordonsenheten först skicka et positivt svarsmeddelande för StartDiagnosticSession innan den nya sessionen blir aktiv i fordonsenheten. Om fordonsenheten inte kan starta den begärda nya diagnossessionen, skall den svara med ett negativt svarsmeddelande för StartDiagnosticSession, och den session som redan är aktiv skall fortsätta.

CPR_026 En diagnossession skall startas endast om kommunikation har upprättats mellan klient och fordonsenhet.

CPR_027 De tidsparametrar som definieras i tabell 5 skall 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 StartDiagnosticSession-primitiver anges i detalj i nedanstående tabeller.

Tabell 14

StartDiagnosticSession Request Message (meddelande med begäran om start av diagnossession)

Byte #	Parameternamn	Hexvärde	Memo
#1	Format byte – physical addressing (format-byte – fysisk adressering)	80	FMT
#2	Target address byte(måladress-byte)	EE	TGT
#3	Source address byte (källadress-byte)	tt	SRC
#4	Additional length byte (extra längd-byte)	02	LEN
#5	StartDiagnosticSession Request Service Id (starta diagnossession begäran tjänste-ID)	10	STDS
#6	diagnosticSession = [ett värde från tabell 17]	xx	DS_…
#7	Checksum (kontrollsumma)	00-FF	CS

Tabell 15

StartDiagnosticSession Positive Response Message(starta diagnossession positivt svarsmeddelande)

Byte #	Parameternamn	Hexvärde	Memo
#1	Format byte – physical addressing (format-byte – fysisk adressering)	80	FMT
#2	Target address byte (måladress-byte)	tt	TGT
#3	Source address byte (källadress-byte)	EE	SRC
#4	Additional length byte (extra längd-byte)	02	LEN
#5	StartDiagnosticSession Positive Response Service Id (starta diagnossession positivt svar tjänste-ID)	50	STDSPR
#6	DiagnosticSession = [samma värde som i byte #6 tabell 14]	xx	DS_…
#7	Checksum (kontrollsumma)	00-FF	CS

Tabell 16

StartDiagnosticSession Negative Response Message (starta diagnossession negativt svarsmeddelande)

Byte #	Parameternamn	Hexvärde	Memo
#1	Format byte – physical addressing (format-byte – fysisk adressering)	80	FMT
#2	Target address byte (måladress-byte)	tt	TGT
#3	Source address byte (källadress-byte)	EE	SRC
#4	Additional length byte (extra längd-byte)	03	LEN
#5	Negative Response Service Id (negativt svar tjänste-ID)	7F	NR
#6	StartDiagnosticSession Request Service Id (starta diagnossession begäran tjänste-ID)	10	STDS
#7	ResponseCode = [subFunctionNotSupported ([a])	12	RC_SFNS
	IncorrectMessageLength ([b])	13	RC_IML
	conditionsNotCorrect ([c])]	22	RC_CNC
#8	Checksum(kontrollsumma)	00-FF	CS

([a]) Det värde som är inlagt i byte #6 i meddelande med begäran stöds inte, dvs. inte i tabell 17.
([b]) Felaktig meddelandelängd.
([c]) Kriterierna för begäran StartDiagnosticSession uppfylls inte.

5.1.3 ***Definition av parametrar***

CPR_029 Parametern diagnosticSession (DS_) används av tjänsten StartDiagnosticSession för att välja serverns/servrarnas specifika uppförande. Följande diagnossessioner specificeras i detta dokument:

Tabell 17

Definition av diagnosticSession-värden

Hex	Beskrivning	Memo
81	StandardDiagnosticSession Denna diagnossession möjliggör alla tjänster som specificeras i Tabell 1 – Sammanfattande tabell över värden på tjänsteidentifierare. Dessa tjänster möjliggör läsning 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 möjliggör alla tjänster som specificeras i Tabell 1 – Sammanfattande tabell över värden på tjänsteidentifierare. Dessa tjänster stödjer minnesprogrammeringen av en server (fordonsenhet). Denna diagnossession får skrivas över av andra diagnossessioner som specificeras i detta avsnitt.	ECUPS
87	ECUAdjustmentSession Denna diagnossession möjliggör alla tjänster som specificeras i Tabell 1 – Sammanfattande tabell över värden på tjänsteidentifierare. Dessa tjänster stödjer en servers (fordonsenhets) kontroll av indata/utdata. Denna diagnossession får skrivas över av andra diagnossessioner som specificeras i detta avsnitt.	ECUAS

5.2 **Tjänsten SecurityAccess (säkerhetstillträde)**

Skrivning av kalibreringsdata eller tillträde till indata-/utdata-linjen för kalibrering är bara möjlig om fordonsenheten är i CALIBRATION-läge. Utöver att sätta i ett giltigt provningskort i fordonsenheten, måste rätt PIN-kod anges för fordonsenheten innan tillträde till CALIBRATION-läge beviljas.

Tjänsten SecurityAccess ger möjlighet att slå in PIN-koden och för provaren ange om fordonsenheten är i CALIBRATION-läge.

Det är godtagbart att PIN-koden anges med alternativa metoder.

5.2.1 ***Meddelandebeskrivning***

Tjänsten SecurityAccess består av ett SecurityAccess-meddelande ('requestSeed'), eventuellt följt av ett SecurityAccess-meddelande ('sendKey') Tjänsten SecurityAccess måste utföras efter tjänsten StartDiagnosticSession.

CPR_033 Provaren skall använda SecurityAccess-meddelandet ('requestSeed') för att kontrollera om fordonsenheten är beredd att godta en PIN-kod.

CPR_034 Om fordonsenheten redan är i CALIBRATION-läge skall den svara på begäran genom att sända ett startvärde (seed) av 0x0000 med hjälp av tjänsten SecurityAccess Positive Response (begäran om säkerhetstillträde positivt svar).

CPR_035 Om fordonsenheten är beredd att godta en PIN-kod för verifiering med ett provningskort, skall 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 isatta provningskortet inte är giltigt, att inget provningskort har satts i, eller att fordonsenheten förväntar sig PIN-koden från en annan metod, skall den svara på begäran med ett Negative Response (negativt svar) med en svarskod satt till conditionsNotCorrectOrRequestSequenceError.

CPR_037 Provaren skall då slutligen använda SecurityAccess-meddelandet ('sendKey') för att vidaresända en PIN-kod till fordonsenheten. För att ge kortautentiseringen den tid som krävs, skall fordonsenheten använda den negativa svarskoden requestCorrectlyReceived-ResponsePending för att utöka svarstiden. Maximal svarstid skall dock inte överstiga 5 minuter. Så snart den begärda tjänsten har slutförts, skall fordonsenheten skicka ett positivt eller negativt svarsmeddelande med en svarskod som skiljer sig från denna. Den negativa svarskoden requestCorrectlyReceived-ResponsePending får upprepas av fordonsenheten till dess att den begärda tjänsten har slutförts.

CPR_038 Fordonsenheten skall svara på denna begäran genom att använda tjänsten SecurityAccess Positive Response endast när den är i CALIBRATION-läge.

CPR_039 I nedanstående fall skall 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 redo att godta en angivelse av PIN-kod.

— invalidKey: PIN-koden är inte giltig och antal PIN-kontrollförsök har inte överstigits.

— exceededNumberOfAttempts: PIN-koden är inte giltig och antal PIN-kontrollförsök har överstigits.

— generalReject: Riktig PIN-kod men den ömsesidiga autentiseringen med provningskortet misslyckades.

5.2.2 ***Meddelandeformat – SecurityAccess – requestSeed***

CPR_040 Meddelandeformat för SecurityAccess 'requestSeed'-primitiver anges i detalj i nedanstående tabeller.

Tabell 18

SecurityAccess Request - requestSeed (meddelande med begäran om säkerhetstillträde)

Byte #	Parameternamn	Hexvärde	Memo
#1	Format byte – physical addressing (format-byte – fysisk adressering)	80	FMT
#2	Target address byte (måladress-byte)	EE	TGT
#3	Source address byte (källadress-byte)	tt	SRC
#4	Additional length byte(extra längd-byte)	02	LEN
#5	SecurityAccess Request Service Id (säkerhetstillträde begäran tjänste-ID)	27	SA
#6	AccessType – requestSeed (tillträdestyp – begär startvärde)	7D	AT_RSD
#7	Checksum (kontrollsumma)	00-FF	CS

Tabell 19

SecurityAccess - requestSeed Positive Response Message (begäran om säkerhetstillträde positivt svarsmeddelande)

Byte #	Parameternamn	Hexvärde	Memo
#1	Format byte – physical addressing (format-byte – fysisk adressering)	80	FMT
#2	Target address byte (måladress-byte)	tt	TGT
#3	Source address byte (källadress-byte)	EE	SRC
#4	Additional length byte (extra längd-byte)	04	LEN
#5	SecurityAccess Positive Respons Service Id (säkerhetstillträde begäran positivt svar tjänste-ID)	67	SAPR
#6	accessType – requestSeed (tillträdestyp – begär startvärde)	7D	AT_RSD
#7	Seed High (högt startvärde)	00-FF	SEEDH
#8	Seed Low (lågt startvärde)	00-FF	SEEDL
#9	Checksum (kontrollsumma)	00-FF	CS

Tabell 20

SecurityAccess Negative Response Message (begäran om säkerhetstillträde negativt svarsmeddelande)

Byte #	Parameternamn	Hexvärde	Memo
#1	Format byte – physical addressing (format-byte – fysisk adressering)	80	FMT
#2	Target address byte (måladress-byte)	tt	TGT
#3	Source address byte (källadress-byte)	EE	SRC
#4	Additional length byte (extra längd-byte)	03	LEN
#5	NegativeResponse Service Id (negativt svar tjänste-ID)	7F	NR
#6	SecurityAccess Request Service Id (säkerhetstillträde begäran tjänste-ID)	27	SA
#7	ResponseCode = [conditionsNotCorrectOrRequestSequenceError	22	RC_CNC
	incorrectMessageLength]	13	RC_IML
#8	Checksum (kontrollsumma)	00-FF	CS

5.2.3 ***Meddelandeformat – SecurityAccess – sendKey***

CPR_041 Meddelandeformat för SecurityAccessRequest 'sendKey'-primitiver anges i detalj i nedanstående tabeller.

Tabell 21

SecurityAccess Request sendKey (meddelande med begäran om säkerhetstillträde)

Byte #	Parameternamn	Hexvärde	Memo
#1	Format byte – physical addressing (format-byte – fysisk adressering)	80	FMT
#2	Target address byte (måladress-byte)	EE	TGT
#3	Source address byte (källadress-byte)	tt	SRC
#4	Additional length byte (extra längd-byte)	m+2	LEN
#5	SecurityAccess Request Service Id (säkerhetstillträde begäran tjänste-ID)	27	SA
#6	AccessType – sendKey (tillträdestyp – sänd nyckel)	7E	AT_SK
#7 till #m+6	Key #1 (hög)	xx	KEY
	…	…	
	Key #m (låg, m måste vara minst 4, och högst 8)	xx	
#m+7	Checksum (kontrollsumma)	00-FF	CS

Tabell 22

SecurityAccess - sendKey Positive Response Message (begäran om säkerhetstillträde positivt svarsmeddelande)

Byte #	Parameternamn	Hexvärde	Memo
#1	Format byte – physical addressing (format-byte – fysisk adressering)	80	FMT
#2	Target address byte (måladress-byte)	tt	TGT
#3	Source address byte (källadress-byte)	EE	SRC
#4	Additional length byte (extra längd-byte)	02	LEN
#5	SecurityAccessReques Positive Response Service Id (säkerhetstillträde begäran positivt svar tjänste-ID)	67	SAPR
#6	accessType – sendKey (tillträdestyp – sänd nyckel)	7E	AT_SK
#7	Checksum (kontrollsumma)	00-FF	CS

Tabell 23

SecurityAccess Negative Response Message (begäran om säkerhetstillträde negativt svarsmeddelande)

Byte #	Parameternamn	Hexvärde	Memo
#1	Format byte – physical addressing (format-byte – fysisk adressering)	80	FMT
#2	Target address byte (måladress-byte)	tt	TGT
#3	Source address byte(källadress-byte)	EE	SRC
#4	Additional length byte (extra längd-byte)	03	LEN
#5	NegativeResponse Service Id (negativt svar tjänste-Id)	7F	NR
#6	SecurityAccessRequest#2 Service Id (säkerhetstillträde begäran #2 tjänste-ID)	27	SA
#7	ResponseCode (svarskod) = [generalReject	10	RC_GR
	subFunctionNotSupported (underfunktion stöds ej)	12	RC_SFNS
	incorrectMessageLength	13	RC_IML
	conditionsNotCorrectOrRequestSequenceError	22	RC_CNC
	invalidKey (ogiltig nyckel)	35	RC_IK
	exceededNumberOfAttempts	36	RC_ENA
	requestCorrectlyReceived-ResponsePending]	78	RC_RCR_RP
#8	Checksum (kontrollsumma)	00-FF	CS

6. DATAÖVERFÖRINGSTJÄNSTER

Tillgängliga tjänster specificeras i nedanstående tabell.

Tabell 24

Tjänster för överföring av data

Namn på tjänsten	Beskrivning
ReadDataByIdentifier	Klienten begär överföring av befintligt värde av en post som nås via recordDataIdentifier.
WriteDataByIdentifier	Klienten begär att få skriva en post som nås via recordDataIdentifier.

6.1 **Tjänsten ReadDataByIdentifier (läs data med lokal identifierare)**

6.1.1 ***Meddelandebeskrivning***

CPR_050 Tjänsten ReadDataByIdentifier används av klienten för att begära datapostvärden från en server. Data identifieras av en recordDataIdentifier. Tillverkaren av fordonsenheten har ansvaret för att de villkor som gäller för servern uppfylls när denna tjänst utförs.

6.1.2 ***Meddelandeformat***

CPR_051 Meddelandeformaten för ReadDataByIdentifier-primitiver anges i detalj i nedanstående tabeller.

Tabell 25

ReadDataByIdentifier Request Message (meddelande med begäran om läs data med identifierare)

Byte #	Parameternamn	Hexvärde	Memo
#1	Format byte – physical addressing (format-byte – fysisk adressering)	80	FMT
#2	Target address byte (måladress-byte)	EE	TGT
#3	Source address byte (källadress-byte)	tt	SRC
#4	Additional length byte (extra längd-byte)	03	LEN
#5	ReadDataByIdentifier Request Service Id	22	RDBI
#6 till #7	RecordDataIdentifier = [ett värde från tabell 28]	xxxx	RDI_…
#8	Checksum (kontrollsumma)	00-FF	CS

Tabell 26

ReadDataByIdentifier Positive Response Message (Läsa data med identifierare positivt svarsmeddelande)

Byte #	Parameternamn	Hexvärde	Memo
#1	Format byte – physical addressing (format-byte – fysisk adressering)	80	FMT
#2	Target address byte (måladress-byte)	tt	TGT
#3	Source address byte (källadress-byte)	EE	SRC
#4	Additional length byte (extra längd-byte)	m+3	LEN
#5	ReadDataByIdentifier Positive Response Service Id (Läs data med identifierare positivt svar tjänste-ID)	62	RDBIPR
#6 och #7	recordDataIdentifier = [samma värde som byte #6 och #7 tabell 25]	xxxx	RDI_…
#8 till #m+7	dataRecord[] = [data#1	xx	DREC_DATA1
	:	:	:
	data#m]	xx	DREC_DATAm
#m+8	Checksum (kontrollsumma)	00-FF	CS

Tabell 27

ReadDataByIdentifier Negative Response Message (Läs data med identifierare negativt svarsmeddelande)

Byte #	Parameternamn	Hexvärde	Memo
#1	Format byte – physical addressing (format-byte – fysisk adressering)	80	FMT
#2	Target address byte (måladress-byte)	tt	TGT
#3	Source address byte (källadress-byte)	EE	SRC
#4	Additional length byte (extra längd-byte)	03	LEN
#5	NegativeResponse Service Id (negativt svar tjänste-ID)	7F	NR
#6	ReadDataByIdentifier Request Service Id (läs data med lokal identifierare begäran tjänste-ID)	22	RDBI
#7	ResponseCode = [requestOutOfRange	31	RC_ROOR
	incorrectMessageLength	13	RC_IML
	conditionsNotCorrect]	22	RC_CNC
#8	Checksum (kontrollsumma)	00-FF	CS

6.1.3 ***Definition av parametrar***

CPR_052 Parametern recordDataIdentifier (RDI_) i ReadDataByIdentifier request message (meddelande med begäran om läs data med lokal identifierare) identifierar en datapost.

CPR_053 De värden för recordDataIdentifier som definieras i detta dokument visas i tabellen nedan.

Tabellen för recordDataLocalIdentifier består av fyra kolumner och flera rader.

— Den första kolumnen (Hex) inbegriper det 'Hexvärde' som tilldelas den recordDataIdentifier som specificeras i den tredje kolumnen.

— I den andra kolumnen (Dataelement) specificeras de dataelement i tillägg 1 som ligger till grund för recordData Identifier (ibland är omkodning nödvändig).

— I den tredje kolumnen (Beskrivning) specificeras motsvarande namn på recordDataIdentifier.

— I den fjärde kolumnen (Memo) specificeras memo för denna recordDataIdentifier.

Tabell 28

Definition av värden på recordDataIdentifier

Hex	Dataelement	recordDataIdentifier (namn) (se format i avsnitt 8.2)	Memo
F90B	CurrentDateTime	TimeDate (Tid datum)	RDI_TD
F912	HighResOdometer	HighResolutionTotalVehicleDistance (hög upplösning sammanlagd fordonssträcka)	RDI_HRTVD
F918	K-ConstantOfRecordingEquipment	Kfactor (K-faktor)	RDI_KF
F91C	L-TyreCircumference	LfactorTyreCircumference (L-faktor däckens omkrets)	RDI_LF
F91D	W-VehicleCharacteristicConstant	WvehicleCharacteristicFactor (W fordonets karakteristiska faktor)	RDI_WVCF
F921	TyreSize	TyreSize (däckstorlek)	RDI_TS
F922	nextCalibrationDate	NextCalibrationDate (nästa kalibreringsdatum)	RDI_NCD
F92C	SpeedAuthorised	SpeedAuthorised (tillåten hastighet)	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 ReadDataByIdentifier för att tillhandahålla det datapostvärde som identifieras av recordDataIdentifier till klienten (provaren). Dataformaten specificeras i avsnitt 8. Ytterligare valfria användardata (dataRecords), inklusive fordonsenhetsspecifika ingående, interna och utgående data, kan implementeras, men de definieras inte i detta dokument.

6.2 **Tjänsten WriteDataByLocalIdentifier (skriv data med lokal identifierare)**

6.2.1 ***Meddelandebeskrivning***

CPR_056 Tjänsten WriteDataByIdentifier används av klienten för att skriva datapostvärden till en server. Dessa data identifieras genom en recordDataIdentifier. Det åligger tillverkaren av fordonsenheten att se till att server-villkoren uppfylls när denna tjänst utförs. Vid uppdatering av de parametrar som förtecknas i tabell 28 måste fordonsenheten vara i CALIBRATION-läge.

6.2.2 ***Meddelandeformat***

CPR_057 Meddelandeformaten för WriteDataByIdentifier-primitiver anges i detalj i nedanstående tabeller.

Tabell 29

WriteDataByIdentifier Request Message

Byte #	Parameternamn	Hexvärde	Memo
#1	Format byte – physical addressing (format-byte – fysisk adressering)	80	FMT
#2	Target address byte (måladress-byte)	EE	TGT
#3	Source address byte (källadress-byte)	tt	SRC
#4	Additional length byte (extra längd-byte)	m+3	LEN
#5	WriteDataByIdentifier Request Service Id	2E	WDBI
#6 till #7	RecordDataIdentifier = [ett värde från tabell 28]	xxxx	RDI_…
#8 till #m+7	DataRecord[] = [data#1 : data#m]	xx : xx	DREC_DATA1 : DREC_DATAm
#m+8	Checksum (kontrollsumma)	00-FF	CS

Tabell 30

WriteDataByIdentifier Positive Response Message (skriv data med identifierare positivt svarsmeddelande)

Byte #	Parameternamn	Hexvärde	Memo
#1	Format byte – physical addressing	80	FMT
#2	Target address byte	tt	TGT
#3	Source address byte	EE	SRC
#4	Additional length byte	03	LEN
#5	WriteDataByIdentifier Positive Response Service Id	6E	WDBIPR
#6 till #7	RecordDataIdentifier = [samma värde som byte #6 och #7 tabell 27]	xxxx	RDI_…
#8	Checksum	00-FF	CS

Tabell 31

WriteDataByIdentifier Negative Response Message (skriv data med identifierare negativt svarsmeddelande)

Byte #	Parameternamn	Hexvärde	Memo
#1	Format byte – physical addressing	80	FMT
#2	Target address byte	tt	TGT
#3	Source address byte	EE	SRC
#4	Additional length byte	03	LEN
#5	NegativeResponse Service Id	7F	NR
#6	WriteDataByIdentifier Request Service Id	2E	WDBI
#7	ResponseCode = [requestOutOfRange	31	RC_ROOR
	IncorrectMessageLength	13	RC_IML
	ConditionsNotCorrect]	22	RC_CNC
#8	Checksum	00-FF	CS

6.2.3 ***Definition av parametrar***

Parametern recordDataIdentifier (RDI_) definieras i tabell 28.

Parametern dataRecord (DREC_) används av meddelandet WriteDataByIdentifier för att tillhandahålla de datapostvärden som identifieras genom recordDataIdentifier för servern (fordonsenheten). 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	Klienten begär kontroll över indata/utdata som är specifika för servern.

7.1 Tjänsten InputOutputControlByIdentifier (kontroll av in-/utdata med identifierare)

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.

CPR_058 Denna I/O-signallinje för kalibrering kan konfigureras genom K-linje-kommandot med hjälp av tjänsten InputOutputControlByIdentifier som väljer begärd ingående eller utgående funktion för linjen. Linjen har följande tillstånd:

— Avaktiverad.

— speedSignalInput, där I/O-signallinjen används för inmatning av en hastighetssignal (testsignal) som ersätter hastighetssignalen för rörelsedetektorn.

— realTimeSpeedSignalOutputSensor, där I/O-signallinjen används för utmatning av hastighetssignalen för rörelsedetektorn.

— RTCOutput, där I/O-signallinjen används för utmatning av klocksignalen (UTC).

CPR_059 Fordonsenheten måste ha påbörjat en inställningssession och den måste vara i CALIBRATION-läge för att konfigurera linjens tillstånd. Vid avslutande av inställningssession eller av CALIBRATION-läge måste fordonsenheten se till att I/O-signalen för kalibrering återställs till 'avaktiverat' (förvalt) tillstånd.

CPR_060 Om hastighetspulser (speed pulses) tas emot i den ingående linjen för hastighetssignal i realtid i fordonsenheten medan I/O-signalen för kalibrering är satt till ingående, så skall I/O-signallinjen för kalibrering sättas till utgående eller återställas till det avaktiverade tillståndet.

CPR_061 Sekvensen skall vara följande:

— Upprätta kommunikation genom StartCommunication Service.

— Påbörja en inställningssession genom StartDiagnosticSession Service och stå i driftläge CALIBRATION (ordningen på dessa två åtgärder saknar betydelse).

— Ändra tillstånd för utgående data med hjälp av InputOutputControlByIdentifier.

