II

(Forberedende retsakter)

KOMMISSIONEN

Forslag til Rådets forordning om syvende tilpasning til den tekniske udvikling af Rådets forordning (EØF) nr. 3821/85 om kontrolapparatet inden for vejtransport

(2002/C 126 E/01)

(EØS-relevant tekst)

KOM(2001) 698 endelig udg.

(Forelagt af Kommissionen den 30. november 2001)

RÅDET FOR DE EUROPÆISKE FÆLLESSKABER HAR —

under henvisning til traktaten om oprettelse af Det Europæiske Fællesskab,

under henvisning til Rådets forordning (EØF) nr. 3821/85 af 20. december 1985 om kontrolapparatet inden for vejtransport ([1]), senest ændret ved forordning (EF) nr. 2135/98 ([2]), særlig artikel 17 og 18, og

ud fra følgende betragtninger:

(1) De tekniske forskrifter i bilag I B til forordning (EØF) nr. 3821/85 må tilpasses til den tekniske udvikling med særligt henblik på systemets totale sikkerhed og interoperabiliteten mellem kontrolapparat og førerkort.

(2) Tilpasning af apparatet kræver endvidere tilpasning af bilag II til forordning (EØF) nr. 3821/85, som fastlægger mærker og godkendelsesattester.

(3) Det udvalg, der er nedsat i medfør af artikel 18 i Rådets forordning (EF) nr. 3821/85, afgav ikke en udtalelse om foranstaltningerne i forslaget.

(4) I overensstemmelse med artikel 18, stk. 5, litra b), skal Kommissionen snarest over for Rådet fremsætte forslag til de foranstaltninger, der skal træffes —

UDSTEDT FØLGENDE FORORDNING:

Artikel 1

Bilaget til forordning (EF) nr. 2135/98 erstattes af bilaget til denne forordning.

Artikel 2

Bilag II til forordning (EØF) nr. 3821/85 ændres således:

1. Kapitel I, punkt 1, første led, ændres som følger:
   — standardsymbolet for Grækenland »GR« erstattes af »23«;
   — standardsymbolet for Irland »IRL« erstattes af »24«;
   — der tilføjes standardsymbolet »12« for Østrig;
   — der tilføjes standardsymbolet »17« for Finland;
   — der tilføjes standardsymbolet »5« for Sverige.
2. Kapitel I, punkt 1, andet led, ændres som følger:
   — Ordene »eller af et fartskriverkort« indsættes efter ordet »diagramark«.
3. Kapitel I, punkt 2, ændres som følger:
   — Ordene »og på hvert fartskriverkort« indsættes efter ordet »diagramark«.
4. I kapitel II tilføjes følgende til titlen »FOR PRODUKTER, SOM ER I OVERENSSTEMMELSE MED BILAG I«

([1]) EFT L 370 af 31.12.1985, s. 8.

([2]) EFT L 274 af 9.10.1998, s. 1.

5. Der tilføjes følgende kapitel III:

»III. GODKENDELSESATTEST FOR PRODUKTER, SOM ER I OVERENSSTEMMELSE MED BILAG I B

Den medlemsstat, der har meddelt en typegodkendelse, udsteder en typegodkendelsesattest til ansøgeren efter følgende model. Til underretning af andre medlemsstater om den meddelte typegodkendelse eller om eventuelle inddragelser anvender medlemsstaterne kopier af denne attest.

GODKENDELSESATTEST FOR PRODUKTER, SOM ER I OVERENSSTEMMELSE MED BILAG I B

Myndighedens navn: .....

Meddelelse om (*):

☐ Godkendelse af

☐ Inddragelse af godkendelse af

☐ kontrolapparat model

☐ komponent til kontrolapparat (**) .....

☐ et førerkort

☐ et værkstedskort

☐ et firmakort

☐ et kontrolkort

Godkendelse nr. .....

1. Fabrikat eller varemærke .....
2. Modellens navn .....
3. Fabrikantens navn .....
4. Fabrikantens adresse .....
5. Godkendelse ansøgt for .....
6. Laboratorie(r) .....
7. Dato og nummer på prøve(r) .....
8. Godkendelsesdato .....
9. Dato for inddragelse af godkendelse .....
10. Model af kontrolapparatkomponent(er), som komponenten er bestemt til anvendelse sammen med .....
11. Sted.....
12. Dato .....
13. Beskrivende dokumenter vedlagt .....

---

14. Bemærkninger (herunder eventuelle plombers placering)

.....
(underskrift)

(*) Afkryds de relevante felter.
(**) Angiv, hvilken komponent anmeldelsen vedrører.«

Artikel 3

Denne forordning træder i kraft på tyvendedagen efter offentliggørelsen i *De Europæiske Fællesskabers Tidende*.