7.1.2 *Meddelandeformat*

CPR_062 Meddelandeformat för InputOutputControlByIdentifier-primitiver anges i detalj i nedanstående tabeller.

Tabell 33

InputOutputControlByIdentifier Request Message (meddelande med begäran om kontroll av in-/utdata med identifierare)

Byte #	Parameternamn	Hexvärde	Memo
#1	Format byte – physical addressing (Format-byte – fysisk adressering)	80	FMT
#2	Target address byte (måladress-byte)	EE	TGT
#3	Source address byte (källadress-byte)	tt	SRC
#4	Additional length byte (extra längd-byte)	xx	LEN
#5	InputOutputControlByIdentifier Request Sid	2F	IOCBI
#6 and #7	InputOutputIdentifier = [CalibrationInputOutput]	F960	IOI_CIO
#8 eller #8 till #9	ControlOptionRecord = [		COR_…
	inputOutputControlParameter – ett värde från Tabell 36 – Definition av värden för inputOutputControlParameter	xx	IOCP_…
	controlState – ett värde från Tabell 37 – Definition av controlState-värden (se anmärkning nedan)]	xx	CS_…
#9 eller #10	Checksum (kontrollsumma)	00-FF	CS

Märk: Parametern controlState (kontrolltillstånd) är närvarande endast i vissa fall (se 7.1.3).

Tabell 34

InputOutputControlByIdentifier Request Message (kontroll av in-/utdata med identifierare positivt svarsmeddelande)

Byte #	Parameternamn	Hexvärde	Memo
#1	Format byte – physical addressing (format-byte – fysisk adressering)	80	FMT
#2	Target address byte (måladress-byte)	tt	TGT
#3	Source address byte (källadress-byte)	EE	SRC
#4	Additional length byte (extra längd-byte)	xx	LEN
#5	inputOutputControlByIdentifier Positive Response SId	6F	IOCBIPR
#6 and #7	inputOutputIdentifier = [CalibrationInputOutput]	F960	IOI_CIO
#8 eller #8 till #9	controlStatusRecord = [		CSR_
	inputOutputControlParameter (samma värde som byte #8 Tabell 33 – InputOutputControlByIdentifier Request Message (meddelande med begäran om kontroll av in-/utdata med identifierare)	xx	IOCP_…
	controlState (samma värde som byte #9 Tabell 33 – InputOutputControlByIdentifier Request Message (meddelande med begäran om kontroll av in-/utdata med identifierare) (i förekommande fall)]	xx	CS_…
#9 eller #10	Checksum (kontrollsumma)	00-FF	CS

Tabell 35

InputOutputControlByIdentifier Negative Response Message (kontroll av in-/utdata med identifierare negativt svarsmeddelande)

Byte #	Parameternamn	Hexvärde	Memo
#1	Format byte – physical addressing (format-byte – fysisk adressering)	80	FMT
#2	Target address byte (måladress-byte)	tt	TGT
#3	Source address byte (källadress-byte)	EE	SRC
#4	Additional length byte (extra längd-byte)	03	LEN
#5	negativeResponse Service Id	7F	NR
#6	inputOutputControlByIdentifier Request SId	2F	IOCBI
#7	responseCode = [		
	incorrectMessageLength	13	RC_IML
	conditionsNotCorrect	22	RC_CNC
	requestOutOfRange	31	RC_ROOR
	deviceControlLimitsExceeded]	7A	RC_DCLE
#8	Checksum	00-FF	CS

7.1.3 ***Definition av parametrar***

CPR_064 Parametern inputOutputControlParameter (IOCP_) definieras i nedanstående tabell.

Tabell 36

Definition av värden för inputOutputControlParameter

Hex	Beskrivning	Memo
01	ReturnControlToECU Detta värde skall ange för servern (fordonsenheten) att provaren inte längre har kontroll över I/O-signallinjen för kalibrering.	RCTECU
01	ResetToDefault Med detta värde får servern (fordonsenheten) en begäran om att återställa I/O-signallinjen för kalibrering till dess förvalda tillstånd.	RTD
03	ShortTermAdjustment Med detta värde får servern (fordonsenheten) en begäran om att ställa in I/O-signallinjen för kalibrering på det värde som ingår i controlState-parametern.	STA

CPR_065 Parametern controlState är närvarande endast när inputOutputControlParameter har satts till ShortTermAdjustment och den definieras i nedanstående tabell.

Tabell 37

Definition av controlState-värden

Mode	Hexvärde	Beskrivning
Avaktivera	00	I/O-linjen är avaktiverad (förvalt tillstånd)
Aktivera	01	Aktivera I/O-linjen för kalibrering som speedSignalInput
Aktivera	02	Aktivera I/O-linjen för kalibrering som realTimeSpeedSignalOutputSensor
Aktivera	03	Aktivera I/O-linjen för kalibrering som RTCOutput

8. FORMAT FÖR DATARECORDS

I detta avsnitt beskrivs följande:

— Allmänna regler som skall tillämpas på de olika parametrar som överförs av fordonsenheten till provaren.

— Format som skall användas för data som överförs via de dataöverföringstjänster som beskrivs i avsnitt 6.

CPR_067 Alla parametrar som beskrivs här skall kunna hanteras av fordonsenheten.

CPR_068 Data som överförs av fordonsenheten till provaren som svar på en begäran skall vara uppmätta (dvs. aktuellt värde på den begärda parametern enligt fordonsenhetens mätning eller observation).

8.1 **Giltiga värden på överförda parametrar**

CPR_069 Tabell 38 definieras 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 giltiga värden 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.

CPR_072 Om ett komponentfel förhindrar överföringen av giltiga data för en parameter, bör den felindikator som beskrivs i Tabell 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 man använda motsvarande minsta eller största parametervärde vid dataöverföringen.

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 till 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 39 till 42 nedan beskrivs de format som skall användas via tjänsterna ReadDataByIdentifier och WriteDataByIdentifier.

CPR_074 Tabell 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	Mer detaljerade uppgifter finns i Tabell 40	
HighResolutionTotalVehicleDistance	4	5 m/bit ökning, 0 m offset	0 till + 21 055 406 km
Kfactor	2	0,001 impulser/m /bit ökning, 0 offset	0 till 64,255 impulser/m
LfactorTyreCircumference	2	0,125 10^{-3} m/bit ökning, 0 offset	0 till 8 031 m
WvehicleCharacteristicFactor	2	0,001 impulser/m /bit ökning, 0 offset	0 till 64,255 impulser/m
TyreSize	15	ASCII	ASCII
NextCalibrationDate	3	Mer detaljerade uppgifter finns i Tabell 41	
SpeedAuthorised	2	1/256 km/h/bit ökning, 0 offset	0 till 25 0996 km/h
RegisteringMemberState	3	ASCII	ASCII
VehicleRegistrationNumber	14	Mer detaljerade uppgifter finns i Tabell 42	
VIN	17	ASCII	ASCII

CPR_075 Tabell 40 innehåller uppgifter om formaten för de olika databyte som ingår i parametern TimeDate:

Tabell 40

Format för TimeDate (recordDataIdentifier # F00B)

Byte	Parameterdefinition	Upplösning	Driftsintervall
1	Sekunder	0,25 s/bit ökning, 0 s offset	0 till 59,75 s
2	Minuter	1 min/bit ökning, 0 min offset	0 till 59 min
3	Timmar	1 h/bit ökning, 0 h offset	0 tikk 23 h
4	Månad	1 månad/bit ökning, 0 månad offset	1 till 12 månader
5	Dag	0,25 dag/bit ökning, 0 dag offset (se anmärkning under Tabell 41)	0,25 till 31,75 dagar
6	År	1 år/bit ökning, +1985 år offset (se anmärkning under Tabell 41)	1985 till 2235 år
7	Lokal förskjutning – minuter	1 min/bit ökning, – 125 min offset	– 59 till 59 min
8	Lokal förskjutning – timmar	1 h/bit ökning, – 125 h offset	– 23 till + 23 h

CPR_076 Tabell 41 innehåller uppgifter om formaten för varje byte i parametern NextCalibrationDate parameter.

Tabell 41

Detaljerat format för NextCalibrationDate (recordDataIdentifier # F022)

Byte	Parameterdefinition	Upplösning	Driftsintervall
1	Månad	1 månad/bit ökning, 0 månader offset	1 till 12 månader
2	Dag	0,25 dagar/bit ökning, 0 dagar offset (se anmärkning nedan)	0,25 till 31,75 dagar
3	År	1 år/bit ökning, +1985 år offset (se anmärkning nedan)	1985 till 2235 år

Anmärkning beträffande användningen av parametern '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 etc.
2. Denna parameter ändrar eller påverkar inte parametern 'timmar' ovan.

Anmärkning beträffande användningen av parametern 'År':
Värdet 0 för år betecknar år 1985; värdet 1 betecknar 1986 etc.

CPR_078 Tabell 42 innehåller uppgift om formaten för de olika delarna i parametern VehicleRegistrationNumber:

Tabell 42

Detaljerat format för VehicleRegistrationNumber (recordDataIdentifier # F07E)

Byte	Parameterdefinition	Upplösning	Driftsintervall
1	Teckentabell (enligt definitionen i bilaga 1)	ASCII	01 till 0A
2–14	Fordonets registreringsnummer (enligt definitionen i bilaga 1)	ASCII	ASCII

Tillägg 9

TYPGODKÄNNANDE – FÖRTECKNING ÖVER MINSTA ANTAL PROVNINGAR SOM KRÄVS

INNEHÅLL

1. INLEDNING

1.1 **Typgodkännande**

EEG:s typgodkännande för en färdskrivare (eller komponent) eller ett färdskrivarkort bygger på följande:

— En säkerhetscertifiering som utförs av en ITSEC-myndighet, i förhållande till ett säkerhetsmål som till fullo överensstämmer med tillägg 10 till denna bilaga.

— En funktionscertifiering som utförs av en myndighet i en medlemsstat, för att intyga att det provade föremålet uppfyller kraven i denna bilaga med avseende på funktioner, exakthet hos uppmätningar och miljöegenskaper.

— En certifiering av driftskompatibiliteten, som utförs av ett behörigt organ, för att intyga att färdskrivaren (eller färdskrivarkortet) är fullständigt driftskompatibel med de nödvändiga färdskrivarkortmodellerna (eller färdskrivarmodellerna) (se bilagan, kapitel VIII).

I detta tillägg anges de provningar som måste utföras av en myndighet i en medlemsstat vid funktionsprovningarna, och de provningar som måste utföras av ett behörigt organ vid provningarna av driftskompatibiliteten. Förfaranden för att utföra provningarna eller typ av provningar specificeras inte ytterligare.

Säkerhetscertifiering omfattas inte av detta tillägg. Om vissa provningar som krävs för typgodkännande utförs vid säkerhetsutvärderingen och säkerhetscertifieringen behöver dessa provningar inte utföras igen. I detta fall behöver bara resultaten från dessa säkerhetsprovningar undersökas. De krav som förväntas bli testade (eller som liknar de provningar som förväntas bli utförda) vid säkerhetscertifieringen, är markerade med '*' i detta tillägg.

I detta tillägg ses typgodkännandet av rörelsesensorn och av fordonsenheten separat som komponenter i färdskrivaren. Driftskompatibilitet mellan varje rörelsesensormodell och varje fordonsenhetsmodell krävs inte, och därför kan typgodkännande av en rörelsesensor endast beviljas i kombination med typgodkännande av en fordonsenhet, och omvänt.

1.2 **Referenser**

Följande referenser används i detta tillägg:

IEC 68-2-1	Environmental testing – Part 2: Tests – Tests A: Cold. 1990 + Amendment 2: 1994.
IEC 68-2-2	Environmental testing – Part 2: Tests – Tests B: Dry Heat. 1974 + Amendment 2: 1994.
IEC 68-2-6	Basic environmental testing procedures – Test methods – Test Fc and guidance: Vibration (sinusoidal). 6th edition: 1985.
IEC 68-2-14	Basic environmental testing procedures – Test methods – Test N: Change of temperature. Modification 1: 1986.
IEC 68-2-27	Basic environmental testing procedures – Test methods – Test Ea and guidance: Shock. Edition 3: 1987.
IEC 68-2-30	Basic environmental testing procedures – Test methods – Test Db and guidance: Damp heat, cyclic (12 + 12 – hour cycle). Modification 1: 1985.
IEC 68-2-35	Basic environmental testing procedure – Test methods – Test Fda: Random vibration wide band – Reproductibility High. Modification 1: 1983.
IEC 529	Kapslingsklasser för elektrisk materiel (IP-kod). Utgåva 2: 1989.
IEC 61000-4-2	Electromagnetic Compatibility (EMC) – Testing and measurement techniques – Electrostatic discharge immunity test: 1995/Amendment 1: 1998
ISO 7637-1	Vägfordon – Ledningsbundna och kopplade elstörningar – Del 1: Personbilar, lätta lastbilar och bussar med 12 V elsystem – Elektriska transienter längs matningsledning. Utgåva 2: 1990.

ISO 7637-2 Vägfordon – Ledningsbundna och kopplade elstörningar – Del 2: Lastbilar och bussar med 24 V elsystem – Elektriska transienter längs matningsledning. Utgåva 1: 1990.

ISO 7637-3 Road vehicles – Electrical disturbance by conduction and coupling – Part 3: Vehicles with 12 V or 24 V supply voltage – Electrical transient transmission by capacitive and inductive coupling via lines other than supply lines. First Edition: 1995 + Cor 1: 1995.

ISO/IEC 7816-1 Transaktionskort – Aktivt kort – Fysiska egenskaper. Utgåva 1: 1998.

ISO/IEC 7816-2 Transaktionskort – Aktivt kort – Kontaktdon. Utgåva 1: 1999.

ISO/IEC 7816-3 Transaktionskort – Aktivt kort – Signaler och protokoll. Utgåva 2: 1997.

ISO/IEC 10373 Transaktionskort – Provningsmetoder. Utgåva 1: 1993.

2. FUNKTIONSTEST AV FORDONSENHETER

nr	Provning	Beskrivning	Berörda krav
1.	**Administrativ undersökning**		
1.1	Dokumentation	Dokumentationens korrekthet	
1.2	Tillverkarens provningsresultat	Resultat från tillverkarens provning som utfördes under visning av integrationspapper	070, 071, 073
2.	**Visuell besiktning**		
2.1	Överensstämmelse med dokumentation		
2.2	Identifiering/märkningar		168, 169
2.3	Material		163–167
2.4	Plombering		251
2.5	Externa gränssnitt		
3.	**Funktionstest**		
3.1	Tillhandahållna funktioner		002, 004, 244
3.2	Driftlägen		006*, 007*, 008*, 009*, 106, 107
3.3	Rättigheter till tillgång till data och funktioner		010*, 011*, 240, 246, 247
3.4	Övervakning av isättning och urtagning av kort		013, 014, 015*, 016*, 106
3.5	Mätning av hastighet och sträcka		017–026
3.6	Tidsmätning (provning utförd vid 20 °C)		027–032
3.7	Övervakning av förarens aktiviteter		033–043, 106
3.8	Övervakning av förarens status		044, 045, 106
3.9	Manuella angivelser		046–050b
3.10	Hantering av företagslås		051–055
3.11	Övervakning av kontrollaktiviteter		056, 057
3.12	Upptäckt av händelser och/eller fel		059–069, 106

nr	Provning	Beskrivning	Berörda krav
3.13	Data för identifiering av utrustning		075*, 076*, 079
3.14	Övervakning av isättning och urtagning av kort		081*–083*
3.15	Data om föraraktiviteter		084*–086*
3.16	Platsdata		087*–089*
3.17	Vägmätardata		090*–092*
3.18	Detaljerade hastighetsdata		093*
3.1.	Händelsedata		094*, 095
3.20	Feldata		096*
3.21	Kalibreringsdata		097*, 098*
3.22	Data om tidsinställning		100*, 101*
3.23	Data om kontrollaktiviteter		102*, 103*
3.24	Data om företagslås		104*
3.25	Överföringsdata		105*
3.26	Data om särskilda omständigheter		105a*, 105b*
3.27	Registrering och lagring på färdskrivarkort		108, 109*, 109a*, 110*, 111, 112
3.28	Visning		072, 106, 113–128, PIC_001, DIS_001
3.29	Utskrift		072, 106, 129–138, PIC_001, PRT_001 a PRT_012
3.30	Varning		106, 139–148, PIC_001
3.31	Överföring av data till externa media		072, 106, 149–151
3.32	Utgående data till ytterligare externa anordningar		152, 153
3.33	Kalibrering		154*, 155*, 156*, 245
3.34	Tidsinställning		157*, 158*
3.35	Avsaknad av störningar från ytterligare funktioner		003, 269

nr	Provning	Beskrivning	Berörda krav
4.	**Miljöprovningar**		
4.1	Temperatur	Kontrollera funktionalitet genom: — IEC 68-2-1, test Ad, med en varaktighet för provningen av 72 timmar vid den lägre temperaturen (- 20 °C), 1 timme i drift, 1 timme ej i drift — IEC 68-2-2, test Bd, med en varaktighet för provningen av 72 timmar vid den högre temperaturen (+ 70 °C), 1 timme i drift, 1 timme ej i drift Temperaturcykler: Kontrollera att fordonsenheten tål snabba förändringar av omgivningens temperatur genom IEC 68-2-14 test Na, 20 cykler, var och en med temperatur som varierar mellan den lägre temperaturen (- 20 °C) och den högre temperaturen (+ 70 °C) och två sammanhängande timmar både vid den lägre och den högre temperaturen. En minskad uppsättning provningar (bland dem som anges i del 3 i denna tabell) kan utföras vid den lägre temperaturen, den högre temperaturen och under temperaturcyklerna	159
4.2	Luftfuktighet	Kontrollera att fordonsenheten tål en cyklisk fuktighet (värmeprovning) genom IEC 68-2-30, 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	160
4.3	Vibrationer	1. Sinusformade vibrationer: Kontrollera att fordonsenheten tål sinusformade vibrationer med följande egenskaper: Konstant variation mellan 5 och 11 Hz: En topp på 10 mm. Konstant acceleration mellan 11 och 300 Hz: 5 g. Detta krav kontrolleras genom IEC 68-2-6, test Fc, med en minsta provningsvaraktighet av 3 x 12 timmar (12 timmar per axel). 2. Slumpartade vibrationer: Kontrollera att fordonsenheten tål slumpartade vibrationer med följande egenskaper: Frekvens på 5–150 Hz, nivå 0.02 g^2/Hz Detta krav kontrolleras genom IEC 68-2-35, test Ffda, med en minsta provningsvaraktighet av 3 x 12 timmar (12 timmar per axel) De två provningarna ovan skall utföras på två olika exemplar av den utrustning som provas	163
4.4	Skydd mot vatten och främmande föremål	Kontrollera att fordonsenhetens skyddsklass enligt IEC 529 är åtminstone IP 40, när den är monterad för driftsvillkor i ett fordon	164, 165
4.5	Skydd mot överspänning	Kontrollera att fordonsenheten tål strömtillförsel av: 24 V-versioner: 34 V vid + 40 °C 1 timme 12 V-versioner: 17 V vid + 40 °C 1 timme	161
4.6	Skydd mot omkastade poler	Kontrollera att fordonsenheten tål en omkastning av strömtillförseln	161

nr	Provning	Beskrivning	Berörda krav
4.7	Skydd mot kortslutning	Kontrollera att inkommande och utgående signaler skyddas mot kortslutning i strömtillförsel och jord	161
5.	**EMC-provningar**		
5.1	Utstrålning och känslighet	Överensstämmelse med direktiv 95/54/EEG	162
5.2	Elektrostatiska laddningar	Överensstämmelse med IEC 61000-4-2, ± 2 kV (nivå 1)	162
5.3	Känslighet för överförda transienter i strömtillförseln	För 24 V-versionerna: överensstämmelse med ISO 7637-2 puls 1a: Vs = - 100 V, Ri = 10 Ohm puls 2: Vs = + 100 V, Ri = 10 Ohm puls 3a: Vs = - 100 V, Ri = 50 Ohm puls 3b: Vs = + 100 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 puls 1: Vs = - 100 V, Ri = 10 Ohm puls 2: Vs = + 100 V, Ri = 10 Ohm puls 3a: Vs = - 100 V, Ri = 50 Ohm puls 3b: Vs = + 100 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 skall endast provas för de fordonsenheter som är avsedda att installeras i fordon för vilka inget externt gemensamt skydd mot laddningsdump (load dump) används	162

3. FUNKTIONSTEST AV RÖRELSESENSOR

nr	Provning	Beskrivning	Berörda krav
1.	**Administrativ undersökning**		
1.1	Dokumentation	Dokumentationens korrekthet	
2.	**Visuell besiktning**		
2.1	Överensstämmer med dokumentation		
2.2	Identifiering/märkningar		169, 170
2.3	Material		163–167
2.4	Plombering		251
3.	**Funktionsprovningar**		
3.1	Identifieringsdata för sensorn		077*
3.2	Hopkoppling av rörelsesensor med fordonsenhet		099*, 155
3.3	Rörelseavkänning Korrekt rörelsemätning		 022–026

nr	Provning	Beskrivning	Berörda krav
4.	**Miljöprovningar**		
4.1	Drifttemperaturer	Kontrollera funktionalitet (enligt definition i provning nr. 3.3) i temperaturområdet – 40 °C till + 135 °C genom följande: — IEC 68-2-1 test Ad, med en provningsvaraktighet av 96 timmar vid en lägsta temperatur av To_{min}, — IEC 68-2-2 test Bd, med en provningsvaraktighet av 96 timmar vid en högsta temperatur av To_{min},	159
4.2	Temperaturcykler	Kontrollera funktionalitet (enligt definition i provning nr 3.3) genom IEC 68-2-14 test Na, 20 cykler, var och en med en temperatur som varierar mellan den lägre temperaturen (– 40 °C) och den högre temperaturen (+ 135 °C) och två sammanhängande timmar både vid den lägre och den högre temperaturen. En minskad uppsättning provningar (bland dem som anges i provning 3.3) kan utföras vid den lägre temperaturen, den högre temperaturen och under temperaturcyklerna	159
4.3	Luftfuktighetscykler	Kontrollera funktionalitet (enligt definition i provning nr 3.3) genom IEC 68-2-30, 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	160
4.4	Vibrationer	Kontrollera funktionalitet (enligt definition i provning nr 3.3) genom IEC 68-2-6, test Fc, med en provningsvaraktighet av 100 frekvenscykler. Konstant variation mellan 10 och 57 Hz: En topp på 1,5 mm Konstant acceleration mellan 57 och 500 Hz: 20 g	163
4.5	Mekaniska stötar	Kontrollera funktionalitet (enligt definition i provning nr 3.3) genom IEC 68-2-27, test Ea, tre stötar i båda riktningar hos de tre vinkelräta axlarna	163
4.6	Skydd mot vatten och främmande föremål	Kontrollera att rörelsesensorns skyddsklass enligt IEC 529 är åtminstone IP 64, när den är monterad för driftsvillkor i ett fordon	165
4.7	Skydd mot omkastade poler	Kontrollera att rörelsesensorn tål en omkastning av strömtillförseln	161
4.8	Skydd mot kortslutning	Kontrollera att inkommande signaler är skyddade mot kortslutning i strömtillförsel och jord	161
5.	**EMC**		
5.1	Utstrålning och känslighet	Kontrollera överensstämmelse med direktiv 95/54/EEG	162
5.2	Elektrostatiska laddningar	Överensstämmelse med IEC 61000-4-2, ± 2 kV (nivå 1)	162
5.3	Känslighet för överförda transienter i datalinjer	Överensstämmelse med ISO 7637-3 (nivå III)	162

4. FUNKTIONSPROVNING AV FÄRDSKRIVARKORT

nr	Provning	Beskrivning	Berörda krav
1.	**Administrativ undersökning**		
1.1	Dokumentation	Dokumentationens korrekthet	
2.	**Visuell besiktning**		
2.1		Kontrollera att alla skyddsegenskaper och synliga data skrivs ut korrekt på kortet och att de uppfyller bestämmelserna	171–181
3.	**Fysiska provningar**		
3.1	Kontrollera kortets dimensioner och kontakternas placering		184 ISO/IEC 7816-1 ISO/IEC 7816-2
4.	**Protokollprovningar**		
4.1	ATR	Kontrollera att ATR uppfyller bestämmelserna	ISO/IEC 7816-3 TCS 304, 307, 308
4.2	T=0	Kontrollera att protokollet T=0 uppfyller bestämmelserna	ISO/IEC 7816-3 TCS 302, 303, 305
4.3	PTS	Kontrollera att PTS-kommandot uppfyller bestämmelserna genom att sätta T=1 från T=0	ISO/IEC 7816-3 TCS 309–311
4.4	T=1	Kontrollera att protokollet T=1 uppfyller bestämmelserna	ISO/IEC 7816-3 TCS 303, / 306
5.	**Kortets struktur**		
5.1		Prova att filstrukturen på kortet uppfyller bestämmelserna genom att kontrollera förekomsten av obligatoriska filer på kortet och deras villkor för tillträde	TCS 312 TCS 400*, 401, 402, 403*, 404, 405*, 406, 407, 408*, 409, 410*, 411, 412, 413*, 414, 415*, 416, 417, 418*, 419
6.	**Funktionsprovningar**		
6.1	Normal behandling	Prova varje tillåten användning av varje kommando åtminstone en gång (till exempel: prova UPDATE BINARY-kommandot med CLA = '00', CLA = '0C' och med olika P1-, P2- och Lc-parametrar). Kontrollera att uppgifterna verkligen har utförts på kortet (exempelvis genom att läsa den fil som kommandot har utförts på)	TCS 313 till TCS 379
6.2	Felmeddelanden	Prova varje felmeddelande åtminstone en gång (enligt angivelse i tillägg 2) för varje kommando. Prova varje generiskt fel (utom '6400'-integritetsfel som kontrollerats vid säkerhetscertifiering) åtminstone en gång	
7.	**Miljöprovningar**		
7.1		Kontrollera att korten fungerar inom de gränsvillkor som fastställts i enlighet med ISO/IEC 10373	185–188 ISO/IEC 7816-1

5. PROVNING AV DRIFTSKOMPATIBILITET

nr	Provning	Beskrivning
1.	Ömsesidig autentisering	Kontrollera att den ömsesidiga autentiseringen mellan fordonsenheten och färdskrivarkortet fungerar normalt
2.	Skriv-/läsprovningar	Utför ett typiskt aktivitetsscenario på fordonsenheten. Scenariot skall anpassas till den typ av kort som provas och inbegripa skrivningar på så många EF som möjligt på kortet Verifiera genom en kortöverföring att alla motsvarande registreringar har gjorts korrekt Verifiera genom en daglig utskrift från kort att alla motsvarande registreringar kan läsas korrekt

Tillägg 10

ALLMÄNNA SÄKERHETSMÅL

I detta tillägg anges det minsta tillåtna innehållet i säkerhetsmålen för rörelsesensorer, fordonsenheter och färdskrivarkort.

För att utforma de säkerhetsmål gentemot vilka tillverkare får ansöka om säkerhetscertifiering, skall de förädla och fylla i dokumenten på vederbörligt sätt, utan att ändra eller ta bort befintliga hot, mål, förfaranden eller specifikationer av säkerhetsfunktioner.

INNEHÅLL

Allmänt säkerhetsmål för rörelsesensorer

Allmänt säkerhetsmål för fordonsenheter

Allmänt säkerhetsmål för färdskrivarkort

ALLMÄNT SÄKERHETSMÅL FÖR RÖRELSESENSORER

1. **Inledning**

Här beskrivs rörelsesensorn, de hot den skall kunna motverka och de säkerhetsmål den skall uppnå. Vidare specificeras de säkerhetsfunktioner som krävs. Här anges erfordrad minsta tillåtna styrka hos säkerhetsmekanismer och erfordrad garnantinivå för utveckling och evaluering.

De krav som anges här är desamma som i huvudtexten i bilaga I B. För att det skall bli lättare att läsa förekommer ibland dubblering mellan kraven i huvudtexten i bilaga I B och i säkerhetsmålen. Vid tvetydighet mellan ett krav i säkerhetsmålen och ett krav i huvudtexten i bilaga I B som avses i detta krav i säkerhetsmålen skall kravet i huvudtexten i bilaga I B gälla.

De krav i huvudtexten i bilaga I B som inte anges i säkerhetsmålen omfattas inte av säkerhetsfunktionerna.

Hot, mål, förfaranden och specifikationer av säkerhetsfunktioner har fått en unik märkning för att underlätta spårning till utvecklings- och evalueringsdokument.

2. **Förkortningar, definitioner och hänvisningar**

2.1 ***Förkortningar***

ROM	Read Only Memory – Minne för enbart avläsning
SEF	Security Enforcing Function – Säkerhetsfunktion
TBD	To Be Defined – Skall definieras
TOE	Target Of Evaluation – Evalueringsobjekt
VU	Vehicle Unit – Fordonsenhet

2.2 ***Definitioner***

Digital färdskrivare	Färdskrivare
Enhet	En anordning ansluten till rörelsesensorn
Rörelsedata	De data som utbyts med fordonsenheten, om hastighet och tillryggalagd sträcka
Fysiskt åtskilda delar	Fysiska komponenter i rörelsesensorn som fördelats i fordonet, i motsats till fysiska komponenter som samlats i rörelsesensorns kåpa
Säkerhetsdata	De särskilda data som krävs för att stödja säkerhetsfunktioner (exempelvis kryptografiska nycklar)
System	Utrustning, personer eller organisationer som har något samband med färdskrivaren
Användare	En person som använder en rörelsesensor (utom i uttrycket 'användardata')
Användardata	Alla data, utom rörelse- eller säkerhetsdata, som registreras av eller lagras i rörelsesensorn.

2.3 ***Referenser***

ITSEC ITSEC Information Technology Security Evaluation Criteria 1991 (kriterier för utvärdering av informationsteknologisk säkerhet).

3. **Produkternas syfte**

3.1 ***Beskrivning av rörelsesensorn och användningsmetod***

Rörelsesensorn skall installeras i vägtransportfordon. Dess syfte är att förse en fordonsenhet (VU) med krypterade rörelsedata om fordonets hastighet och tillryggalagd sträcka.

Rörelsesensorn har ett mekaniskt gränssnitt med en rörlig fordonsdel vars rörelse kan återge fordonets hastighet eller tillryggalagda sträcka. Den får vara placerad i fordonets växellåda eller i någon annan del av fordonet.

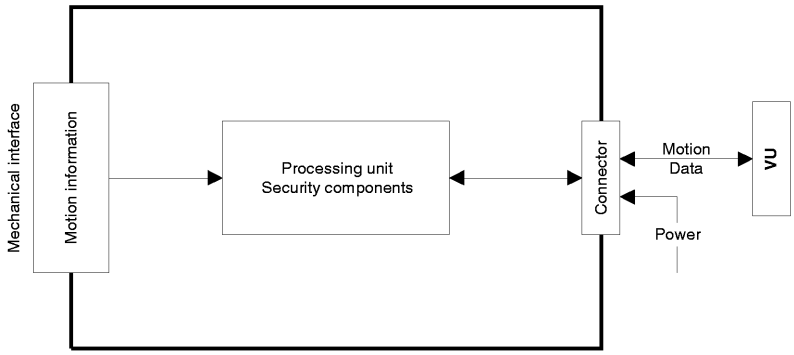
I driftläge är rörelsesensorn ansluten till en fordonsenhet.

Den får också anslutas till särskild utrustning i förvaltningssyfte (som tillverkaren skall definiera).

I följande figur beskrivs en typisk rörelsesensor:

Figur 1

Typisk rörelsesensor

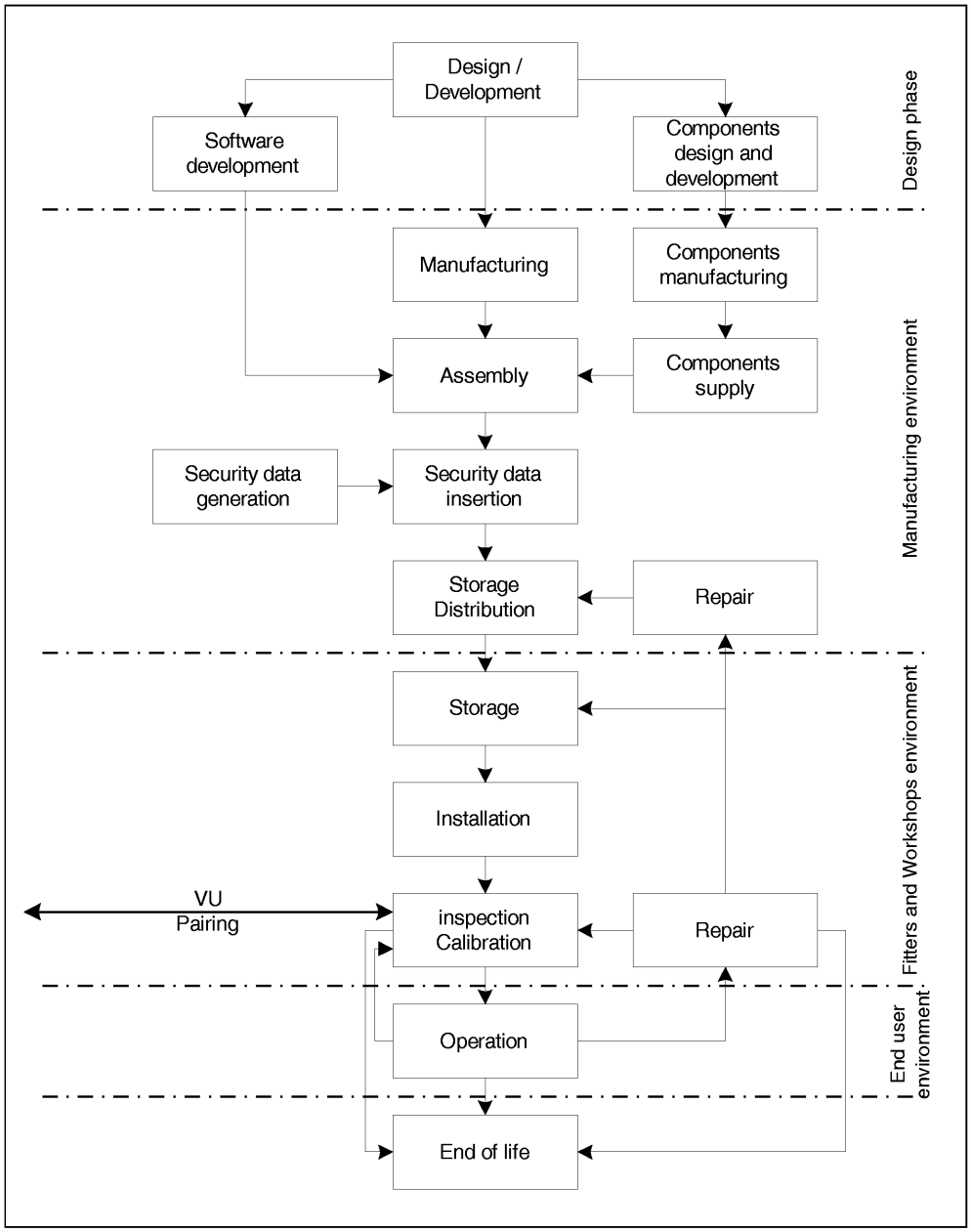


3.2 ***En rörelsesensors livscykel***

I följande figur beskrivs den typiska livscykeln för en rörelsesensor:

Figur 2

Typisk livscykel för en rörelsesensor



3.3 ***Hot***

I detta stycke beskrivs de hot som en rörelsesensor kan komma att utsättas för.

3.3.1 *Hot med avseende på bestämmelser om tillträdeskontroll*

T.Access	Användare skulle kunna försöka få tillträde till funktioner som inte är tillåtna för dem

3.3.2 *Hot med avseende på konstruktion*

T.Faults	Fel i maskinvara, programvara och kommunikationsförfaranden skulle kunna utsätta rörelsesensorn för oförutsedda förhållanden som äventyrar dess säkerhet
T.Tests	Användning av icke-validerade provningssätt eller av befintliga bakdörrar skulle kunna äventyra rörelsesensorns säkerhet
T.Design	Användare skulle kunna försöka tillgodogöra sig olovliga kunskaper om konstruktionen antingen från tillverkarens material (genom stöld, mutor, …) eller genom baklängeskonstruktion (reverse engineering)

3.3.3 *Hot med avseende på drift*

T.Environment	Användare skulle kunna äventyra säkerheten i rörelsesensorn genom miljöpåverkan (termisk, elektromagnetisk, optisk, kemisk, mekanisk, …)
T.Hardware	Användare skulle kunna ändra rörelsesensorns maskinvara
T.Mechanical_Origin	Användare skulle kunna försöka manipulera data som matas in i rörelsesensorn (exempelvis genom att skruva bort den från växellådan, …)
T.Motion_Data	Användare skulle kunna försöka ändra fordonets rörelsedata (tillägg, ändring, borttagande, återspelning av signal)
T.Power_Supply	Användare skulle kunna försöka omintetgöra säkerhetsmålen för rörelsesensorer genom att ändra (avbryta, minska, öka) strömtillförseln till dem
T.Security_Data	Användare skulle kunna försöka att få olovliga kunskaper om säkerhetsdata vid generering av säkerhetsdata eller transport eller lagring i färdskrivaren
T.Software	Användare skulle kunna ändra rörelsesensorns programvara
T.Stored_Data	Användare skulle kunna försöka ändra lagrade data (säkerhetsdata eller användardata)

3.4 ***Säkerhetsmål***

Det digitala färdskrivarsystemets huvudsakliga säkerhetsmål är följande:

O.Main	De data som skall kontrolleras skall finnas tillgängliga och till fullo och korrekt återspegla de kontrollerade förarnas och fordonens aktiviteter med avseende på körning, arbete, tillgänglighet, viloperioder och fordonets hastighet

Säkerhetsmålet för rörelsesensorn, som bidrar till det övergripande säkerhetsmålet, är följande:

O.Sensor_Main	De data som rörelsesensorn överför skall finnas tillgängliga för fordonsenheten så att denna till fullo och korrekt kan avgöra fordonets rörelser med avseende på hastighet och tillryggalagd sträcka

3.5 ***Informationstekniska säkerhetsmål***

De särskilda IT-säkerhetsmålen för rörelsesensorn, som bidrar till dess övergripande säkerhetsmål, är följande:

O.Access	Rörelsesensorn skall kontrollera anslutna enheters tillträde till funktioner och data
O.Audit	Rörelsesensorn skall granska försök till att undergräva dess säkerhet och den bör spåra dem till berörda enheter
O.Authentication	Rörelsesensorn skall autentisera anslutna enheter

O.Processing	Rörelsesensorn skall se till att behandlingen av inmatade data för att erhålla rörelsedata är korrekt
O.Reliability	Rörelsesensorn skall fungera tillförlitligt
O.Secured_Data_Exchange	Rörelsesensorn skall säkra utbytet av data med fordonsenheten

3.6 ***Fysiska förfaranden, personalförfaranden och övriga förfaranden***

Här beskrivs de fysiska förfaranden, personalförfaranden och övriga förfaranden som bidrar till rörelsesensorns säkerhet.

3.6.1 *Utrustningens konstruktion*

M.Development	De som utvecklar rörelsesensorer skall se till att ansvarsfördelningen vid utvecklingsarbetet görs på ett sådant sätt att IT-säkerheten upprätthålls
M.Manufacturing	Tillverkare av rörelsesensorer skall se till att ansvarsfördelningen under tillverkning görs på ett sådant sätt att IT-säkerheten upprätthålls, och att rörelsesensorn under tillverkning skyddas mot fysiska angrepp som kan äventyra IT-säkerheten

3.6.2 *Leverans av utrustningen*

M.Delivery	Tillverkare av rörelsesensorer och fordon samt montörer eller verkstäder skall se till att hanteringen av rörelsesensorn sker på ett sådant sätt att IT-säkerheten upprätthålls

3.6.3 *Generering och leverans av säkerhetsdata*

M.Sec_Data_Generation	Algoritmer för generering av säkerhetsdata får endast vara tillgängliga för auktoriserade och betrodda personer
M.Sec_Data_Transport	Säkerhetsdata skall genereras, transporteras och matas in i rörelsesensorn på ett sådant sätt att dess sekretess och integritet skyddas

3.6.4 *Installation, kalibrering och besiktning av färdskrivare*

M.Approved_Workshops	Installation, kalibrering och reparation av färdskrivare skall utföras av betrodda och godkända montörer eller verkstäder
M.Mechanical_Interface	Sätt att upptäcka fysisk manipulering med det mekaniska gränssnittet skall tillhandahållas (exempelvis plomberingar)
M.Regular_Inpections	Färdskrivaren skall besiktigas och kalibreras regelbundet

3.6.5 *Kontroll av att lagen upprätthålls*

M.Controls	Kontroller av att lagen upprätthålls skall utföras regelbundet och slumpvis och skall inbegripa säkerhetsgranskningar

3.6.6 *Uppgraderingar av programvara*

M.Software_Upgrade	Mjukvarurevisioner skall säkerhetscertifieras innan de får införas i en rörelsesensor

4. **Säkerhetsfunktioner**

4.1 ***Identifiering och autentisering***

UIA_101 Rörelsesensorn skall för varje användning kunna fastställa identiteten hos alla de enheter som den är ansluten till

UIA_102 Identiteten hos en ansluten enhet skall bestå av följande:

— En enhetsgrupp:

— Fordonsenhet (VU)

— Förvaltningsanordning

— Övrigt

Enhetsidentitet (endast fordonsenhet)

UIA_103 En ansluten fordonsenhets enhetsidentitet skall bestå av fordonsenhetens godkännandenummer och serienummer.

UIA_104 Rörelsesensorn skall kunna autentisera alla fordonsenheter eller förvaltningsanordningar som de är anslutna till

— då enheten ansluts,

— då strömtillförseln återupptas.

UIA_105 Rörelsesensorn skall regelbundet kunna återautentisera den fordonsenhet som den är ansluten till.

UIA_106 Rörelsesensorn skall upptäcka och förebygga användning av autentiseringsdata som har kopierats och återspelats.

UIA_107 Efter det att (skall definieras av tillverkare, dock högst 20) misslyckade autentiseringsförsök i rad har upptäckts, skall säkerhetsfunktionen

— generera en registrering om granskning av händelsen,

— varna enheten,

— fortsätta att exportera rörelsedata i okrypterat läge.

4.2 ***Tillträdeskontroll***

Tillträdeskontroller ser till att informationen läses från, skapas i, eller ändras till evalueringsobjektet enbart av dem som är auktoriserade att göra detta.

4.2.1 *Bestämmelser om tillträdeskontroll*

ACC_101 Rörelsesensorn skall kontrollera rättigheter till tillträde till funktioner och data.

4.2.2 *Tillträdesrättigheter till data*

ACC_102 Rörelsesensorn skall se till att data för identifiering av rörelsesensorn endast kan skrivas en gång (krav 078).

ACC_103 Rörelsesensorn skall godta och/eller lagra användardata endast från autentiserade enheter.

ACC_104 Rörelsesensorn skall upprätthålla lämpliga läs- och skrivrättigheter när det gäller tillträde till säkerhetsdata.

4.2.3 *Filstruktur och tillträdesvillkor*

ACC_105 Strukturen på tillämpningsfiler och datafiler samt tillträdesrättigheter skall upprättas vid tillverkningen, och sedan låsas från all eventuell ändring eller borttagning.

4.3 ***Spårbarhet***

ACT_101 Rörelsesensorn skall i sitt minne kunna lagra identiferingsdata för rörelsesensorer (krav 077).

ACT_102 Rörelsesensorn skall i sitt minne lagra installationsdata (krav 099).

ACT_103 Rörelsesensorn skall kunna mata ut spårbarhetsdata till autentiserade enheter på deras begäran.

4.4 ***Granskning***

AUD_101 Rörelsesensorn skall, för händelser som sänker dess säkerhet, generera granskningsregistreringar om händelserna.

AUD_102 Följande händelser påverkar rörelsesensorns säkerhet:

— Försök till säkerhetsöverträdelse:

  — Autentiseringsfel.

  — Integritetsfel hos lagrade data.

  — Fel vid överföring av interna data.

  — Ej auktoriserad öppning av kåpan.

  — Maskinvarusabotage.

— Sensorfel.

AUD_103 Granskningsregistreringar skall inbegripa följande data:

— Datum och tidpunkt för händelsen.

— Händelsetyp

— Identitet hos ansluten enhet.

När begärda data inte finns tillgängliga skall en lämplig default-indikation visas (som skall definieras av tillverkaren).

AUD_104 Rörelsesensorn skall sända de genererade granskningsregistreringarna till fordonsenheten samtidigt som de genereras, och får också lagra dem i sitt minne.

AUD_105 Om rörelsesensorn lagrar granskningsregistreringar skall den se till att 20 granskningsregistreringar bibehålls även om granskningslagringen har tagit slut, och den skall ha kapacitet att mata ut lagrade granskningsregistreringar till autentiserade enheter på deras begäran.

4.5 ***Korrekthet***

4.5.1 *Bestämmelser om kontroll av informationsflöden*

ACR_101 Rörelsesensorn skall se till att rörelsedata kan behandlas och härledas endast från mekaniska sensorinmatningar.

4.5.2 *Interna dataöverföringar*

Kraven i detta stycke skall endast tillämpas om rörelsesensorn använder sig av delar som är fysiskt åtskilda.

ACR_102 Om data överförs mellan fysiskt åtskilda delar i rörelsesensorn, skall de skyddas mot ändringar.

ACR_103 Om ett dataöverföringsfel upptäcks vid en intern överföring skall överföringen upprepas och säkerhetsfunktionerna generera en granskningsregistrering av händelsen.

4.5.3 *Integritet hos lagrade data*

ACR_104 Rörelsesensorn skall kontrollera de användardata som finns lagrade i dess minne för att upptäcka integritetsfel.

ACR_105 Om ett integritetsfel för lagrade användardata upptäcks skall säkerhetsfunktionerna generera en granskningsregistrering.

4.6 ***Funktionsduglighet***

4.6.1 *Provningar*

RLB_101 Alla kommandon, åtgärder, eller provningspunkter som är specifika för provningen i tillverkningsskedet skall avaktiveras och tas bort innan tillverkningsskedet är avslutat. Det skall inte vara möjligt att återställa dem för senare användning.

RLB_102 Rörelsesensorn skall utföra självprovningar vid initialstart och vid normal drift för att verifiera att den fungerar korrekt. Rörelsesensorns självprovning skall inbegripa en kontroll av integriteten hos säkerhetsdata och av integriteten hos den lagrade exekverbara koden (om den inte finns i ROM).