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

BILAG

»*BILAG I B*

FORSKRIFTER FOR KONSTRUKTION, AFPRØVNING, MONTERING OG EFTERSYN

For at sikre interoperabiliteten af programmellet til det udstyr, der beskrives i dette bilag, er visse EDB-mæssige forkortelser, begreber og udtryk holdt i originalsproget, dvs. engelsk. Ordrette oversættelser dog tilføjet i parentes til orientering og til at lette forståelsen

I. DEFINITIONER

I dette bilag forstås ved:

a) »**aktivering**«:

Den fase, hvori kontrolapparatet bliver helt driftsklart og implementerer alle funktioner, herunder sikkerhedsfunktioner;

For at aktivere et kontrolapparat skal man benytte et værkstedskort og indtaste dettes PIN-kode.

b) »**ægthedsbekræftelse**«:

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

c) »**ægthed**«:

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

d) »**indbygget test (BIT)**«:

Test, som køres på ordre fra operatøren eller fra eksternt udstyr;

e) »**kalenderdag**«:

et døgn fra kl. 0.00 til kl. 24.00. Alle kalenderdage går efter UTC-tid (koordineret verdenstid);

f) »**kalibrering**«:

Opdatering eller bekræftelse af de køretøjsparametre, som skal ligge i datalageret. Køretøjsparametre omfatter køretøjsidentifikation (VIN, indregistreringsnummer og den medlemsstat, der foretager registreringen) samt køretøjskarakteristika (w, k, l, dækstørrelse, indstilling af hastighedsbegrænser (hvis relevant), aktuel UTC-tid, aktuel kilometerstand);

Til kalibrering af et kontrolapparat kræves værkstedskort.

g) »**kortnummer**«:

Et nummer, som består af 16 alfanumeriske tegn og entydigt identificerer et fartskriverkort i en medlemsstat. I kortnummeret indgår et fortløbende indeks (hvis relevant), et erstatningsindeks og et fornyelsesindeks.

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

h) »**fortløbende kortindeks**«:

Kortnummerets 14. alfanumeriske tegn, som anvendes til at skelne mellem de forskellige kort, som udstedes til en virksomhed eller instans med ret til at få udstedt flere forskellige fartskriverkort. Den pågældende virksomhed eller instans er entydigt identificeret ved de første 13 tegn i kortnummeret;

i) »**kortfornyelsesindeks«:**

Kortnummerets 16. alfanumeriske tegn, som øges, hver gang et fartskriverkort fornys;

j) »**korterstatningsindeks«:**

Kortnummerets 15. alfanumeriske tegn, som øges, hver gang et fartskriverkort erstattes;

k) »**køretøjets vejdrejetal«:**

Den karakteristiske størrelse, der angiver talværdien af udgangssignalet fra den køretøjsdel, der forbinder kontrolapparatet med køretøjet (gearkassens udgangsaksel eller hjulakslen), mens det tilbagelægger en afstand på 1 km under normale prøvebetingelser (se kapitel VI.-5). Vejdrejetallet udtrykkes i impulser pr. km (w = . . . imp/km);

l) »**virksomhedskort«:**

Et fartskriverkort, som af medlemsstatens myndigheder er udstedt til ejeren eller indehaveren af køretøjer monteret med kontrolapparat;

Virksomhedskortet identificerer virksomheden og gør det muligt at vise, overføre og printe data, som er gemt i det kontrolapparat, som denne virksomhed har låst.

m) »**kontrolapparatets konstant«:**

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

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

Aktuel akkumuleret køretid for en given fører siden afslutningen af dennes sidste RÅDIGHED, PAUSE/HVILE eller periode som er UKENDT [2] på 45 minutter eller derover (denne periode kan være fordelt på flere perioder på mindst 15 minutter). I beregningerne tages efter behov hensyn til tidligere aktiviteter, som er gemt på førerkortet. Når føreren ikke har isat sit kort, baseres beregningerne på de data, der er registreret vedrørende den aktuelle periode, hvor der ikke var isat et kort, og som vedrører den pågældende kortplads;

o) »**kontrolkort«:**

Et fartskriverkort, som af en medlemsstats myndigheder er udstedt til en national kompetent kontrolmyndighed;

Kontrolkortet identificerer kontrolinstansen og eventuelt kontrolpersonen og giver mulighed for adgang til data i datalageret eller på førerkortene med henblik på læsning, udprintning og/eller overførsel.