RLB_103 Om ett internt fel upptäcks vid självprovningen, skall säkerhetsfunktionerna generera en granskningsregistrering (sensorfel).

4.6.2 *Programvara*

RLB_104 Det skall inte gå att i fält analysera eller avlusa rörelsesensorns programvara.

RLB_105 Inmatade data från externa källor skall inte godtas som exekverbar kod.

4.6.3 *Fysiskt skydd*

RLB_106 Om rörelsesensorn är utformad så att den kan öppnas, skall den upptäcka alla öppningar av kåpan, även utan extern strömtillförsel under minst sex månader. I detta fall skall säkerhetsfunktionerna generera en granskningsregistrering av händelsen (som får genereras och lagras efter det att strömtillförseln återupptagits).

Om rörelsesensorn är utformad så att den inte kan öppnas, skall den vara utformad så att försök till fysisk manipulering lätt kan upptäckas (exempelvis genom visuell besiktning).

RLB_107 Rörelsesensorn skall upptäcka angivet (att definieras av tillverkaren) maskinvarusabotage.

RLB_108 I fallet ovan skall säkerhetsfunktionerna generera en granskningsregistrering och rörelsesensorn skall (skall definieras av tillverkaren).

4.6.4 *Avbrott av strömtillförseln*

RLB_109 Rörelsesensorn skall upprätthålla säkerheten om strömtillförseln bryts eller ändras.

4.6.5 *Villkor för återställning*

RLB_110 Vid strömavbrott, eller om en överföring stoppas innan den är slutförd, eller vid andra omständigheter för återställning, skall rörelsesensorn återställas kontrollerat.

4.6.6 *Datatillgänglighet*

RLB_111 Rörelsesensorn skall se till att tillträde till resurser erhålls om så krävs och att resurser inte begärs eller behålls i onödan.

4.6.7 *Flera tillämpningar*

RLB_112 Om rörelsesensorn tillhandahåller andra tillämpningar än färdskrivartillämpningen, skall alla tillämpningar hållas fysiskt och/eller logiskt åtskilda från varandra. Dessa tillämpningar får inte dela säkerhetsdata. Endast en uppgift skall vara aktiv åt gången.

4.7 ***Utbyte av data***

DEX_101 Rörelsesensorn skall exportera rörelsedata till fordonsenheten med tillhörande säkerhetsattribut, så att fordonsenheten kan verifiera dess integritet och autenticitet.

4.8 ***Kryptografiskt stöd***

Kraven i detta stycke är bara tillämpliga vid behov, beroende på de säkerhetsmekanismer som används och tillverkarens lösningar.

CSP_101 All kryptering som utförs av rörelsesensorn skall ske i överensstämmelse med en specificerad algoritm och en specificerad nyckelstorlek.

CSP_102 Om rörelsesensorn genererar kryptografiska nycklar skall det ske i överensstämmelse med specificerade algoritmer för generering av kryptografiska nycklar och specificerade storlekar på de kryptografiska nycklarna.

CSP_103 Om rörelsesensorn distribuerar kryptografiska nycklar skall det ske i överensstämmelse med specificerade metoder för distribution av nycklar.

CSP_104 Om rörelsesensorn har tillträde till kryptografiska nycklar skall det ske i överensstämmelse med specificerade metoder för tillträde till kryptografiska nycklar.

CSP_105 Om rörelsesensorn förstör kryptografiska nycklar skall det ske i överensstämmelse med specificerade metoder för förstöring av kryptografiska nycklar.

5. **Definition av säkerhetsmekanismer**

Säkerhetsmekanismerna, som utför rörelsesensorns säkerhetsfunktioner, skall definieras av tillverkaren av rörelsesensorer.

6. **Säkerhetsmekanismernas minsta tillåtna styrka**

Den minsta tillåtna styrkan hos rörelsesensorns säkerhetsmekanismer är High, enligt definition i referens ITSEC (kriterier för utvärdering av informationsteknologisk säkerhet).

7. **Garantinivå**

Målgarantinivån för rörelsesensorn är ITSEC-nivå E3, enligt definition i referens ITSEC (kriterier för utvärdering av informationsteknologisk säkerhet).

8. **Grund**

Följande matriser ger en logisk grund för säkerhetsfunktionerna genom att visa

— vilka säkerhetsfunktioner eller förfaranden som motverkar vilka hot,

— vilka säkerhetsfunktioner som uppfyller vilka mål för IT-säkerhet.

	Threats											IT Objectives					
	Access	Faults	Tests	Design	Environment	Hardware	Mechanical_Origin	Motion_Data	Power_Supply	Security_Data	Software	Stored_Data	Access	Audit	Authentication	Processing	Reliability	Secured_Data_Exchange
Physical Personnel Procedural means																		
Development		x	x	x														
Manufacturing			x	x														
Delivery						x					x	x						
Security Data Generation										x								
Security Data Transport										x								
Approved Workshops							x											
Mechanical interface							x											
Regular Inspection						x	x		x		x							
Law enforcement controls					x	x	x		x	x	x							
Software Upgrades											x							
Security Enforcing Functions																		
Identification and authentication																		
UIA_101 Entities identification	x							x					x		x			x
UIA_102 Entities identity	x												x		x			
UIA_103 VU identity														x				
UIA_104 Entities authentication	x							x					x		x			x
UIA_105 re-authentication	x							x					x		x			x
UIA_106 Unforgeable authentication	x							x					x		x			
UIA_107 Authentication failure								x						x			x	
Access control																		
ACC_101 Access control policy	x									x		x	x					
ACC_102 Motion sensor ID												x	x					

	Threats												IT Objectives					
	Access	Faults	Tests	Design	Environment	Hardware	Mechanical_Origin	Motion_Data	Power_Supply	Security_Data	Software	Stored_Data	Access	Audit	Authentication	Processing	Reliability	Secured_Data_Exchange
ACC_103 User data												x	x					
ACC_104 Security Data										x		x	x					
ACC_105 File structure and access conditions	x									x		x	x					
Accountability																		
ACT_101 Motion sensor ID data														x				
ACT_102 Pairing data														x				
ACT_103 Accountability data														x				
Audit																		
AUD_101 Audit records														x				
AUD_102 Audit events list	x				x	x						x		x				
AUD_103 Audit data														x				
AUD_104 Audit tools														x				
AUD_105 Audit records storage														x				
Accuracy																		
ACR_101 Information flow control policy								x								x	x	
ACR_102 Internal transfers																x	x	
ACR_103 Internal transfers														x				
ACR_104 Stored data integrity												x					x	
ACR_105 Stored data integrity												x		x				
Reliability																		
RLB_101 Manufacturing tests			x	x													x	
RLB_102 Self tests		x				x			x		x						x	
RLB_103 Self tests						x			x		x			x				
RLB_104 Software analysis				x							x						x	
RLB_105 Software input											x					x	x	
RLB_106 Case opening				x	x	x				x	x	x					x	
RLB_107 Hardware sabotage						x											x	
RLB_108 Hardware sabotage						x								x				
RLB_109 Power supply interruptions									x								x	
RLB_110 Reset		x															x	
RLB_111 Data Availability																x	x	
RLB_112 Multiple Applications																	x	
Data exchange																		
DEX_101 Secured motion data export								x										x
Cryptographic support																		
CSP_101 Algorithms																	x	x
CSP_102 key generation																	x	x
CSP_103 key distribution																	x	x
CSP_104 key access																	x	x
CSP_105 key destruction																	x	x

ALLMÄNT SÄKERHETSMÅL FÖR FORDONSENHETER

1. **Inledning**

Här beskrivs fordonsenheten, de hot den skall kunna motverka och de säkerhetsmål den skall uppnå. Vidare specificeras de säkerhetsfunktioner som krävs. Här anges erfordrad minsta tillåtna styrka hos säkerhetsmekanismer och erfordrad garantinivå för utveckling och evaluering.

De krav som anges här är desamma som i huvudtexten i bilaga I B. För att det skall bli lättare att läsa förekommer ibland dubblering mellan kraven i huvudtexten i bilaga I B och i säkerhetsmålen. Vid tvetydighet mellan ett krav i säkerhetsmålen och ett krav i huvudtexten i bilaga I B som avses i detta krav i säkerhetsmålen skall kravet i huvudtexten i bilaga I B gälla.

De krav i huvudtexten i bilaga I B som inte anges i säkerhetsmålen omfattas inte av säkerhetsfunktionerna.

Hot, mål, förfaranden och specifikationer av säkerhetsfunktioner har fått en unik märkning för att underlätta spårning till utvecklings- och evalueringsdokument.

2. **Förkortningar, definitioner och hänvisningar**

2.1 ***Förkortningar***

PIN	Personal Identification Number – Personligt identifieringsnummer
ROM	Read Only Memory – Minne för enbart avläsning
SEF	Security Enforcing Function – Säkerhetsfunktion
TBD	To Be Defined – Skall definieras
TOE	Target Of Evaluation – Evalueringsobjekt
VU	Vehicle Unit – Fordonsenhet

2.2 ***Definitioner***

Digital färdskrivare	Färdskrivare
Rörelsedata	De data som utbyts med rörelsesensorn om hastighet och tillryggalagd sträcka
Fysiskt åtskilda delar	Fysiska komponenter i fordonsenheten som fördelats i fordonet, i motsats till fysiska komponenter som samlats i fordonsenhetens kåpa
Säkerhetsdata	De särskilda data som krävs för att stödja säkerhetsfunktioner (exempelvis kryptografiska nycklar)
System	Utrustning, personer eller organisationer som har något samband med färdskrivaren
Användare	Användare skall förstås som personer som använder utrustningen. Sedvanliga användare av fordonsenheten är förare, kontrollanter, verkstäder och företag
Användardata	Alla data, utom säkerhetsdata, som registreras av eller lagras i fordonsenheten, och som krävs enligt kapitel III.12

2.3 ***Referenser***

ITSEC	ITSEC Information Technology Security Evaluation Criteria 1991 (kriterier för utvärdering av informationsteknologisk säkerhet)

3. **Produkternas syfte**

3.1 ***Beskrivning av fordonsenheten och användningsmetod***

Fordonsenheten skall installeras i vägtransportfordon. Dess syfte är att registrera, lagra, visa, skriva ut och mata ut data om föraraktiviteter.

Den är ansluten till en rörelsesensor med vilken den utbyter data om fordonsrörelser.

Användare identifierar sig för fordonsenheten med hjälp av färdskrivarkort.

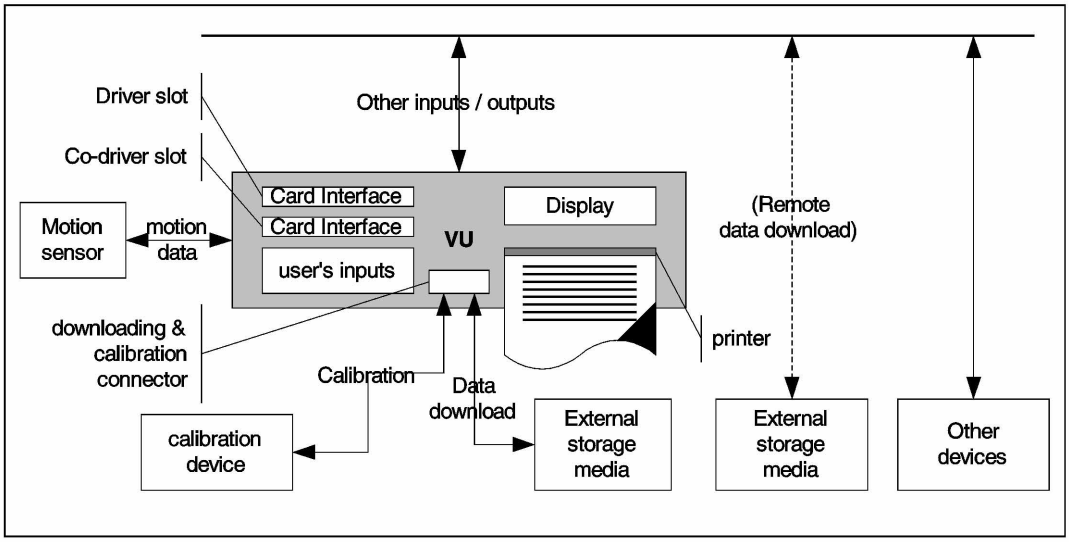
Fordonsenheten registrerar och lagrar data om användarnas aktiviteter i sitt dataminne och den registrerar data om användarnas aktiviteter på färdskrivarkort.

Fordonsenheten matar ut data till display, skrivare och externa anordningar.

Fordonsenhetens driftsmiljö när den är installerad i ett fordon beskrivs i följande figur:

Figur 2

Fordonsenhetens driftsmiljö



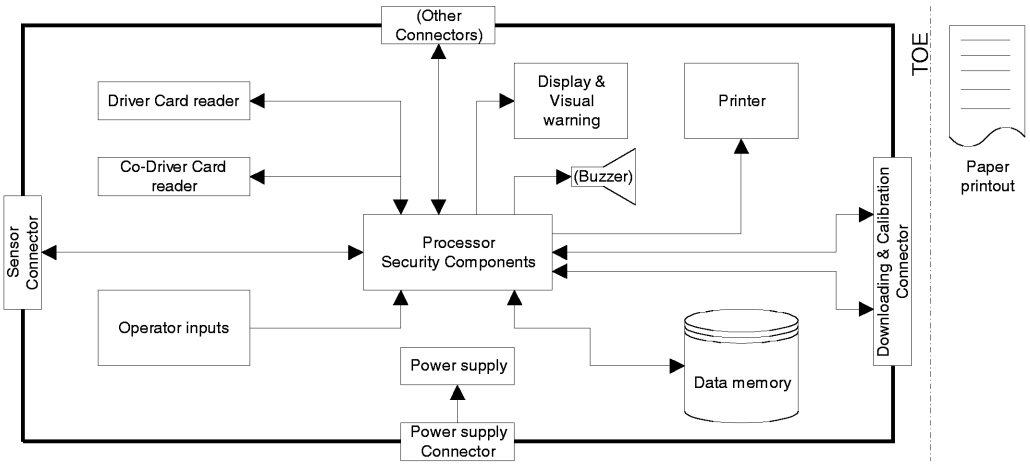
Fordonsenhetens allmänna egenskaper, funktioner och driftlägen beskrivs i kapitel II i bilaga I B.

Funktionskraven för fordonsenheten anges i kapitel III i bilaga I B.

I följande figur beskrivs en typisk fordonsenhet:

Figur 3

Typisk fordonsenhet (…) valbart



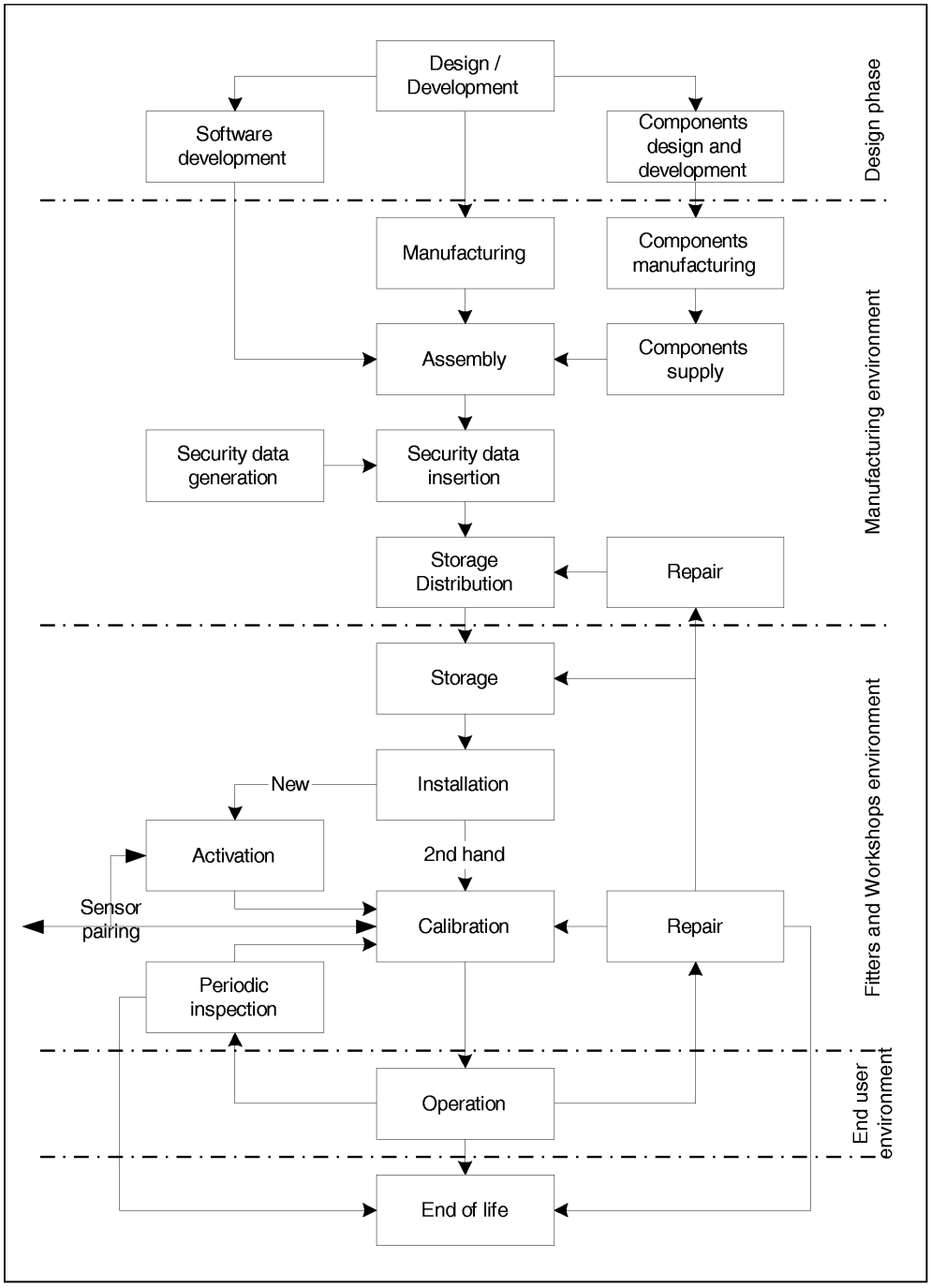
Observera att pappersdokumentet när det väl har producerats inte är en del av evalueringsobjektet, även om skrivarmekanismen är det.

3.2 ***Fordonsenhetens livscykel***

I följande figur beskrivs den typiska livscykeln för en fordonsenhet:

Figur 4

Typisk livscykel för en fordonsenhet



3.3 ***Hot***

I detta stycke beskrivs de hot som en fordonsenhet kan komma att utsättas för.

3.3.1 *Hot med avseende på kontrollbestämmelser för identifiering och tillträde*

T.Access	Användare skulle kunna försöka få tillträde till funktioner som inte är tillåtna för dem (exempelvis förare som får tillträde till kalibreringsfunktionen)
T.Identification	Användare skulle kunna försöka använda flera eller inga identifieringar

3.3.2 *Hot med avseende på konstruktion*

T.Faults	Fel i maskinvara, programvara och kommunikationsförfaranden skulle kunna utsätta fordonsenheten för oförutsedda förhållanden som äventyrar dess säkerhet
T.Tests	Användning av icke-validerade provningssätt eller av befintliga bakdörrar skulle kunna äventyra fordonsenhetens säkerhet
T.Design	Användare skulle kunna försöka tillgodogöra sig olovliga kunskaper om konstruktionen antingen från tillverkarens material (genom stöld, mutor, …) eller genom baklängeskonstruktion (reverse engineering)

3.3.3 *Hot med avseende på drift*

T.Calibration_Parameters	Användare skulle kunna försöka använda felkalibrerad utrustning (genom att ändra kalibreringsdata, eller genom organisatoriska svagheter)
T.Card_Data_Exchange	Användare skulle kunna försöka ändra data när de utbyts mellan fordonsenhet och färdskrivarkort (tillägg, ändring, borttagande, återspelning av signal)
T.Clock	Användare skulle kunna försöka ändra den interna klockan
T.Environment	Användare skulle kunna äventyra säkerheten i fordonsenheten genom miljöpåverkan (termisk, elektromagnetisk, optisk, kemisk, mekanisk, …)
T.Fake_Devices	Användare skulle kunna försöka ansluta förfalskade anordningar (rörelsesensor, smartkort) till fordonsenheten
T.Hardware	Användare skulle kunna försöka ändra fordonsenhetens maskinvara
T.Motion_Data	Användare skulle kunna försöka ändra fordonets rörelsedata (tillägg, ändring, borttagande, återspelning av signal)
T.Non_Activated	Användare skulle kunna använda icke-aktiverad utrustning
T.Output_Data	Användare skulle kunna försöka ändra utmatade data (utskrift, visning eller överföring)
T.Power_Supply	Användare skulle kunna försöka omintetgöra säkerhetsmålen för fordonsenheter genom att ändra (avbryta, minska, öka) strömtillförseln till dem
T.Security_Data	Användare skulle kunna försöka att få olovliga kunskaper om säkerhetsdata vid generering av säkerhetsdata eller transport eller lagring av dem i färdskrivaren
T.Software	Användare skulle kunna försöka ändra fordonsenhetens programvara
T.Stored_Data	Användare skulle kunna försöka ändra lagrade data (säkerhetsdata eller användardata)

3.4 ***Säkerhetsmål***

Det digitala färdskrivarsystemets huvudsakliga säkerhetsmål är följande:

O.Main	De data som skall kontrolleras av kontrollmyndigheterna skall finnas tillgängliga och till fullo och korrekt återspegla de kontrollerade förarnas och fordonens aktiviteter med avseende på körning, arbete, tillgänglighet, viloperioder och fordonets hastighet.

Säkerhetsmålen för fordonsenheter, som bidrar till det övergripande säkerhetsmålet, är följande:

O.VU_Main	De data som skall mätas, registreras och sedan kontrolleras av kontrollmyndigheterna skall finnas tillgängliga och korrekt återspegla de kontrollerade förarnas och fordonens aktiviteter med avseende på körning, arbete, tillgänglighet, viloperioder och fordonets hastighet.
O.VU_Export	Fordonsenheten skall kunna exportera data till externa lagringsmedia på ett sådant sätt att det går att kontrollera deras integritet och autenticitet.

3.5 ***Informationstekniska säkerhetsmål***

De särskilda IT-säkerhetsmålen för fordonsenheten, som bidrar till de övergripande säkerhetsmålen, är följande:

O.Access	Fordonsenheten skall kontrollera användares tillträde till funktioner och data.
O.Accountability	Fordonsenheten skall samla in korrekta spårbarhetsdata.
O.Audit	Fordonsenheten skall granska försök till att sänka systemets säkerhet och bör spåra dem till berörda användare.
O.Authentication	Fordonsenheten skall autentisera användare och anslutna enheter (när en säker kanal behöver upprättas mellan två enheter).
O.Integrity	Fordonsenheten skall bibehålla integriteten hos lagrade data.
O.Output	Fordonsenheten skall se till att utmatade data korrekt återspeglar uppmätta eller lagrade data.
O.Processing	Fordonsenheten skall se till att behandlingen av inmatade data för att erhålla användardata är korrekt.
O.Reliability	Fordonsenheten skall fungera tillförlitligt.
O.Secured_Data_Exchange	Fordonsenheten skall säkra utbytet av data med rörelsesensor och färdskrivarkort.

3.6 ***Fysiska förfaranden, personalförfaranden och övriga förfaranden***

Här beskrivs de fysiska förfaranden, personalförfaranden och övriga förfaranden som bidrar till fordonsenhetens säkerhet.

3.6.1 *Utrustningens konstruktion*

M.Development	De som utvecklar fordonsenheter skall se till att ansvarsfördelningen vid utvecklingsarbetet görs på ett sätt som upprätthåller IT-säkerheten.
M.Manufacturing	Tillverkare av fordonsenheter skall se till att ansvarsfördelningen under tillverkning görs på ett sätt varvid IT-säkerheten upprätthålls, och att fordonsenheten under tillverkning skyddas mot fysisk åverkan som kan äventyra IT-säkerheten.

3.6.2 *Leverans och aktivering av utrustning*

M.Delivery	Tillverkare av fordonsenheter och fordon samt montörer eller verkstäder skall se till att hanteringen av icke aktiverade fordonsenheter sker på ett sådant sätt att fordonsenhetens säkerhet upprätthålls
M.Activation	Fordonstillverkare och montörer skall aktivera fordonsenheten efter installering av den, innan fordonet lämnar den anläggning där installationen utfördes

3.6.3 *Generering och leverans av säkerhetsdata*

M.Sec_Data_Generation	Algoritmer för generering av säkerhetsdata får endast vara tillgängliga för auktoriserade och betrodda personer
M.Sec_Data_Transport	Säkerhetsdata skall genereras, transporteras och matas in i fordonsenheten på ett sådant sätt att dess sekretess och integritet skyddas

3.6.4 *Utfärdande av kort*

M.Card_Availability	Färdskrivarkort får endast finnas tillgängliga för och utfärdas till auktoriserade personer
M.Driver_Card_Uniqueness	Förare får ha endast ett giltigt förarkort åt gången
M.Card_Traceability	Utfärdandet av kort skall gå att spåra (vitlistor, svartlistor), och svartlistor skall användas vid säkerhetsgranskningar

3.6.5 *Installation, kalibrering och besiktning av färdskrivare*

M.Approved_Workshops	Installation, kalibrering och reparation av färdskrivare skall utföras av betrodda och godkända montörer eller verkstäder
M.Regular_Inpections	Färdskrivaren skall besiktigas och kalibreras regelbundet
M.Faithful_Calibration	Godkända montörer och verkstäder skall ange korrekta fordonsparametrar för färdskrivaren vid kalibrering

3.6.6 *Drift av utrustningen*

M.Faithful_Drivers	Förarna skall följa reglerna och uppföra sig ansvarsfullt (exempelvis använda sina förarkort, välja korrekta aktiviteter i de fall de väljs manuellt, …)

3.6.7 *Kontroll av att lagen upprätthålls*

M.Controls	Kontroller av att lagen upprätthålls skall utföras regelbundet och slumpvis och skall inbegripa säkerhetsgranskningar

3.6.8 *Uppgraderingar av programvara*

M.Software_Upgrade	Mjukvarurevisioner skall säkerhetscertifieras innan de får införas i en fordonsenhet

4. **Säkerhetsfunktioner**

4.1 ***Identifiering och autentisering***

4.1.1 *Identifiering och autentisering av rörelsesensor*

UIA_201 Fordonsenheten skall för varje användning kunna fastställa identiteten hos den rörelsesensor som den är ansluten till.

UIA_202 Rörelsesensorns identitet skall bestå av sensorns godkännandenummer och dess serienummer.

UIA_203 Fordonsenheten skall autentisera den rörelsesensor som den är ansluten till

— då rörelsesensorn ansluts,

— varje gång färdskrivaren kalibreras,

— då strömtillförseln återupptas.

Autentiseringen skall vara ömsesidig och utlösas av fordonsenheten.

UIA_204 Fordonsenheten skall regelbundet (perioden skall definieras av tillverkaren, dock minst en gång per timme) återidentifiera och återautentisera den rörelsesensor som den är ansluten till, och se till att den rörelsesensor som identifierades vid den senaste kalibreringen av färdskrivaren inte har ändrats.

UIA_205 Fordonsenheten skall upptäcka och förebygga användning av autentiseringsdata som har kopierats och återspelats.

UIA_206 Efter det att (skall definieras av tillverkaren, dock högst 20) misslyckade autentiseringsförsök i rad har upptäckts och/eller efter att ha upptäckt att rörelsesensorns identitet har ändrats utan tillstånd (dvs. ej vid kalibrering av färdskrivaren) skall säkerhetsfunktionerna

— generera en registrering om granskning av händelsen,

— varna användaren,

— fortsätta att godta och använda okrypterade rörelsedata som sänds av rörelsesensorn.

4.1.2 *Identifiering och autentisering av användare*

UIA_207 Fordonsenheten skall ständigt och selektivt spåra två användares identiteter, genom att övervaka de färdskrivarkort som sätts i förarens kortplats respektive medförarens kortplats i färdskrivaren.

UIA_208 Användaridentiteten skall bestå av följande:

— En användargrupp:

  — DRIVER (förare) (förarkort)

  — CONTROLLER (kontrollant) (kontrollkort)

  — WORKSHOP (verkstad) (verkstadskort)

  — COMPANY (företag) (företagskort)

  — UNKNOWN (okänd) (inget kort isatt)

— en användaridentifiering, bestående av

  — kod för den medlemsstat som utfärdat kortet och av kortnumret,

  — UNKNOWN (okänd) om användargruppen är UNKNOWN (okänd).

Okända (UNKNOWN) identiteter kan vara indirekt eller direkt kända.

UIA_209 Fordonsenheten skall autentisera sina användare då kortet sätts i.

UIA_210 Fordonsenheten skall återautentisera sina användare

— då strömtillförseln återupptas,

— regelbundet eller efter det att särskilda händelser har inträffat (skall definieras av tillverkare, dock minst en gång per dag).

UIA_211 Autentiseringen skall utföras genom att det bevisas att det isatta kortet är ett giltigt färdskrivarkort, med säkerhetsdata som endast systemet kan fördela. Autentiseringen skall vara ömsesidig och utlösas av fordonsenheten.

UIA_212 Utöver ovanstående skall verkstäder autentisera sig med hjälp av en PIN-kod. PIN-koderna skall bestå av minst fyra tecken.

Obs: Om PIN-koden överförs till fordonsenheten från en utrustning som är belägen utanför men i närheten av fordonsenheten, behöver PIN-sekretessen inte skyddas vid överföringen.

UIA_213 Fordonsenheten skall upptäcka och förebygga användning av autentiseringsdata som har kopierats och återspelats.

UIA_214 Efter det att fem misslyckade autentiseringsförsök i rad har upptäckts skall säkerhetsfunktionerna

— generera en registrering om granskning av händelsen,

— varna användaren,

— anta att användaren är okänd (UNKNOWN), och att kortet är ogiltigt (definition z och krav 007).

4.1.3 *Identifiering och autentisering av fjärranslutet företag*

Kapacitet för fjärranslutet företag är frivillig. Detta stycke skall därför endast tillämpas om denna funktion används.

UIA_215 Vid varje interaktion med ett fjärranslutet företag, skall fordonsenheten kunna fastställa företagets identitet.

UIA_216 Det fjärranslutna företagets identitet skall bestå av koden för den medlemsstat som utfärdat dess företagskort och numret på dess företagskort.

UIA_217 Fordonsenheten skall autentisera det fjärranslutna företaget innan den tillåter någon dataexport dit.

UIA_218 Autentiseringen skall utföras genom att det bevisas att företaget äger ett giltigt förarkort, med säkerhetsdata som endast systemet kan fördela.

UIA_219 Fordonsenheten skall upptäcka och förebygga användning av autentiseringsdata som har kopierats och återspelats.

UIA_220 Efter det att fem misslyckade autentiseringsförsök i rad har upptäckts skall fordonsenheten

— varna det fjärranslutna företaget.

4.1.4 *Identifiering och autentisering av förvaltningsanordning*

Tillverkare av fordonsenheter får använda särskilda anordningar för ytterligare funktioner för förvaltning av fordonsenheter (exempelvis uppgradering av programvara, omladdning av säkerhetsdata, …). Detta stycke skall därför endast tillämpas om denna funktion används.

UIA_221 Vid varje interaktion med en förvaltningsanordning, skall fordonsenheten kunna fastställa anordningens identitet.

UIA_222 Innan någon ytterligare interaktion tillåts skall fordonsenheten autentisera förvaltningsanordningen.

UIA_223 Fordonsenheten skall upptäcka och förebygga användning av autentiseringsdata som har kopierats och återspelats.

4.2 ***Tillträdeskontroll***

Tillträdeskontroller ser till att informationen läses från, skapas i, eller ändras till evalueringsobjekt enbart av dem som är auktoriserade att göra detta.

Observera att de användardata som registreras av fordonsenheten inte är konfidentiella, även om de kan vara känsliga i privatlivs- eller kommersiellt hänseende. Därför omfattas funktionskravet som kopplas till tillträdesrättigheter för läsning av data (krav 011) inte av någon säkerhetsfunktion.

4.2.1 *Bestämmelser om tillträdeskontroll*

ACC_201 Fordonsenheten skall hantera och kontrollera tillträdesrättigheter till funktioner och data.

4.2.2 *Tillträdesrättigheter till funktioner*

ACC_202 Fordonsenheten skall upprätthålla reglerna för val av driftläge (krav 006 till 009).

ACC_203 Fordonsenheten skall använda driftläget för att upprätthålla reglerna för kontroll av tillträde till funktioner (krav 010).

4.2.3 *Tillträdesrättigheter till data*

ACC_204 Fordonsenheten skall upprätthålla reglerna för identifiering av fordonsenhet för tillträde till dataskrivning (krav 076).

ACC_205 Fordonsenheten skall upprätthålla reglerna för tillträdesrättigheter till skrivning av data vid identifiering av hopkopplade rörelsesensorer (krav 79).

ACC_206 Efter det att fordonsenheten har aktiverats skall den se till att kalibreringsdata kan matas in i fordonsenheten och lagras i dess dataminne endast i kalibreringsläge (krav 154 och 156).

ACC_207 Efter det att fordonsenheten har aktiverats skall den upprätthålla tillträdesreglerna för skrivning och borttagning av kalibreringsdata (krav 097).

ACC_208 Efter det att fordonsenheten aktiverats skall den se till att tidsinställningsdata kan matas in i fordonsenheten och lagras i dess dataminne endast i kalibreringsläge (detta krav skall inte tillämpas på de små tidsjusteringar som tillåts enligt krav 157 och 158).

ACC_209 Efter det att fordonsenheten har aktiverats skall den upprätthålla tillträdesreglerna för skrivning och borttagning av tidsinställningsdata (krav 100).

ACC_210 Fordonsenheten skall upprätthålla lämpliga läs- och skrivrättigheter när det gäller tillträde till säkerhetsdata (krav 080).

4.2.4 *Filstruktur och tillträdesvillkor*

ACC_211 Strukturen på tillämpningsfiler och datafiler och tillträdesrättigheter skall upprättas vid tillverkningen, och sedan låsas från all eventuell ändring eller borttagning.

4.3 ***Spårbarhet***

ACT_201 Fordonsenheten skall se till att förarna är spårbara för sina aktiviteter (krav 081, 084, 087, 105a, 105b, 109 och 109a).

ACT_202 Fordonsenheten skall lagra permanenta identifieringsdata (krav 075).

ACT_203 Fordonsenheten skall se till att verkstäderna är spårbara för sina aktiviteter (krav 098, 101 och 109).

ACT_204 Fordonsenheten skall se till att kontrollanterna är spårbara för sina aktiviteter (krav 102, 103 och 109).

ACT_205 Fordonsenhetens skall registrera vägmätardata (krav 090) och detaljerade hastighetsdata (krav 093).

ACT_206 Fordonsenheten skall se till att de användardata som berör krav 081-093 och 102-105b inte ändras när de väl har registrerats, utom när de blir de data som lagrats längst och därför skall ersättas med nya data.

ACT_207 Fordonsenheten skall se till att den inte ändrar data som redan har lagrats på ett färdskrivarkort (krav 109 och 109a) utom för att ersätta äldsta data med nya data (krav 110) eller i det fall som beskrivs i anmärkningen till tillägg 1 punkt 2.1.

4.4 ***Granskning***

Granskning krävs endast vid eventuella försök till manipulering eller säkerhetsöverträdelse. Granskning krävs inte för normalt utövande av rättigheter även om det är relevant för säkerheten.

AUD_201 Fordonsenheten skall, vid händelser som omintetgör fordonsenhetens säkerhet, registrera dessa händelser med tillhörande data (krav 094, 096 och 109).

AUD_202 Följande händelser påverkar fordonsenhetens säkerhet:

— Följande försök till säkerhetsöverträdelse:

  — Fel vid autentisering av rörelsesensor.

  — Fel vid autentisering av färdskrivarkort.

  — Icke auktoriserad ändring av rörelsesensor.

  — Integritetsfel hos inmatade kortdata.

  — Integritetsfel hos lagrade användardata.

  — Fel vid överföring av interna data.

  — Ej auktoriserad öppning av kåpan.

  — Maskinvarusabotage.

— Senaste kortanvändning ej korrekt avslutad.

— Händelsen 'fel i rörelsedata'.

— Händelsen 'avbrott av strömtillförsel'.

— Internt fel i fordonsenheten (VU).

AUD_203 Fordonsenheten skall upprätthålla reglerna för lagring av granskningsregistreringar (krav 094 och 096).

AUD_204 Fordonsenheten skall i sitt dataminne lagra de granskningsregistreringar som rörelsesensorn registrerar.

AUD_205 Det skall gå att skriva ut, visa och överföra granskningsregistreringar.

4.5 ***Återanvändning av objekt***

REU_201 Fordonsenheten skall se till att tillfälliga lagringsobjekt kan återanvändas utan att detta medför otillåtliga informationsflöden.

4.6 ***Korrekthet***

4.6.1 *Bestämmelser om kontroll av informationsflöden*

ACR_201 Fordonsenheten skall se till att användardata som berör krav 081, 084, 087, 090, 093, 102, 104, 105, 105a och 109 endast kan behandlas från följande inmatningskällor:

— Data om fordonsrörelser.

— Fordonsenhetens realtidsklocka.

— Kalibreringsparametrar för färdskrivaren.

— Färdskrivarkort.

— Användarnas inmatade data.

ACR_201a Fordonsenheten skall se till att de användardata som berör krav 109a endast kan tillgås för perioden senaste urtagning av kort - aktuell isättning (krav 050a).

4.6.2 *Interna dataöverföringar*

Kraven i detta stycke skall endast tillämpas om fordonsenheten använder sig av fysiskt åtskilda delar.

ACR_202 Om data överförs mellan fysiskt åtskilda delar i fordonsenheten skall de skyddas mot ändringar.

ACR_203 Om ett dataöverföringsfel upptäcks vid en intern överföring skall överföringen upprepas och säkerhetsfunktionerna generera en granskningsregistrering av händelsen.

4.6.3 *Integritet hos lagrade data*

ACR_204 Fordonsenheten skall kontrollera de användardata som finns lagrade i dataminnet för att upptäcka integritetsfel.

ACR_205 Om ett integritetsfel för lagrade användardata upptäcks skall säkerhetsfunktionerna generera en granskningsregistrering.

4.7 ***Funktionell pålitlighet***

4.7.1 *Provningar*

RLB_201 Alla kommandon, åtgärder, eller provningspunkter som är specifika för provningen när fordonsenheten tillverkas skall avaktiveras och tas bort innan den aktiveras. Det skall inte vara möjligt att återställa dem för senare användning.

RLB_202 Fordonsenheten skall utföra självprovningar vid initialstart och vid normal drift för att verifiera att den fungerar korrekt. Fordonsenhetens självprovning skall inbegripa en kontroll av integriteten hos säkerhetsdata och av integriteten hos lagrad exekverbar kod (om den inte finns i ROM).

RLB_203 Vid upptäckt av ett inre fel under självprovningen skall säkerhetsfunktionen

— generera en granskningsregistrering (förutom i kalibreringsläge (internt fel i fordonsenheten)),

— bevara integriteten hos lagrade data.

4.7.2 *Programvara*

RLB_204 Det skall inte gå att i fält analysera eller avlusa programvara efter det att fordonsenheten har aktiverats.

RLB_205 Inmatade data från externa källor skall inte godtas som exekverbar kod.

4.7.3 *Fysiskt skydd*

RLB_206 Om fordonsenheten är utformad så att den kan öppnas, skall den upptäcka alla öppningar av kåpan, utom i kalibreringsläge, även utan extern strömtillförsel under minst sex månader. I detta fall skall säkerhetsfunktionerna generera en granskningsregistrering (som får genereras och lagras efter det att strömtillförseln återupptagits).

Om fordonsenheten är utformad så att den inte kan öppnas, skall den vara utformad så att försök till fysisk manipulering lätt kan upptäckas (exempelvis genom visuell besiktning).

RLB_207 Efter aktivering skall fordonsenheten upptäcka angivet (att definieras av tillverkaren) maskinvarusabotage.

RLB_208 I fallet ovan skall säkerhetsfunktionerna generera en granskningsregistrering och fordonsenheten skall (skall definieras av tillverkaren).

4.7.4 *Avbrott av strömtillförseln*

RLB_209 Fordonsenheten skall upptäcka avvikelser från angivna värden för strömtillförseln, inbegripet avbrott.

RLB_210 I ovanstående fall skall säkerhetsfunktionen

— generera en granskningsregistrering (förutom i kalibreringsläge),

— upprätthålla fordonsenhetens säkerhet,

— upprätthålla säkerhetsfunktionerna, med avseende på de komponenter eller processer som fortfarande är i drift,

— bevara integriteten hos lagrade data.

4.7.5 *Villkor för återställning*

RLB_211 Vid strömavbrott, eller om en överföring stoppas innan den är slutförd, eller vid andra omständigheter för återställning, skall fordonsenheten återställas kontrollerat.

4.7.6 *Datatillgänglighet*

RLB_212 Fordonsenheten skall se till att tillträde till resurser erhålls om så krävs och att resurser inte begärs eller behålls i onödan.

RLB_213 Fordonsenheten skall se till att kort inte ges tillbaka innan relevanta data har lagrats på dem (krav 015 och 016).

RLB_214 I fallet ovan skall säkerhetsfunktionerna generera en granskningsregistrering av händelsen.

4.7.7 *Flera tillämpningar*

RLB_215 Om fordonsenheten tillhandahåller andra tillämpningar än färdskrivartillämpningen, skall alla tillämpningar hållas fysiskt och/eller logiskt åtskilda från varandra. Dessa tillämpningar får inte dela säkerhetsdata. Endast en uppgift skall vara aktiv åt gången.

4.8 ***Utbyte av data***

Detta stycke handlar om dataöverföring mellan fordonsenhet och anslutna anordningar.

4.8.1 *Datautbyte med rörelsesensorn*

DEX_201 Fordonsenheten skall verifiera integritet och autenticitet hos rörelsedata som importeras från rörelsesensorn

DEX_202 Vid upptäckt av fel i integritet eller autenticitet hos rörelsedata skall säkerhetsfunktionerna

— generera en granskningsregistrering,

— fortsätta att använda importerade data

4.8.2 *Datautbyte med färdskrivarkort*

DEX_203 Fordonsenheten skall verifiera integritet och autenticitet hos data som importeras från färdskrivarkort.

DEX_204 Vid upptäckt av fel i integritet eller autenticitet hos kortdata skall fordonsenheten:

— generera en granskningsregistrering,

— inte använda dessa data.

DEX_205 Fordonsenheten skall exportera data till färdskrivarsmartkorten med tillhörande säkerhetsattribut, så att kortet kan verifiera dess integritet och autenticitet.

4.8.3 *Datautbyte med externa lagringsmedia (överföringsfunktionen)*

DEX_206 Fordonsenheten skall generera ursprungsbevis för de data som överförs till externa media.

DEX_207 Fordonsenheten skall kunna verifiera ursprungsbeviset för överförda data till mottagaren.

DEX_208 Fordonsenheten skall överföra data till externa lagringsmedia med tillhörande säkerhetsattribut, så att integritet och autenticitet hos överförda data kan kontrolleras.

4.9 ***Kryptografiskt stöd***

Kraven i detta stycke är bara tillämpliga vid behov, beroende på de säkerhetsmekanismer som används och tillverkarens lösningar.

CSP_201 All kryptering som utförs av fordonsenheten skall ske i överensstämmelse med en specificerad algoritm och en specificerad nyckelstorlek.

CSP_202 Om fordonsenheten genererar kryptografiska nycklar skall det ske i överensstämmelse med specificerade algoritmer för generering av kryptografiska nycklar och specificerade storlekar på de kryptografiska nycklarna.

CSP_203 Om fordonsenheten distribuerar kryptografiska nycklar skall det ske i överensstämmelse med specificerade metoder för distribution av nycklar.

CSP_204 Om fordonsenheten har tillträde till kryptografiska nycklar skall det ske i överensstämmelse med specificerade metoder för tillträde till kryptografiska nycklar.

CSP_205 Om fordonsenheten förstör kryptografiska nycklar skall det ske i överensstämmelse med specificerade metoder för förstörelse av kryptografiska nycklar.

5. **Definition av säkerhetsmekanismer**

Säkerhetsmekanismer som skall finnas specificeras i tillägg 11.

Alla andra säkerhetsmekanismer skall definieras av tillverkaren.

6. **Säkerhetsmekanismernas minsta tillåtna styrka**

Den minsta tillåtna styrkan hos fordonsenhetens säkerhetsmekanismer är High, enligt definition i referens ITSEC (kriterier för utvärdering av informationsteknologisk säkerhet).

7. **Garantinivå**

Målgarantinivån för fordonsenheten är ITSEC-nivå E3, enligt definition i referens ITSEC (kriterier för utvärdering av informationsteknologisk säkerhet).

8. **Grund**

Följande matriser ger en logisk grund för säkerhetsfunktionerna genom att visa

— vilka säkerhetsfunktioner eller förfaranden som motverkar vilka hot,

— vilka säkerhetsfunktioner som uppfyller vilka mål för IT-säkerhet.