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

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

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

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

q) »**datalager«:**

En elektronisk datalagerenhed, som er indbygget i kontrolapparatet;

---

[1] Denne beregningsmetode for sammenhængende køretid og akkumuleret pausetid benyttes af kontrolapparatet, til beregning af advarselssignal for sammenhængende køretid. Den foregriber ikke, hvilken retlig fortolkning disse tider skal gøres til genstand for.

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

r) »**digital underskrift«:**

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

s) »**dataoverførsel«:**

Kopiering, sammen med den digitale underskrift, af en del af eller et komplet sæt data, der er gemt i køretøjets eller et fartskriverkorts datalager;

Overførslen må ikke bevirke, at lagrede data ændres eller slettes.

t) »**førerkort«:**

Et fartskriverkort, som af medlemsstatens myndigheder er udstedt til en bestemt fører;

Førerkortet identificerer føreren og har mulighed for lagring af aktivitetsdata for føreren.

u) »**effektiv dækperiferi«:**

Gennemsnittet af de afstande, hvert enkelt af køretøjets trækkende hjul tilbagelægger ved en fuld omdrejning. Måling af sådanne afstande skal finde sted under normale prøvebetingelser (kapitel VI.5.) og angives i formen »l = . . . mm«. Køretøjsfabrikanten kan erstatte måling af sådanne afstande med en teoretisk beregning, som tager hensyn til vægtfordelingen på akslerne for det driftsklare, ubelastede køretøj [1]. Metoderne til en sådan teoretisk beregning skal godkendes af de kompetente myndigheder i en medlemsstat;

v) »**hændelse«:**

Unormal funktion, som detekteres af kontrolapparatet og kan skyldes forsøg på misbrug;

w) »**fejl«:**

Unormal funktion, som detekteres af kontrolapparatet og kan skyldes funktionsfejl ved apparatet eller svigt af dette;

x) »**montering«:**

Montering af kontrolapparatet i et køretøj;

y) »**bevægelsesføler«:**

En del af kontrolapparatet, som afgiver et signal, som repræsenterer kørehastighed og/eller tilbagelagt afstand;

z) »**ugyldigt kort«:**

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

aa) »**uden for gyldighedsområdet«:**

Når kontrolapparat ikke kræves anvendt efter bestemmelserne i Rådets forordning (EØF) nr. 3820/85.

bb) »**overskridelse af tilladt hastighed«:**

Overskridelse af tilladt hastighed for køretøjet, defineret som en vilkårlig periode op over 60 sekunder, i hvilken køretøjets målte hastighed overskrider den grænse for indstilling af hastighedsbegrænseren, som er fastlagt i Rådets direktiv 92/6/EØF af 10. februar 1992 om montering og anvendelse af hastighedsbegrænsende anordninger i visse klasser af motorkøretøjer i Fællesskabet [2];

cc) »**periodisk eftersyn«:**

Et sæt operationer, som udføres for at kontrollere, at kontrolapparatet fungerer korrekt og at dets indstillinger svarer til køretøjets parametre;

---

[1] Europa-Parlamentets og Rådets direktiv 97/27/EF af 22. juli 1997 om masse og dimensioner for visse motorkøretøjsklasser og påhængskøretøjer dertil og om ændring af direktiv 70/156/EØF (EFT L 233 af 25.8.1997, s. 1).

[2] EFT L 57 af 2.3.1992, s. 27.

dd) »**printer«:**

Den komponent i kontrolapparatet, som leverer udskrifter af lagrede data;

ee) »**kontrolapparat«:**

Alt det udstyr, der er bestemt til montering i motorkøretøjer for hel- eller halvautomatisk at vise, registrere og lagre oplysninger om kørslen og om bestemte perioder i førernes arbejdstid;

ff) »**fornyelse«:**

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

gg) »**reparation«:**

enhver sådan reparation af en bevægelsesføler eller af en køretøjsenhed, som kræver afbrydelse af dens strømforsyning, afbrydelse fra andre af kontrolapparatets dele eller oplukning af føleren;

hh) »**erstatning«:**

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

ii) »**sikkerhedsattestering«:**

Den proces, hvorved det attesteres af et ITSEC ([1]) attesteringsorgan, at kontrolapparat (eller -komponent) eller det undersøgte fartskriverkort opfylder sikkerhedsforskrifterne i tillæg 10, fælles sikkerhedsmål;

jj) »**selvtest«:**

Tests, som af kontrolapparatet foretages periodisk og automatisk til afsløring af fejl;

kk) »**fartskriverkort«:**

Chipkort til brug sammen med kontrolapparatet. Fartskriverkort gør det muligt for kontrolapparatet at identificere kortindehaverens identitet (eller identitetsgruppe) og giver mulighed for at overføre og gemme data. Fartskriverkort kan være af følgende typer:

— førerkort,

— kontrolkort,

— værkstedskort,

— virksomhedskort;

ll) »**typegodkendelse«:**

Den proces, hvormed en medlemsstat attesterer, at kontrolapparatet eller -komponenten eller det undersøgte fartskriverkort opfylder forskrifterne i denne forordning;

mm) »**dækstørrelse«:**

dækdimensionsbetegnelse (udvendige drivende hjul) i henhold til direktiv 92/23/EØF ([2]);

nn) »**køretøjsidentifikation«:**

De numre, som identificerer køretøjet: Køretøjets registreringsnummer (VRN) med angivelse af den medlemsstat, hvor det er indregistreret, og køretøjets identifikationsnummer (VIN) ([3]);

([1]) Rådets henstilling 95/144/EF af 7. april 1995 om ensartede kriterier for vurdering af informationsteknologisk sikkerhed (EFT L 93 af 26.4.1995, s. 27).
([2]) EFT L 129 af 14.5.1992, s. 95.
([3]) Direktiv 76/114/EØF af 18.12.1975 (EFT L 24 af 30.1.1976, s. 1).

oo) »**køretøjsenhed (VU)«:**

Kontrolapparatet uden bevægelsesføler og uden dennes tilslutningskabler. Køretøjsenheden kan enten være en enkelt enhed eller flere enheder, som er fordelt i køretøjet, når blot den opfylder sikkerhedsforskrifterne i dette regulativ;

pp) **til beregningsformål i kontrolapparatet forstås ved »uge«:**

Tidsrummet fra mandag kl. 00.00 UTC til søndag kl. 24.00 UTC;

qq) »**værkstedskort«:**

Et fartskriverkort, som af medlemsstatens myndigheder er udstedt til en fabrikant af kontrolapparater, en installatør, en køretøjsfabrikant eller et værksted, som er godkendt af samme medlemsstat.

Værkstedskortet identificerer kortindehaveren og giver mulighed for prøvning, kalibrering og/eller dataoverførsel på kontrolapparatet.

II. KONTROLAPPARATETS GENERELLE EGENSKABER OG FUNKTIONER

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

1. **Generelle egenskaber**

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

001 Kontrolapparatet omfatter kabler, en bevægelsesføler og en køretøjsenhed.

002 Køretøjsenheden består af en processor, et datalager, en datahukommelse, et tidstro ur, to chipkortinterface-enheder (fører og medchauffør), en printer, en skærm, et visuelt advarselssignal, et kalibrerings- og udlæsningsstik samt faciliteter til indlæsning foretaget af bruger.

Kontrolapparatet kan være tilsluttet andre enheder gennem ekstra stik.

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

Kontrolapparatets brugere identificerer sig over for apparatet gennem fartskriverkort.

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

Kontrolapparatet registrerer og gemmer data i sit datalager og på fartskriverkortene.

Dette sker i overensstemmelse med Europa-Parlamentets og Rådets direktiv 95/46/EF af 24. oktober 1995 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger ([1]).

2. **Funktioner**

005 Kontrolapparatet skal garantere følgende funktioner:

— overvågning af indsætninger og udtagninger af kort,

— måling af hastighed og tilbagelagt afstand,

— tidsmåling,

— overvågning af førerens aktiviteter,

— overvågning af kørestatus,

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

— manuel indlæsning foretaget af føreren:

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

  — manuel indlæsning af førerens aktiviteter,

  — indlæsning af særlige omstændigheder,

— forvaltning af virksomhedslåse,

— overvågning af kontrolaktiviteter,

— detektion af hændelser og/eller fejl,

— indbyggede tests og selvtests,

— læsning fra datalager,

— registrering og lagring i datalager,

— læsning fra fartskriverkort,

— registrering og lagring på fartskriverkort,

— visning på skærm,

— udprintning,

— advarselssignaler,

— overførsel af data til eksterne medier,

— udlæsning af data til supplerende eksterne enheder,

— kalibrering,

— tidsjustering.

3. **Funktionsmåder**

006 Kontrolapparatet skal have fire funktionsmåder:

— driftsmåde,

— kontrolmåde,

— kalibreringsmåde,

— virksomhedsmåde.