	Threats																		IT Objectives								
	Access	Identification	Faults	Tests	Design	Calibration_Parameters	Card_Data_Exchange	Clock	Environment	Fake_Devices	Hardware	Motion_Data	Non_Activated	Output_Data	Power_Supply	Security_Data	Software	Stored_Data	Access	Accountability	Audit	Authentication	Integrity	Output	Processing	Reliability	Secured_Data_Exchange
Physical Personnel Procedural Means																											
Development			x	x	x																						
Manufacturing				x	x																						
Delivery													x														
Activation	x												x														
Security Data Generation																x											
Security Data Transport																x											
Card Availability		x																									
One Driver Card		x																									
Card Traceability		x																									
Approved Workshops						x		x																			
Regular Inspection Calibration						x		x				x	x		x												
Faithful workshops						x		x																			
Faithful drivers		x																									
Law enforcement controls		x				x		x	x		x		x		x			x	x								
Software Upgrade																		x									
Security Enforcing Functions																											
Identification and Authentication																											
UIA_201 Sensor identification										x		x										x					x
UIA_202 Sensor identity										x		x										x					x
UIA_203 Sensor authentication										x		x										x					x
UIA_204 Sensor re-identification and re-authentication										x		x										x					x
UIA_205 Unforgeable authentication										x		x										x					
UIA_206 Authentication failure										x		x									x					x	
UIA_207 Users identification	x	x								x									x			x					x
UIA_208 User identity	x	x								x									x			x					x
UIA_209 User authentication	x	x								x									x			x					x
UIA_210 User re-authentication	x	x								x									x			x					x
UIA_211 Authentication means	x	x								x									x			x					
UIA_212 PIN checks	x	x				x		x											x			x					
UIA_213 Unforgeable authentication	x	x								x									x			x					

	Threats																			IT Objectives								
	Access	Identification	Faults	Tests	Design	Calibration_Parameters	Card_Data_Exchange	Clock	Environment	Fake_Devices	Hardware	Motion_Data	Non_Activated	Output_Data	Power_Supply	Security_Data	Software	Stored_Data	Access	Accountability	Audit	Authentication	Integrity	Output	Processing	Reliability	Secured_Data_Exchange
UIA_214 Authentication failure	x	x								x											x							
UIA_215 Remote user identification	x	x																	x			x						x
UIA_216 Remote user identity	x	x																	x			x						
UIA_217 Remote user authentication	x	x																	x			x						x
UIA_218 Authentication means	x	x																	x			x						
UIA_219 Unforgeable authentication	x	x																	x			x						
UIA_220 Authentication failure	x	x																										
UIA_221 Management device Identification	x	x																	x			x						
UIA_222 Management device Authentication	x	x																	x			x						
UIA_223 Unforgeable authentication	x	x																	x			x						
Access Control																												
ACC_201 Access control policy	x					x		x								x		x	x									
ACC_202 Access rights to functions	x					x		x											x									
ACC_203 Access rights to functions	x					x		x											x									
ACC_204 VU ID																		x	x									
ACC_205 Connected sensor ID										x								x	x									
ACC_206 Calibration data	x					x												x	x									
ACC_207 Calibration data						x												x	x									
ACC_208 Time adjustment data								x										x	x									
ACC_209 Time adjustment data								x										x	x									
ACC_210 Security Data																x		x	x									
ACC_211 File structure and access conditions	x					x										x		x	x									
Accountability																												
ACT_201 Drivers accountability																				x								
ACT_202 VU ID data																				x	x							
ACT_203 Workshops accountability																				x								
ACT_204 Controllers accountability																				x								
ACT_205 Vehicle movement accountability																				x								
ACT_206 Accountability data modification																		x					x			x		
ACT_207 Accountability data modification																		x					x			x		

	Threats																		IT Objectives							
	Access	Identification	Faults	Tests	Design	Calibration_Parameters	Card_Data_Exchange	Clock	Environment	Fake_Devices	Hardware	Motion_Data	Non_Activated	Output_Data	Power_Supply		Security_Data	Software	Stored_Data	Access	Accountability	Audit	Authentication	Integrity	Output	Processing	Reliability	Secured_Data_Exchange
Audit																												
AUD_201 Audit records																						x						
AUD_202 Audit events list	x						x				x	x		x	x				x			x						
AUD_203 Audit records storage rules																						x						
AUD_204 Sensor audit records																						x						
AUD_205 Audit tools																						x						
Reuse																												
REU_201 Reuse																	x									x	x	
Accuracy																												
ACR_201 Information flow control policy						x			x		x															x	x	
ACR_202 Internal transfers														x											x	x	x	
ACR_203 Internal transfers														x								x						
ACR_204 Stored data integrity																			x				x			x		
ACR_205 Stored data integrity																			x			x						
Reliability																												
RLB_201 Manufacturing tests				x	x																					x		
RLB_202 Self tests			x								x				x			x									x	
RLB_203 Self tests											x				x			x				x						
RLB_204 Software analysis					x													x									x	
RLB_205 Software input																		x							x	x	x	
RLB_206 Case opening					x				x		x			x			x	x	x						x		x	
RLB_207 Hardware sabotage											x																x	
RLB_208 Hardware sabotage											x											x						
RLB_209 Power supply interruptions															x												x	
RLB_210 Power supply interruptions															x							x						
RLB_211 Reset			x																								x	
RLB_212 Data Availability																										x	x	
RLB_213 Card release																											x	
RLB_214 Card session not correctly closed																							x					
RLB_215 Multiple Applications																											x	
Data exchange																												
DEX_201 Secured motion data import												x																x
DEX_202 Secured motion data import												x							x									
DEX_203 Secured card data import							x																					x

	Threats																			IT Objectives								
	Access	Identification	Faults	Tests	Design	Calibration_Parameters	Card_Data_Exchange	Clock	Environment	Fake_Devices	Hardware	Motion_Data	Non_Activated	Output_Data	Power_Supply		Security_Data	Software	Stored_Data	Access	Accountability	Audit	Authentication	Integrity	Output	Processing	Reliability	Secured_Data_Exchange
DEX_204 Secured card data import							x															x						
DEX_205 Secured data export to cards							x																					x
DEX_206 Evidence of origin																								x	x			
DEX_207 Evidence of origin																								x	x			
DEX_208 Secured export to external media																								x	x			
Cryptographic support																												
CSP_201 Algorithms																											x	x
CSP_202 Key generation																											x	x
CSP_203 Key distribution																											x	x
CSP_204 Key access																											x	x
CSP_205 Key destruction																											x	x

ALLMÄNT SÄKERHETSMÅL FÖR FÄRDSKRIVARKORT

1. **Inledning**

Här beskrivs färdskrivarkortet, de hot det skall kunna motverka och de säkerhetsmål det skall uppnå. Vidare specificeras de säkerhetsfunktioner som krävs. Här anges erfordrad minsta tillåtna styrka hos säkerhetsmekanismer och erfordrad garnantinivå för utveckling och evaluering.

De krav som anges här är desamma som i huvudtexten i bilaga I B. För att det skall bli lättare att läsa förekommer ibland dubblering mellan kraven i huvudtexten i bilaga B och i säkerhetsmålen. Vid tvetydighet mellan ett krav i säkerhetsmålen och ett krav i bilaga I B som avses i detta krav i säkerhetsmålen skall kravet i huvudtexten i bilaga I B gälla.

De krav i huvudtexten i bilaga I B som inte anges i säkerhetsmålen omfattas inte av säkerhetsfunktionerna.

Ett färdskrivarkort är ett standardsmartkort med en särskild tillämpning för färdskrivare, och det skall uppfylla de aktuella säkerhetskrav med avseende på funktion och garanti som tillämpas på smartkort. Detta säkerhetsmål inbegriper därför endast de extra säkerhetskrav som behövs för färdskrivartillämpningen.

Hot, mål, förfaranden och specifikationer av säkerhetsfunktioner har fått en unik märkning för att underlätta spårning till utvecklings- och evalueringsdokument.

2. **Förkortningar, definitioner och hänvisningar**

2.1 ***Förkortningar***

IC	Integrated circuit – Integrerad krets (Elektronisk komponent avsedd att utföra behandlings- och/eller minnesfunktioner)
OS	Operating system – Operativsystem
PIN	Personal Identification Number – Personligt identifieringsnummer
ROM	Read Only Memory – Minne för enbart avläsning
SFP	Security Functions Policy – Bestämmelser för säkerhetsfunktioner
TBD	To be defined – Skall definieras
TOE	Target of Evaluation –Evalueringsobjekt
TSF	TOE Security Function – Evalueringsobjektets säkerhetsfunktion
VU	Vehicle Unit – Fordonsenhet

2.2 ***Definitioner***

Digital färdskrivare	Färdskrivare
Känsliga data	Data som lagras av ett färdskrivarkort och som behöver skyddas med avseende på integritet, icke-auktoriserad ändring och sekretess (där så är tillämpligt för säkerhetsdata). Känsliga data inbegriper säkerhetsdata och användardata
Säkerhetsdata	De särskilda data som krävs för att stödja säkerhetsfunktioner (exempelvis kryptografiska nycklar)
System	Utrustning, personer eller organisationer som har något samband med färdskrivaren
Användare	Alla enheter (mänsklig eller extern IT-enhet) utanför evalueringsobjektet som interagerar med evalueringsobjektet (utom vid användning i uttrycket 'användardata')

Användardata	Känsliga data som lagras på ett färdskrivarkort, förutom säkerhetsdata. Användardata inbegriper identifieringsdata och aktivitetsdata
Identifieringsdata	Identifieringsdata inbegriper data för identifiering av kort och kortinnehavare
Kortidentifieringsdata	Användardata för kortidentifiering i enlighet med krav 190, 191, 192, 194, 215, 231 och 235
Identifieringsdata för kortinnehavaren	Användardata för identifiering av kortinnehavare enligt krav 195, 196, 216, 232 och 236
Aktivitetsdata	Aktivitetsdata inbegriper data om kortinnehavarens aktiviteter, data om händelser och fel samt data om kontrollaktiviteter
Data om kortinnehavarens aktiviteter	Användardata om kortinnehavarens aktiviteter enligt krav 197, 199, 202, 212, 212a, 217, 219, 221, 226, 227, 229, 230a, 233 och 237
Data om händelser och fel	Användardata om händelser och fel enligt krav 204, 205, 207, 208 och 223
Data om kontrollaktiviteter	Användardata om kontroll av att lagen upprätthålls enligt krav 210 and 225

2.3 *Referenser*

ITSEC	ITSEC Information Technology Security Evaluation Criteria 1991 (kriterier för utvärdering av informationsteknologisk säkerhet)
IC PP	Smartcard Integrated Circuit Protection Profile – version 2.0 – utgåva september 1998. Registrerad hos franskt certifieringsorgan under nummer PP/9806
ES PP	Smartcard Integrated Circuit With Embedded Software Protection Profile – version 2.0 – utgåva juni 99. Registrerad hos franskt certifieringsorgan under nummer PP/9911

3. **Produkternas syfte**

3.1 *Beskrivning av färdskrivarkort och användningsmetod*

Ett färdskrivarkort är ett smartkort, enligt beskrivning i referens IC PP och referens ES PP, som har en tillämpning avsedd för användning med en färdskrivare.

Färdskrivarkortets grundläggande funktioner är att

— lagra data om identifiering av kort och kortinnehavare, vilka används av fordonsenheten för att identifiera kortinnehavaren, i enlighet med detta tillhandahålla funktioner och tillträdesrättigheter till data, och se till att kortinnehavaren kan hållas ansvarig för sina aktiviteter,

— lagra data om kortinnehavarens aktiviteter, data om händelser och fel samt data om kontrollaktiviteter med avseende på föraren.

Ett färdskrivarkort är därför avsett att användas i en fordonsenhets kortplats. Det får även användas av övriga kortläsare (exempelvis av en persondator), som skall ha fullständiga tillträdesrättigheter för läsning av alla användardata.

Under slutanvändningsfasen av färdskrivarkortets livscykel (fas 7 av livscykeln enligt referens ES PP), får endast fordonsenheter skriva användardata till kortet.

Funktionskraven för färdskrivarkort anges i huvudtexten i bilaga I B och i tillägg 2.

3.2 *Färdskrivarkortets livscykel*

Färdskrivarkortets livscykel överensstämmer med livscykeln för smartkort, som anges i referens ES PP.

3.3 ***Hot***

Utöver de allmänna hot för smartkort som förtecknas i referens ES PP och referens IC PP, kan färdskrivarkortet utsättas för följande hot:

3.3.1 *Slutliga syften*

Angripares slutliga syfte kommer att vara att ändra de användardata som finns lagrade inom evalueringsobjektet.

T.Ident_Data	En lyckad ändring av de identifieringsdata som finns lagrade i evalueringsobjektet (exempelvis typ av kort, kortets sista giltighetsdag eller data för identifiering av kortinnehavare) skulle möjliggöra orättmätig användning av evalueringsobjektet och utgöra ett stort hot mot systemets övergripande säkerhetsmål
T.Activity_Data	En lyckad ändring av de aktivitetsdata som finns lagrade i evalueringsobjektet skulle utgöra ett hot mot säkerheten i evalueringsobjektet
T.Data_Exchange	En lyckad ändring av aktivitetsdata (tillägg, borttagande, ändring) vid import eller export, skulle utgöra ett hot mot säkerheten i evalueringsobjektet.

3.3.2 *Angreppssätt*

Evalueringsobjektets funktioner kan angripas på följande sätt:

— Genom att man försöker erhålla olovliga kunskaper om utformningen av evalueringsobjektets maskinvara och programvara och i synnerhet om dess säkerhetsfunktioner eller säkerhetsdata. Olovliga kunskaper kan erhållas genom angrepp på konstruktörens eller tillverkarens material (stöld, mutor, …) eller genom direkt undersökning av evalueringsobjektet (fysisk undersökning, inferensanalys, …)

— Genom att man utnyttjar svagheter i utformning eller genomförande av evalueringsobjektet (utnyttjande av fel i maskinvara och programvara, överföringsfel, fel som uppstått i evalueringsobjektet på grund av miljöpåkänning, och utnyttjande av svagheter i säkerhetsfunktionerna, exempelvis i autentiseringsförfaranden, kontroll av datatillträde, kryptering,…)

— Genom att ändra evalueringsobjektet eller dess säkerhetsfunktioner genom fysiska, elektriska eller logiska angrepp eller kombinationer av dessa

3.4 ***Säkerhetsmål***

Hela det digitala färdskrivarsystemets huvudsakliga säkerhetsmål är följande:

O.Main	De data som skall kontrolleras av kontrollmyndigheterna skall finnas tillgängliga och till fullo och korrekt återspegla de kontrollerade förarnas och fordenensaktiviteter med avseende på körning, arbete, tillgänglighet, viloperioder och fordonets hastighet

De huvudsakliga säkerhetsmålen för evalueringsobjektet, som bidrar till detta övergripande säkerhetsmål, är följande:

O.Card_Identification_Data	Evalueringsobjektet skall bevara de data om identifiering av kort och kortinnehavare som lagras då kortet anpassas till användaren
O.Card_Activity_Storage	Evalueringsobjektet skall bevara användardata som fordonsenheter lagrar på kortet

3.5 ***Informationstekniska säkerhetsmål***

Utöver de allmänna säkerhetsmål för smartkort som förtecknas i referens ES PP och referens IC PP, bidrar följande specifika IT-säkerhetsmål för evalueringsobjektet till dess huvudsakliga säkerhetsmål under slutanvändningsfasen av dess livscykel:

O.Data_Access	Evalueringsobjektet skall begränsa tillträdesrättigheter till skrivning av användardata till autentiserade fordonsenheter
O.Secure_Communications	Evalueringsobjektet skall kunna stödja säkra kommunikationsprotokoll och kommunikationsförfaranden mellan kortet och kortplatsen när tillämpningen kräver detta

3.6 ***Fysiska förfaranden, personalförfaranden och övriga förfaranden***

De krav på fysiska förfaranden, personalförfaranden och övriga förfaranden som bidrar till evalueringsobjektets säkerhet förtecknas i referens ES PP och referens IC PP (kapitlen om säkerhetsmål för miljön).

4. **Säkerhetsfunktioner**

Här preciseras vissa av de tillåtna förfarandena, exempelvis tilldelning eller val av referens ES PP och här anges ytterligare funktionskrav för säkerhetsfunktionerna.

4.1 ***Överensstämmelse med skyddsprofiler***

CPP_301 Evalueringsobjektet skall överensstämma med referens IC PP.

CPP_302 Evalueringsobjektet skall överensstämma med referens ES PP enligt ytterligare förbättringar.

4.2 ***Identifiering och autentisering av användare***

Kortet skall identifiera den enhet i vilken det är isatt och känna av huruvida det är en autentiseral fordonsenhet. Kortet får exportera alla användardata oavsett vilken enhet det är anslutet till, utom kontrollkortet, som får exportera data om identifiering av kortinnehavare endast till autentiserade fordonsenheter (så att en kontrollant kan försäkra sig om att fordonsenheten inte är en förfalskning genom att se sitt namn på displayen eller utskrifterna).

4.2.1 *Användaridentifiering*

Tilldelning (FIA_UID.1.1) *Förteckning över TSF-förmedlade åtgärder*: inga.

Tilldelning (FIA_ATD.1.1) *Förteckning över säkerhetsattribut*:

— USER_GROUP: VEHICLE_UNIT, NON_VEHICLE_UNIT,

— USER_ID: Fordonets registreringsnummer (VRN) och kod för registrerande medlemsstat (USER_ID är känt endast för USER_GROUP = VEHICLE_UNIT).

4.2.2 *Användarautentisering*

Tilldelning (FIA_UAU.1.1) *Förteckning över TSF-förmedlade åtgärder*:

— Förar- och verkstadskort: Exportera användardata med säkerhetsattribut (funktion för överföring av kortdata).

— Kontrollkort: Exportera användardata utan säkerhetsattribut, utom data för identifiering av kortinnehavare.

UIA_301 Autentiseringen av en fordonsenhet skall utföras genom att det bevisas att den har säkerhetsdata som endast systemet kan distribuera.

Selection (FIA_UAU.3.1 und FIA_UAU.3.2): prevent.

Tilldelning (FIA_UAU.4.1) *Identifierade autentiseringsmekanismer*: vilken autentiseringsmekanism som helst.

UIA_302 Verkstadskortet skall tillhandahålla en ytterligare autentiseringsmekanism genom att kontrollera en PIN-kod (denna mekanism är utformad så att fordonsenheten skall kunna säkerställa kortinnehavarens identitet; den är inte avsedd att skydda innehållet i verkstadskortet).

4.2.3 *Autentiseringsfel*

Följande tilldelningar beskriver kortets reaktion för varje enskilt fel vid användarautentisering:

Tilldelning (FIA_AFL.1.1) *Nummer*: 1, *förteckning över autentiseringshändelser*: autentisering av en kortplats.

Tilldelning (FIA_AFL.1.2) *Förteckning över åtgärder*:

— varna ansluten enhet

— anta att användaren utgörs av NON_VEHICLE_UNIT.

Följande tilldelningar beskriver hur kortet reagerar vid fel hos den ytterligare mekanism för autentisering som krävs i UIA_302.

Tilldelning (FIA_AFL.1.1) *Nummer*: 5, *förteckning över autentiseringshändelser*: PIN-kontroller (verkstadskort).

Tilldelning (FIA_AFL.1.2) *Förteckning över åtgärder*:

— Varna ansluten enhet.

— Blockera förfarande för PIN-kontroll så att alla följande försök till PIN-kontroll misslyckas.

— Skall kunna ange orsaken till blockeringen för efterföljande användare.

4.3 ***Tillträdeskontroll***

4.3.1 *Bestämmelser om tillträdeskontroll*

Under slutanvändningsfasen av färdskrivarkortets livscykel skall det omfattas av en enda säkerhetsfunktionspolicy (SFP – Security Function Policy) för tillträdeskontroll, benämnd AC_SFP.

Tilldelning (FDP_ACC.2.1) *Tillträdeskontroll SFP*: AC_SFP.

4.3.2 *Funktioner för tillträdeskontroll*

Tilldelning (FDP_ACF.1.1) *Tillträdeskontroll SFP*: AC_SFP.

Tilldelning (FDP_ACF.1.1) *Namngiven grupp av säkerhetsattribut*: USER_GROUP.

Tilldelning (FDP_ACF.1.2) *Regler för tillträde bland kontrollerade subjekt och kontrollerade objekt med hjälp av kontrollerade åtgärder på kontrollerade objekt*:

— GENERAL_READ: Användardata kan läsas från evalueringsobjektet av alla användare, utom data för identifiering av kortinnehavare, som kan läsas från kontrollkort endast av VEHICLE_UNIT (fordonsenhet).

— IDENTIF_WRITE: Identifieringsdata får endast skrivas en gång och före slutet av fas 6 i kortets livscykel. Ingen användare får skriva eller ändra identifieringsdata under slutanvändningsfasen av kortets livscykel.

— ACTIVITY_WRITE: Aktivitetsdata får skrivas till evalueringsobjektet endast av VEHICLE_UNIT (fordonsenhet).

— SOFT_UPGRADE: Ingen användare får uppgradera evalueringsobjektets programvara.

— FILE_STRUCTURE: Filstruktur och tillträdesvillkor skall skapas före slutet av fas 6 i evalueringsobjektets livscykel och därefter låsas från all framtida ändring eller borttagning av alla användare.

4.4 ***Spårbarhet***

ACT_301 Evalueringsobjektet skall lagra permanenta identifieringsdata.

ACT_302 Det skall finnas en angivelse av när och var evalueringsobjektet användaranpassades. Denna angivelse skall inte gå att ändra.

4.5 ***Granskning***

Evalueringsobjektet skall övervaka de händelser som innebär en eventuell överträdelse av dess säkerhet.

Tilldelning (FAU_SAA.1.2) *Underavdelning av definierade granskningsbara händelser*:

— Fel vid autentisering av kortinnehavare (fem misslyckade PIN-kontroller i rad).

— Fel vid självprovning.

— Integritetsfel hos lagrade data.

— Integritetsfel hos ingående aktivitetsdata.

4.6 ***Korrekthet***

4.6.1 *Integritet hos lagrade data*

Tilldelning (FDP_SDI.2.2) *Åtgärder som skall vidtas*: Varna ansluten enhet.

4.6.2 *Grundläggande autentisering av data*

Tilldelning (FDP_DAU.1.1) *Förteckning över objekt eller informationstyper*: Aktivitetsdata.

Tilldelning (FDP_DAU.1.2) *Förteckning över subjekt*: Alla.

4.7 ***Funktionell pålitlighet***

4.7.1 *Provningar*

Selection (FPT_TST.1.1): Vid initialstart, regelbundet vid normal drift.

Märk: Vid den första starten betyder innan koden exekveras (och inte nödvändigtvis under förfarandet Answer To Reset).

RLB_301 Evalueringsobjektets självprovning skall inbegripa kontroll av integriteten hos all programvarukod som inte finns lagrade i ROM.

RLB_302 Vid upptäckt av ett självprovningsfel skall TSF varna ansluten enhet.

RLB_303 Efter det att OS-provningen har slutförts skall alla provningsspecifika kommandon och åtgärder avaktiveras eller tas bort. Det skall inte vara möjligt att åsidosätta dessa kontroller och återlagra dem för användning. Kommandon som endast avser ett skede i livscykeln får aldrig användas i ett annat skede.

4.7.2 *Programvara*

RLB_304 Det skall inte gå att i fält analysera, avlusa eller ändra evalueringsobjektets programvara.

RLB_305 Inmatade data från externa källor får inte godtas som exekverbar kod.

4.7.3 *Strömtillförsel*

RLB_306 Evalueringsobjektet skall upprätthålla säkerheten om strömtillförseln bryts av eller ändras.

4.7.4 *Villkor för återställning*

RLB_307 Om strömtillförseln avbryts (eller ändras) från evalueringsobjektet, eller om en överföring stoppas innan den är slutförd, eller vid andra omständigheter för återställning, skall evalueringsobjektet återställas kontrollerbart.

4.8 ***Utbyte av data***

4.8.1 *Datautbyte med en fordonsenhet*

DEX_301 Evalueringsobjektet skall verifiera integritet och autenticitet hos data som importeras från en fordonsenhet.

DEX_302 Vid upptäckt av fel i integriteten hos importerade data, skall evalueringsobjektet

— varna den enhet som sänder dessa data,

— inte använda dessa data.

DEX_303 Evalueringsobjektet skall exportera användardata till fordonsenheten med tillhörande säkerhetsattribut, så att fordonsenheten kan verifiera integritet och autenticitet hos mottagna data.

4.8.2 *Export av data till en icke-fordonsenhet (överföringsfunktion)*

DEX_304 Evalueringsobjektet skall kunna generera ursprungsbevis för de data som överförs till externa media.

DEX_305 Evalueringsobjektet skall kunna tillhandahålla en kapacitet att verifiera ursprungsbeviset för överförda data till mottagaren.

DEX_306 Evalueringsobjektet skall kunna överföra data till externa lagringsmedia med tillhörande säkerhetsattribut, så att integritet hos överförda data kan kontrolleras.

4.9 ***Kryptografiskt stöd***

CSP_301 Om TSF genererar kryptografiska nycklar skall det ske i överensstämmelse med specificerade algoritmer för generering av kryptografiska nycklar och specificerade storlekar på de kryptografiska nycklarna. Genererade krypterade sessionsnycklar skall ha ett begränsat *(skall definieras av tillverkaren, dock högst 240)* antal möjliga användningar.

CSP_302 Om TSF distribuerar kryptografiska nycklar skall det ske i överensstämmelse med specificerade metoder för distribution av kryptografiska nycklar.

5. **Definition av säkerhetsmekanismer**

Säkerhetsmekanismer som skall finnas specificeras i tillägg 11.

Alla andra säkerhetsmekanismer skall definieras av tillverkaren av evalueringsobjektet.

6. **Erfordrad minsta tillåtna styrka hos mekanismerna**
Minsta tillåtna styrka hos mekanismerna för färdskrivarkortet är High enligt referens ITSEC (kriterier för utvärdering av informationsteknologisk säkerhet).

7. **Garantinivå**
Målgarantinivån för färdskrivarkortet är ITSEC-nivå E3, enligt definition i referens ITSEC (kriterier för utvärdering av informationsteknologisk säkerhet).

8. **Grund**
Följande matriser ger en logisk grund för de ytterligare säkerhetsfunktionerna genom att visa

— vilka säkerhetsfunktioner som motverkar vilka hot,

— vilka säkerhetsfunktioner som uppfyller vilka mål för IT-säkerhet.

	Threats											IT Objectives								
	T.CLON*	T.DIS_ES2	T.T_ES	T.T_CMD	T.MOD_SOFT*	T.MOD_LOAD	T.MOD_EXE	T.MOD_SHARE	Ident_Data	Activity_Data	Data_Exchange	O.TAMPER_ES	O.CLON*	O.OPERATE*	O.FLAW*	O.DIS_MECHANISM2	O.DIS_MEMORY*	O.MOD_MEMORY*	Data_Access	Secured_Communications
UIA_301 Authentication means																			x	
UIA_302 PIN checks																			x	
ACT_301 Identification data																				
ACT_302 Personalisation date																				
RLB_301 Software integrity												x		x						
RLB_302 Self tests												x		x						
RLB_303 Manufacturing tests					x	x						x		x						
RLB_304 Software analysis					x		x	x				x		x						
RLB_305 Software input					x	x		x				x		x						
RLB_306 Power supply									x	x		x		x						
RLB_307 Reset												x		x						
DEX_301 Secured data import											x									x
DEX_302 Secured data import											x									x
DEX_303 Secured data export to VU											x									x
DEX_304 Evidence of origin											x									x
DEX_305 Evidence of origin											x									x
DEX_306 Secured export to external media											x									x
CSP_301 Key generation												x								x
CSP_302 Key distribution												x								x

Tillägg 11

GEMENSAMMA SÄKERHETSMEKANISMER

INNEHÅLL

1. Allmänt

I detta tillägg specificeras de säkerhetsmekanismer som skall säkerställa följande:

— Ömsesidig autentisering mellan fordonsenhet och färdskrivarkort, inbegripet överenskommelse om sessionsnycklar.

— Sekretess i, integritet hos, och autentisering av data som överförs mellan fordonsenhet och färdskrivarkort.

— Integritet och autenticitet hos data som överförs från fordonsenhet till externa lagringsmedia.

— Integritet och autenticitet hos data som överförs från färdskrivarkort till externa lagringsmedia.

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. Oktober 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	Transaktionskort – Aktivt kort – Part 4: Gemensamma kommandon för datautbyte. Första utgåvan: 1995 + Ändring 1: 1997.
ISO/IEC 7816-6	Identifikationskort – Aktivt Gemensamma dataelement. Första utgåvan: 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
ISO/IEC 9798-3	Dataskydd – Teknik för äkthetsbestyrkande Användning av algoritm för öppen nyckel. Andra utgåvan 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 nyckelknippa som skall användas av Triple Data krypteringsalgoritm
CA	Certification Authority – Certifieringsinstans
CAR	Certification Authority reference – Certifieringsinstansens referens
CC	Cryptographic Checksum – Kryptografisk kontrollsumma
CG	Cryptogram – Kryptogram
CH	Command Header – Kommandohuvud
CHA	Certificate Holder Authorisation – Auktorisering av certifikatinnehavaren
CHR	Certificate Holder Reference – Certifikatinnehavarens referens
D()	Decryption with DES – Dekryptering med DES
DE	Data element – Dataelement
DO	Data object – Dataobjekt
d	RSA private key, private exponent – Privat RSA-nyckel, privat exponent
e	Öppen RSA-nyckel, öppen exponent
E()	Encryption with DES – DES-kryptering
EQT	Equipment – Utrustning
Hash()	Hashvärde, ett resultat av *Hash*
Hash	Hashfunktion
KID	Key Identifier – Nyckelidentifierare
Km	TDES-nyckel. Huvudnyckel enligt definitionen i ISO 16844-3
Km_{vu}	TDES-nyckel i fordonsenheterna
Km_{wc}	TDES-nyckel i verkstadskorten
m	Message representative, integer mellan 0 och *n*-1
n	RSA-keys, modulus – RSA-nycklar, modulus
PB	Padding Bytes – Utfyllnads-bytes
PI	Padding Indicator byte (for use in Cryptogram for confidentiality DO – Utfyllnadsindikator-byte (för användning i kryptogram för sekretessdataobjekt)
PV	Plain Value – Klarvärde
s	Signature representative, integer mellan 0 och *n*-1
SSC	Send Sequence Counter
SM	Secure Messaging – Säker meddelandehantering
TCBC	TDEA Cipher Block Chaining Mode of Operation
TDEA	Triple Data Encryption Algorithm – Triple data krypteringsalgoritm
TLV	Tag Length Value – Tagglängd
VU	Vehicle Unit – Fordonsenhet
X.C	Användare X certifikat som utfärdats av en certifieringsinstans
X.CA	Användare X certifieringsinstans
X.CA.PK_oX.C	Uppackning av ett certifikat för att extrahera en öppen nyckel. Det är en infix-operatör, 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	Användare X öppna RSA-nyckel
X.PK[I]	RSA-kryptering av viss information I, med användning av användare X öppna nyckel
X.SK	Användare X privata RSA-nyckel
X.SK[I]	RSA-kryptering av viss information I, med användning av användare X öppna nyckel
'xx'	Ett hexadecimalt värde
||	Concatenation operator – Sammansättningsoperatör

2. KRYPTOSYSTEM OCH ALGORITMER

2.1 **Kryptosystem**

CSM_001 Fordonsenheter och färdskrivarkort skall 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 skall 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:

$$X.SK[m] = s = m^d \bmod n$$

$$X.PK[s] = m = s^e \bmod n$$

En utförligare beskrivning av RSA-funktionen finns i referens [PKCS1].

Den öppna exponenten, e, för RSA-beräkningar kommer att ha ett annat värde än 2 i alla genererade RSA-nycklar.

2.2.2 ***Hashalgoritm***

CSM_004 Mekanismerna för digital signatur skall använda hashalgoritmen SHA-1, som definieras i referens [SHA-1].

2.2.3 ***Datakrypteringsalgoritm***

CSM_005 DES-baserade algoritmer skall användas vid Cipher Block Chaining mode of operation.

3. NYCKLAR OCH CERTIFIKAT

3.1 **Generering och distribuering av nycklar**

3.1.1 ***Generering och distribuering av RSA-nycklar***

CSM_006 RSA-nycklar skall genereras med hjälp av följande tre hierarkiska funktionsnivåer:

— Europeisk nivå.

— Medlemsstatsnivå.

— Utrustningsnivå.

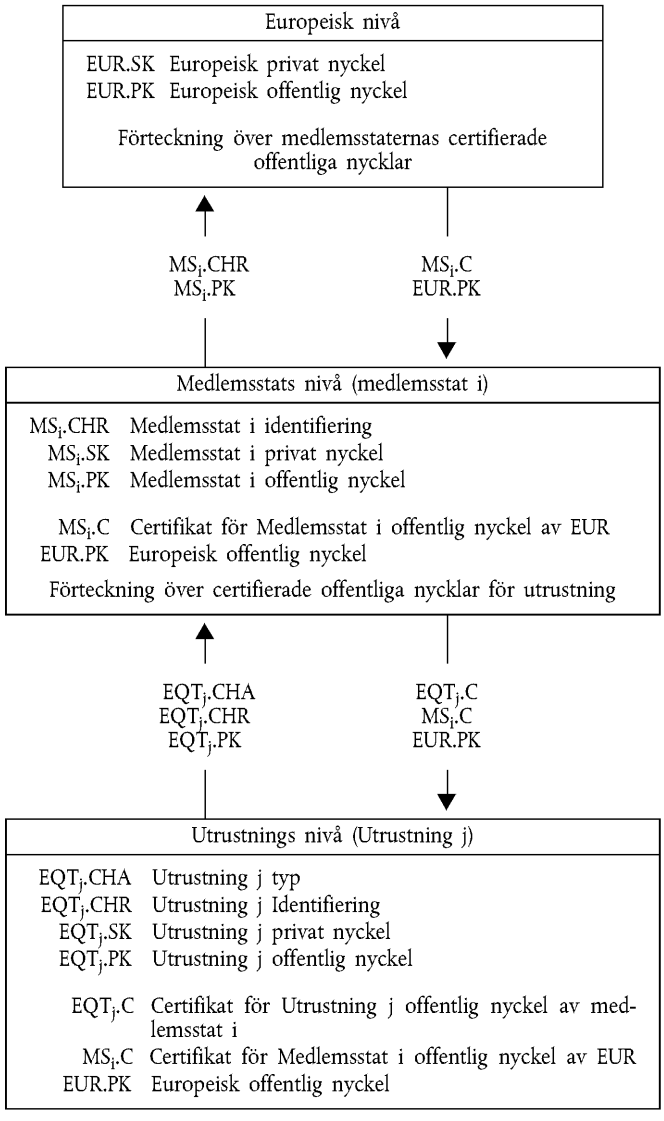
CSM_007 På europeisk nivå skall ett enda europeiskt nyckelpar (EUR.SK och EUR.PK) genereras. Den europeiska privata nyckeln skall användas för att certifiera medlemsstaternas öppna nycklar. Ett register skall föras över alla certifierade nycklar. Dessa uppgifter skall utföras av en europeisk certifieringsinstans, under Europeiska kommissionens överinseende och ansvar.

CSM_008 På medlemsstatsnivå skall ett nyckelpar för medlemsstaten (MS.SK och MS.PK) genereras. Medlemsstaternas öppna nycklar skall certifieras av den europeiska certifieringsinstansen. En medlemsstats privata nyckel skall användas för att certifiera de öppna nycklar som skall sättas i utrustningen (fordonsenhet eller färdskrivarkort). Alla certifierade öppna nycklar skall registreras med identifiering av den utrustning som de är avsedda för. Dessa uppgifter skall utföras av en certifieringsinstans i medlemsstaten. En medlemsstat får regelbundet byta sitt nyckelpar.

CSM_009 På utrustningsnivå skall ett enda nyckelpar (EQT.SK och EQT.PK) genereras och sättas in i varje utrustning. Öppna utrustningsnycklar skall certifieras av en medlemsstats certifieringsinstans. Dessa uppgifter får utföras av tillverkare av utrustningar, dem som anpassar utrustningar, eller medlemsstaternas myndigheter. Detta nyckelpar används för autentisering, digital signering och kryptering.

CSM_010 Sekretessen för privata nycklar skall bibehållas vid generering, eventuell transport och lagring.

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) skall den europeiska certifieringsinstansen generera ett annat enda europeiskt nyckelpar för provning och minst två medlemsstatsnyckelpar för provning, vars öppna nycklar skall certifieras med den europeiska privata provningsnyckeln. I utrustning som provas för typgodkännande skall tillverkarna sätta i provningsnycklar som certifierats av en av dessa medlemsstatsnycklar för provning.

3.1.3 ***Nycklar för rörelsesensorer***

Sekretessen för de tre nedannämnda TDES-nycklarna skall bibehållas på lämpligt sätt vid generering, eventuell transport och lagring.

Som stöd för färdskrivare som uppfyller bestämmelserna i ISO 16844 skall den europeiska certifieringsinstansen och medlemsstatens certifieringsinstanser dessutom garantera följande:

CSM_036 Den europeiska certifieringsinstansen skall generera Km_{VU} och Km_{WC} två oberoende och unika nycklar för Triple DES, och generera Km som:

$$Km = Km_{VU} \text{ XOR } Km_{WC}$$

Den europeiska certifieringsinstansen skall överlämna dessa nycklar på ett säkert sätt till medlemsstaternas certifieringsinstanser på de senares begäran.

CSM_037 Medlemsstaternas certifieringsinstanser skall:

— använda Km för att kryptera de rörelsesensordata som efterfrågas av rörelsesensortillverkarna (de data som skall krypteras med Km definieras i ISO 16844-3),

— överlämna Km_{VU} till fordonsenhetstillverkarna på ett säkert sätt för installation i fordonsenheterna, och

— se till att Km_{WC} kommer att installeras i alla verkstadskort (`SensorInstallationSecData` i datafilen `Sensor_Installation_Data`) då kortet anpassas till användaren.

3.1.4 ***Generering och distribuering av sessionsnycklar för T-DES***

CSM_012 Fordonsenheter och färdskrivarkort skall som en del av den ömsesidiga autentiseringen generera och utbyta nödvändiga data för att utveckla en gemensam sessionsnyckel för Triple DES. Detta utbyte av data skall sekretesskyddas genom en mekanism för RSA-kryptering.

CSM_013 Denna nyckel skall användas för all efterföljande kryptografisk verksamhet där säker meddelandehantering (secure messaging) används. Dess giltighet skall gå ut när sessionen avslutas (urtagning 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 skall (oavsett nivå) ha följande längd: modulus *n* 1024 bits, öppen exponent *e* maximalt 64 bits, privat exponent *d* 1024 bits.

CSM_015 Triple DES-nycklar skall ha formen (K_a, K_b, K_a), där K_a och K_b är oberoende 64 bits långa nycklar. Inga bits för påvisande av paritetsfel skall ställas.

3.3 **Certifikat**

CSM_016 Certifikat för öppna RSA-nycklar skall vara icke-självbeskrivande (non self-descriptive) 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	Bytes	Anmärkningar
CPI	INTEGER	1	Identifierare av certifikatprofil (Certificate Profile Identifier – CPI) ('01' för denna version)
CAR	OCTET STRING	8	Certifieringsinstansens referens (CAR)
CHA	OCTET STRING	7	Certifikatinnehavarens auktorisering
EOV	TimeReal	4	Sista giltighetsdag för certifikatet. Valbar, 'FF' utfylld om ej använd
CHR	OCTET STRING	8	Certifikatinnehavarens referens (CHR)
n	OCTET STRING	128	Öppen nyckel (modulus)
e	OCTET STRING	8	Öppen nyckel (öppen exponent)
		164	

Anmärkningar:

1. Identifieraren av certifikatprofil (certificate Profile Identifier – CPI) beskriver autentiseringscertifikatets exakta struktur. Den kan användas som en intern identifierare för utrustningen av en relevant headerlist som beskriver sammansättningen av dataelement inom certifikatet.

   Den headerlist som associeras med 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'
Extended Headerlist Tag	Length of header list	CPI Tag	CPI Length	CAR Tag	CAR Length	CHA Tag	CHA Length	EOV Tag	EOV Length	CHR Tag	CHR Length	Public Key Tag (Constructed)	Length of subsequent DOs	modulus Tag	modulus length	public exponent Tag	public exponent length

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 av instansnyckel (Authority Key Identifier) för att förse certifieringsinstansens öppna nyckel med hänvisningar (för kodning, se nyckelidentifierare (Authority Key Identifier) nedan).

3. Certifikatinnehavarens auktorisering (Certificate Holder Authorisation – CHA) används för att identifiera certifikatinnehavarens rättigheter. Det består av färdskrivarens tillämpningsidentifiering (Application ID) och av den typ av utrustning för vilken certifikatet är avsett (enligt dataelementet EquipmentType '00' för en medlemsstat).

4. Certifieringsinnehavarens referens (CHR) har som syfte att unikt identifiera certifieringsinnehavaren (CH) på så sätt att dataelementet kan användas samtidigt som en identifierare av subjektnyckel (Subject Key Identifier) för att förse certifikatinnehavarens öppna nyckel med hänvisningar.

5. Med nyckelidentifierare identifieras certifikatinnehavaren eller certifieringsinstanserna unikt. De är kodade på följande sätt:

   5.1. Utrustning (fordonsenhet (VU) eller kort):

Data	Utrustningens serienummer	Datum	Typ	Tillverkare
Längd	4 Bytes	2 Bytes	1 Byte	1 Byte
Värde	INTEGER	mm åå BCD-kodning	Tillverkarspecifik	Tillverkarens kod

När det gäller en fordonsenhet (VU) får tillverkaren vid förfrågan om certifikat ha eller inte ha kunskap om identifieringen av den utrustning i vilken nycklarna sätts i.

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 isätts 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 med tilldelning av nyckel till utrustning (dvs. identifiering av certifikatförfrågan, utrustningens identfiering) efter installation av nyckeln i utrustningen. Nyckelidentifieraren har följande form:

Data	Serienummer för förfrågan om certifikat	Datum	Typ	Tillverkare
Längd	4 Bytes	2 Bytes	1 Byte	1 Byte
Värde	BCD-kodning	mm åå BCD-kodning	'FF'	Tillverkarens kod

5.2. Certifieringsinstans (Certification Authority):

Data	Instans-ID	Nyckelns serienummer	Övrig information	Identifierare
Längd	4 Bytes	1 Byte	2 Bytes	1 Byte
Värde	1 Byte numerisk landskod 3 Bytes alfanumerisk landskod	Integer	Övrig kodning (CA-specific) 'FF FF' om den inte används	'01'

Nyckelns serienummer används för att man skall kunna skilja en medlemsstats olika nycklar åt om nyckeln ändras.

6. Certifikatverifierare skall 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 återskapning av certifikatinnehåll enligt ISO/IEC 9796-2, med certifieringsinstansens referens (Certification Authority Reference – CAR) tillfogad.

$$X.C = X.CA.SK['6A' \,||\, C_r \,||\, \mathit{Hash}(Cc) \,||\, 'BC'] \,||\, C_n \,||\, X.CAR$$

Med certifikatinnehåll $= Cc = \underset{106\ \text{Bytes}}{C_r} \,||\, \underset{58\ \text{Bytes}}{C_n}$

Anmärkningar:

1. Detta certifikat är 194 bytes långt.

2. CAR, som är dold av underskriften och är också tillfogad till signaturen, så att certifieringsinstansens öppna nyckel kan väljas för verifiering av certifikatet.

3. Certifikatverifieraren skall indirekt känna till den algoritm som används av certifieringsinstansen för att signera certifikatet.

4. Den headerlist som associeras med detta utfärdade certifikat ser ut på följande sätt:

'7F 21'	'09'	'5F 37'	'81 80'	'5F 38'	'3A'	'42'	'08'
CV Certificate Tag (Constructed)	Length of subsequent DOs	Signature Tag	Signature Length	Remainder Tag	Remainder Length	CAR Tag	CAR Length

3.3.3 ***Verifiering och uppackning av certifikat***

Verifiering och uppackning består i att underskriften verifieras enligt ISO/IEC 9796-2, och att certifikatinnehållet och den öppna nyckeln däri hämtas: X.PK = X.CA.PK$_o$ X.C, och verifiering av certifikatets giltighet.

CSM_019 Detta inbegriper följande steg:

Verifiera signatur och hämta innehåll:

— from X.C retrieve Sign, C_n' and CAR′: X.C = Sign (128 Bytes) || C_n' (58 Bytes) || CAR' (8 Bytes)

— from CAR' select appropriate Certification Authority Public Key (if not done before through other means)

— open Sign with CA Public Key : Sr' = X.CA.PK [Sign],

— check Sr' starts with ′6A′ and ends with ′BC′

— compute Cr′ and H′ from: Sr' = '6A' || C_r' (106 Bytes) || H' (20 Bytes) || 'BC'

— Recover certificate content C′ = C_r' || C_n',

— check *Hash*(C′) = H′

Om kontrollerna är OK är certifikatet äkta och dess innehåll är C′.

Verifiera giltighet. Från C′:

— om tillämpligt, kontrollera 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

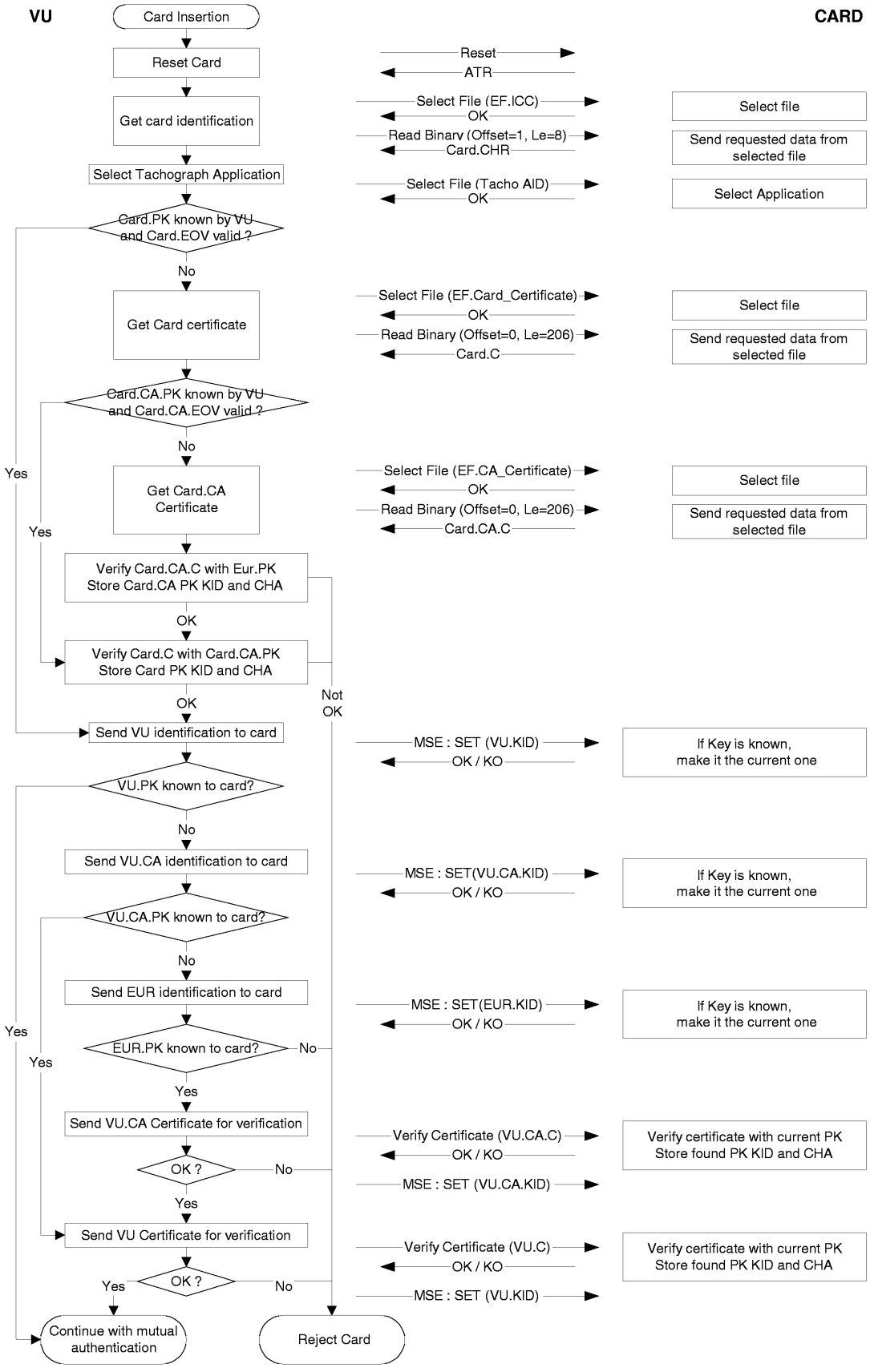
Ömsesidig autentisering mellan kort och fordonsenheter (VUs) bygger på följande princip:

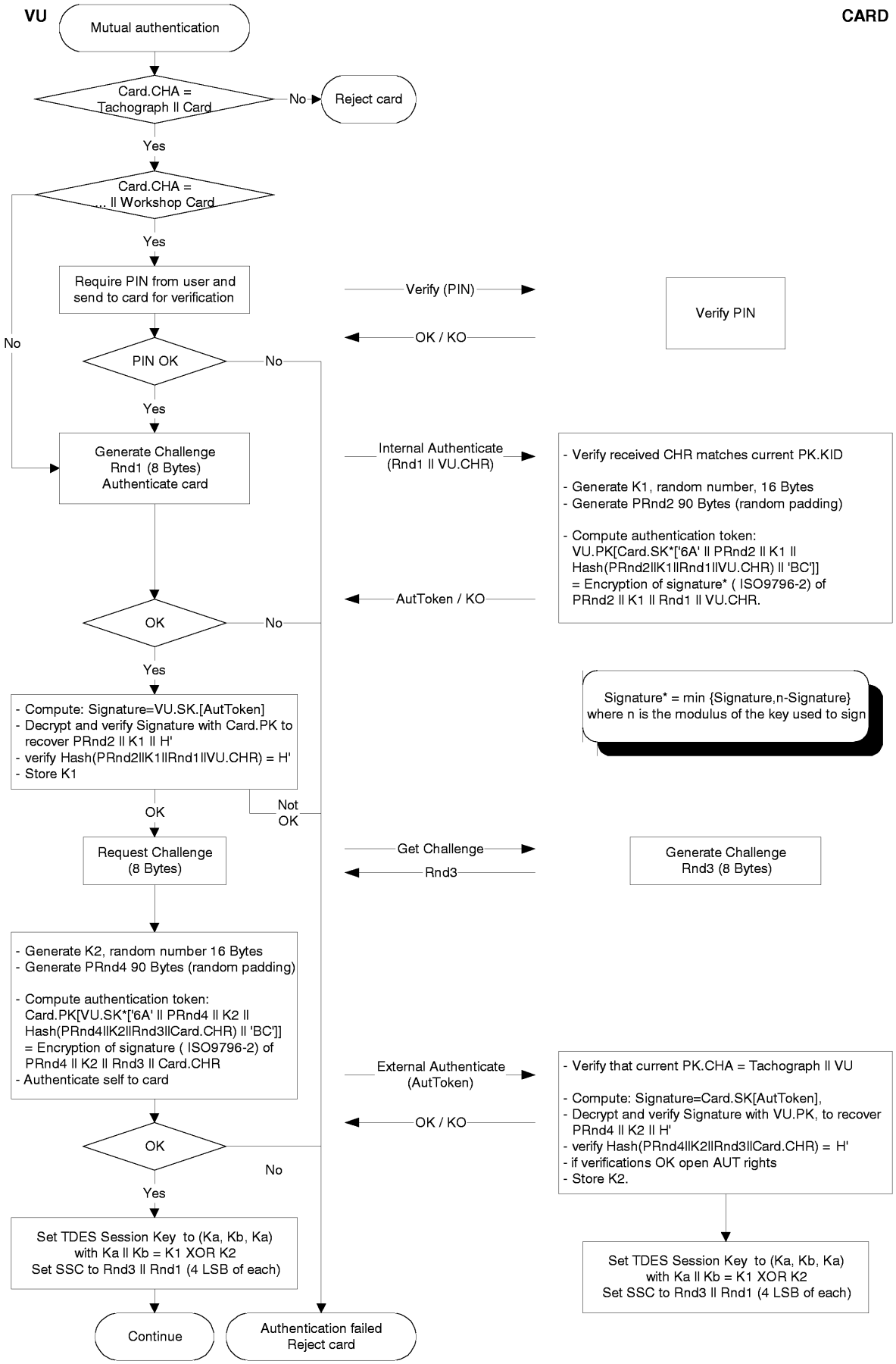
Varje part skall demonstrera för den andra att den äger ett giltigt nyckelpar, vars öppna nyckel har certifierats av en certifieringsinstans i en medlemsstat, som i sin tur har certifierats av den europeiska certifieringsinstansen.

Detta görs genom att man med den privata nyckeln signerar med ett slumptal som sänts av den andra parten, som måste återskapa det sända slumptalet när signaturen verifieras.

Mekanismen utlöses av fordonsenheten (VU) när kortet sätts i. Den börjar med utbyte av certifikat och uppackning av öppna nycklar och slutar med inställning av en sessionsnyckel.

CSM_020 Följande protokoll skall användas (pilar anger kommandon och data som byts ut (se tillägg 2)):




VU
CARD
Mutual authentication
Card.CHA = Tachograph II Card
No
Reject card
Yes
Card.CHA = ... II 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 II 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' II PRnd2 II K1 II Hash(PRnd2IIK1IIRnd1IIVU.CHR) II 'BC']] = Encryption of signature* (ISO9796-2) of PRnd2 II K1 II Rnd1 II 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 II K1 II H'
- verify Hash(PRnd2IIK1IIRnd1IIVU.CHR) = H'
- Store K1
Not OK
OK
Request Challenge (8 Bytes)
Get Challenge
Rnd3
Generate Challenge Rnd3 (8 Bytes)
- Generate K2, random number 16 Bytes
- Generate PRnd4 90 Bytes (random padding)
- Compute authentication token: Card.PK[VU.SK*['6A' II PRnd4 II K2 II Hash(PRnd4IIK2IIRnd3IICard.CHR) II 'BC']] = Encryption of signature (ISO9796-2) of PRnd4 II K2 II Rnd3 II Card.CHR
- Authenticate self to card
External Authenticate (AutToken)
- Verify that current PK.CHA = Tachograph II VU
- Compute: Signature=Card.SK[AutToken],
- Decrypt and verify Signature with VU.PK, to recover PRnd4 II K2 II H'
- verify Hash(PRnd4IIK2IIRnd3IICard.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 II Kb = K1 XOR K2
Set SSC to Rnd3 II Rnd1 (4 LSB of each)
Set TDES Session Key to (Ka, Kb, Ka) with Ka II Kb = K1 XOR K2
Set SSC to Rnd3 II Rnd1 (4 LSB of each)
Continue
Authentication failed Reject card

5. MEKANISMER FÖR SEKRETESS, INTEGRITET OCH AUTENTISERING VID ÖVERFÖRING AV DATA FRÅN FORDONSENHETSKORT

5.1 **Säker meddelandehantering**

CSM_021 Integriteten hos överföring av data från fordonsenhetskort skall skyddas genom säker meddelandehantering (secure messaging) enligt referenserna [ISO/IEC 7816-4] och [ISO/IEC 7816-8].

CSM_022 När data behöver skyddas vid överföring skall ett kryptografiskt kontrollsummedataobjekt (Cryptographic Checksum Data Object) fogas till de dataobjekt som sänds inom kommandot eller svaret. Den kryptografiska kontrollsumman (Cryptographic Checksum) skall verifieras av mottagaren.

CSM_023 Den kryptografiska kontrollsumman hos data som sänds inom ett kommando skall integrera kommandohuvudet (command header), och alla sända dataobjekt (= > CLA = ′0C′, och alla dataobjekt skall kapslas in med taggar i vilka b1 = 1).

CSM_024 Bytes för information om svarets status skall skyddas av en kryptografisk kontrollsumma om svaret inte innehåller något datafält.

CSM_025 Kryptografiska kontrollsummor skall vara 4 Bytes långa.

Strukturen på kommandon och svar vid användning av säker meddelandehantering är därför följande:

De dataobjekt som används är en delmängd (partial set) av de dataobjekt vid säker meddelandehantering som beskrivs i ISO/IEC 7816-4:

Tag	Mnemonic	Meaning
′81′	T_{PV}	Plain Value not BER-TLV coded data (to be protected by CC)
′97′	T_{LE}	Value of Le in the unsecured command (to be protected by CC)
′99′	T_{SW}	Status-Info (to be protected by CC)
′8E′	T_{CC}	Cryptographic Checksum (CC)
′87′	$T_{PI\ CG}$	Padding Indicator Byte || Cryptogram (Plain Value not coded in BER-TLV)

Med ett okrypterat kommandosvarspar:

Command header	Command body
CLA INS P1 P2	[L_c-field [Data field] [L_e-field]
four bytes	L bytes, denoted as B_1 to B_L

Response body	Response trailer
[Data field]	SW1 SW2
L_r data bytes	two bytes

Det motsvarande krypterade kommandosvarsparet är:

Krypterat kommando:

Command header (CH)	Command body										
CLA INS P1 P2	[New L_c-field]	[New Data field]									[New L_e-field]
′OC′	Length of New Data field	T_{PV}	L_{PV}	PV	T_{LE}	L_{LE}	L_e	T_{CC}	L_{CC}	CC	′00′
		′81′	L_c	Data field	′97′	′01′	L_e	′8E′	′04′	CC	

Data som skall integreras i kontrollsumman = CH || PB || T_{PV} || L_{PV} || PV || T_{LE} || L_{LE} || L_e || PB

PB = Padding Bytes (utfyllnads-bytes) (80 .. 00) enligt ISO-IEC 7816-4 und ISO 9797, metod 2.

Dataobjektens klarvärde (PV) och LE är närvarande endast när det finns motsvarande data i det okrypterade kommandot.

Krypterat svar:

1. Fall där svarsdatafältet inte är tomt och inte behöver sekretesskyddas:

Response body						Response trailer
[New Data field]						new SW1 SW2
T_{PV}	L_{PV}	PV	T_{CC}	L_{CC}	CC	
'81'	L_r	Data field	'8E'	'04'	CC	

Data som skall integreras i kontrollsumman = T_{PV} || L_{PV} || PV || PB

2. Fall där svarsdatafältet inte är tomt och behöver sekretesskyddas:

Response body						Response trailer
[New Data field]						new SW1 SW2
$T_{PI\ CG}$	$L_{PI\ CG}$	PI CG	T_{CC}	L_{CC}	CC	
'87'		PI || CG	'8E'	'04'	CC	

Data som skall överföras av CG: icke BER-TLV-kodade data och utfyllnads-bytes.

Data som skall integreras i kontrollsumman = $T_{PI\ CG}$ || $L_{PI\ CG}$ || PI CG || PB

3. Fall där svarsdatafältet är tomt:

Response body						Response trailer
[New Data field]						new SW1 SW2
T_{SW}	L_{SW}	SW	T_{CC}	L_{CC}	CC	
'99'	'02'	New SW1 SW2	'8E'	'04'	CC	

Data som skall integreras i kontrollsumman = T_{SW} || L_{SW} || SW || PB

5.2 **Behandling av fel vid säker meddelandehantering**

CSM_026 När färdskrivarkortet känner av ett fel vid säker meddelandehantering vid tolkning av ett kommando måste status bytes returneras utan säker meddelandehantering. Enligt ISO/IEC 7816-4 definieras följande status bytes för angivelse av fel vid säker meddelandehantering:

'66 88' Verification of Cryptographic Checksum failed,

'69 87' Expected SM Data Objects missing,

'69 88' SM Data Objects incorrect.

CSM_027 När färdskrivarkoret returnerar status bytes utan SM-dataobjekt eller med ett felaktigt SM-dataobjekt måste sessionen avbrytas av fordonsenheten.

5.3 **Algoritm för beräkning av kryptografiska kontrollsummor**

CSM_028 Kryptografiska kontrollsummor byggs med användning av en retail MACs enligt ANSI X9.19 med DES:

— Initial stage: The initial check block y0 is E(Ka, SSC).

— Sequential stage: The check blocks y1, .. , yn are calculated using Ka.

— Final stage: The cryptographic checksum is calculated from the last check block yn as follows: E(Ka, D(Kb, yn)).

där E() betyder kryptering med DES, och D() betyder dekryptering med DES.

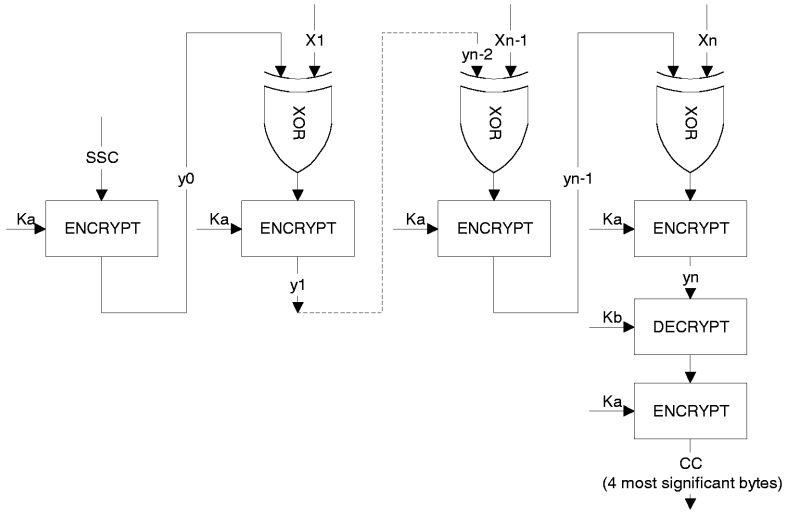
De fyra mest signifikanta bytes i den kryptografiska kontrollsuman överförs.

CSM_029 Send Sequence Counter (SSC) skall initieras vid förfarandet för överenskommelse om nyckel till:

Initial SSC: Rnd3 (4 least significant bytes) || Rnd1 (4 least significant bytes).

CSM_030 Send Sequence Counter skall ökas med 1 varje gång innan en MAC beräknas (dvs. SSC för första kommando är Initial SSC + 1, SSC för det första svaret är Initial SSC + 2).

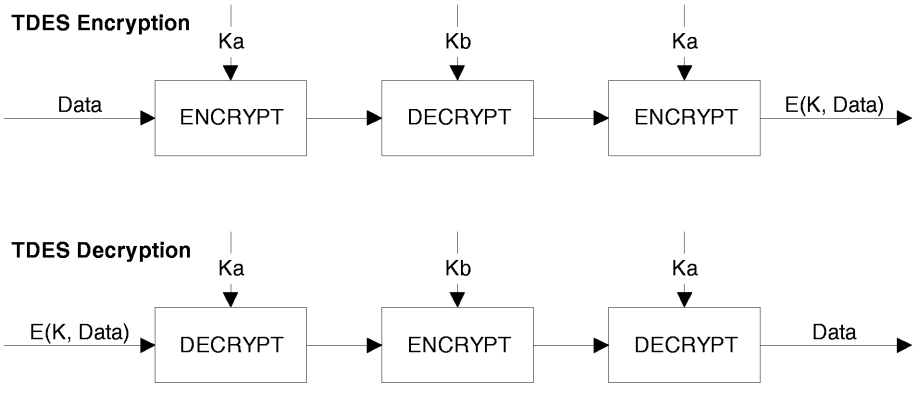
I följande figur visas beräkningen av retail MAC:



5.4 **Algoritm för att beräkna kryptogram för sekretessdataobjekt**

CSM_031 Kryptogram beräknas med hjälp av TDEA i driftläge TCBC enligt referenserna [TDES] och [TDES-OP] och med nollvektorn som Initial Value block.

I följande figur visas tillämpningen av nycklar i TDES:



6. MEKANISMER FÖR DIGITAL SIGNATUR VID DATAÖVERFÖRING

CSM_032 Intelligent Dedicated Equipment (IDE) lagrar data som tas emot från en utrustning (fordonsenhet eller kort) under en överföringssession inom en fysisk datafil. Filen måste innehålla certifikaten MS_i.C och EQT.C. Filen innehåller digitala signaturer av datamängder enligt specifikation i tillägg 7 Protokoll för dataöverföring.

CSM_033 Digitala signaturer för överförda data skall använda ett schema för digitala signaturer med tillägg så att överförda data kan läsas utan att dekrypteras om så önskas.

6.1 **Signaturgenerering**

CSM_034 Utrustningens generering av datasignaturer skall följa det signaturschema med tillägg som definieras i referens [PKCS1] med SHA-1 hashfunktion:

Signature = EQT.SK['00' || '01' || *PS* || '00' || DER(SHA-1(Data))]

PS = Padding string of octets with value 'FF', such that length is 128.

DER(SHA-1(M)) is the encoding of the algorithm ID for the hash function and the hash value into an ASN.1 value of type DigestInfo (distinguished encoding rules):

'30'||'21'||'30'||'09'||'06'||'05'||'2B'||'0E'||'03'||'02'||'1A'||'05'||'00'||'04'||'14'||Hash-Value.

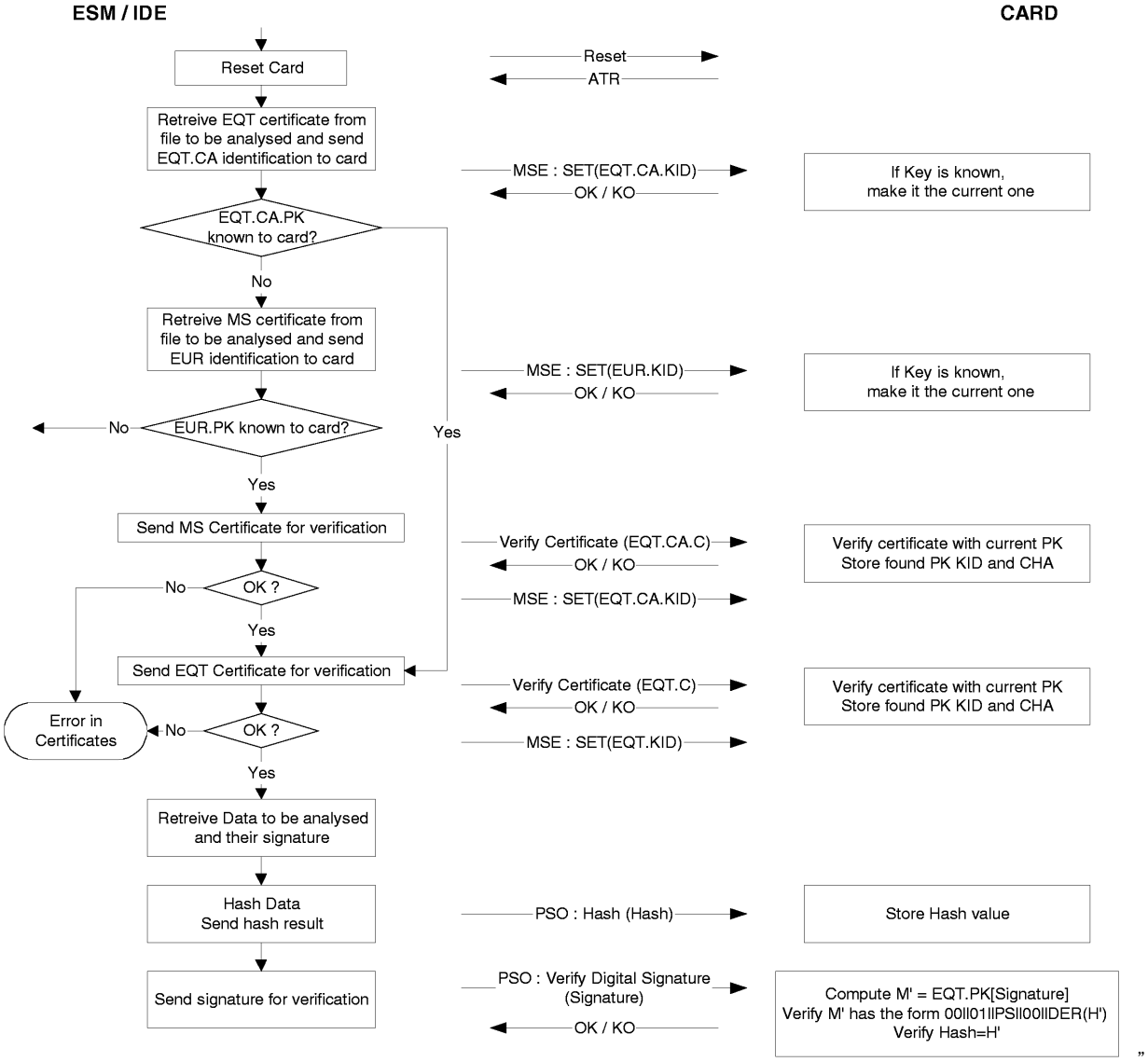
6.2 **Verifiering av signatur**

CSM_035 Verifiering av datasignaturer för överförda data skall följa det signaturschema med tillägg som definieras i referens [PKCS1] med SHA-1 hashfunktion:

Den som verifierar måste oberoende känna till (och lita på) den europeiska öppna nyckeln EUR.PK.

Följande tabell illustrerar det protokoll som en IDE med ett kontrollkort kan följa för att verifiera integriteten hos data som överförs och lagras på externa lagringsmedia (ESM). Kontrollkortet används för att dekryptera digitala signaturer. Denna funktion får i detta fall inte genomföras i IDE.

Den utrustning som har överfört och signerat de data som skall analyseras betecknas EQT.


ESM / IDE
CARD
Reset Card
Reset
ATR
Retreive EQT certificate from file to be analysed and send EQT.CA identification to card
MSE : SET(EQT.CA.KID)
OK / KO
If Key is known, make it the current one
EQT.CA.PK known to card?
No
Retreive MS certificate from file to be analysed and send EUR identification to card
MSE : SET(EUR.KID)
OK / KO
If Key is known, make it the current one
No
EUR.PK known to card?
Yes
Yes
Send MS Certificate for verification
Verify Certificate (EQT.CA.C)
OK / KO
Verify certificate with current PK Store found PK KID and CHA
No
OK ?
MSE : SET(EQT.CA.KID)
Yes
Send EQT Certificate for verification
Verify Certificate (EQT.C)
OK / KO
Verify certificate with current PK Store found PK KID and CHA
Error in Certificates
No
OK ?
MSE : SET(EQT.KID)
Yes
Retreive Data to be analysed and their signature
Hash Data
Send hash result
PSO : Hash (Hash)
Store Hash value
Send signature for verification
PSO : Verify Digital Signature (Signature)
OK / KO
Compute M' = EQT.PK[Signature]
Verify M' has the form 00II01IIPSII00IIDER(H')
Verify Hash=H'

”