007 Kontrolapparatet skal skifte til følgende funktionsmåde, afhængigt af de gyldige fartskriverkort, som indsættes i kortlæserne:

Funktionsmåde		Førerkortplads				
		Intet kort	Førerkort	Kontrolkort	Værkstedskort	Virksomhedskort
Kortplads f. medchauffør	Intet kort	Driftsklar	Driftsklar	Kontrol	Kalibrering	Virksomhed
	Førerkort	Driftsklar	Driftsklar	Kontrol	Kalibrering	Virksomhed
	Kontrolkort	Kontrol	Kontrol	Kontrol (*)	Driftsklar	Driftsklar
	Værkstedskort	Kalibrering	Kalibrering	Driftsklar	Kalibrering (*)	Driftsklar
	Virksomheds-kort	Virksomhed	Virksomhed	Driftsklar	Driftsklar	Virksomhed (*)

008 (*) I disse situationer skal kontrolapparatet kun bruge det fartskriverkort, som er isat i førerkortets kortplads.

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

010 Alle de i kapitel II, punkt 2 angivne funktioner skal virke i alle funktionsmåder, med følgende undtagelser:

— kalibreringsfunktionen er kun tilgængelig i kalibreringsmåde,

— tidsindstillingsfunktionen er begrænset, når apparatet ikke er i kalibreringsmåde,

— funktionerne vedrørende manuel dataindlæsning foretaget af fører er kun tilgængelige i driftsmåde og kalibreringsmåde,

— funktionen styring af virksomhedslåse er kun tilgængelig i virksomhedsmåde,

— funktionen overvågning af kontrolaktivitet er operationel i kontrolmåde,

— dataoverførselsfunktionen er ikke tilgængelig i driftsmåde (bortset fra det i krav 150 fastlagte).

011 Kontrolapparatet kan udlæse alle data til skærm, printer og eksterne interface-enheder, med følgende undtagelser:

— i driftsmåde slettes enhver personlig identifikation (efternavn og fornavn), som ikke modsvarer det isatte fartskriverkort; alle kortnumre, som ikke svarer til det isatte kort, bliver delvis slettet (hver andet tegn — fra venstre til højre — bliver slettet),

— i virksomhedsmåde kan førerrelaterede data (krav 081, 084 og 087) kun udlæses for perioder, som ikke er låst af en anden virksomhed (således som denne er identificeret ved de første 13 cifre i virksomhedskortnummeret),

— når der intet kort sidder i kontrolapparatet, kan førerrelaterede data kun udlæses for den aktuelle dato og de 8 foregående kalenderdage.

4. **Sikkerhed**

Med sikringen af systemet tilstræbes det at beskytte datahukommelsen på en sådan måde, at uvedkommende ikke kan få adgang til og manipulere med data, og således at forsøg herpå opdages, at beskytte integritet og ægthed af data, som udveksles mellem bevægelsesføler og køretøjsenhed, at beskytte integritet og ægthed af data, som udveksles mellem kontrolapparat og fartskriverkort, og at efterprøve integritet og ægthed af data, som overføres.

012 For at systemet skal være sikkert, skal kontrolapparatet opfylde de sikkerhedsforskrifter, der er angivet under fælles sikkerhedsmål for bevægelsesføler og køretøjsenhed (tillæg 10).

III. KONSTRUKTIONS- OG FUNKTIONSKRAV TIL KONTROLAPPARATER

1. **Isætning og udtagning af kontrolkort**

013 Kontrolapparatet skal overvåge isætning og udtagning af kort i kortlæseenhederne.

014 Når et kort isættes, skal kontrolapparatet detektere, om kortet er et gyldigt fartskriverkort, og, i bekræftende fald, dets type.

015 Kontrolapparatet skal være konstrueret således, at det låser fartskriverkortene i stilling, når de isættes korrekt i kortlæserne.

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

2. **Måling af hastighed og tilbagelagt afstand**

017 Denne funktion skal til stadighed måle og kunne angive den kilometerstand, der svarer til den totale afstand tilbagelagt af køretøjet.

018 Denne funktion skal til stadighed måle og kunne angive køretøjets hastighed.

019 Hastighedsmålefunktionen skal endvidere kunne angive, om køretøjet er i bevægelse eller holder stille. Køretøjet anses for at være i bevægelse, så snart funktionen detekterer flere end 1 imp/sek. fra bevægelsesføleren i mindst 5 sekunder, ellers anses det for at holde stille.

Anordninger, som viser hastighed (speedometer) og total tilbagelagt distance (kilometertæller) og er monteret i et køretøj med et kontrolapparat, som opfylder denne forordnings bestemmelser, skal opfylde forskrifterne for tilladelige maksimale tolerancer i dette bilag (kapitel III.2.1 og III.2.2).

2.1. ***Måling af tilbagelagt afstand***

020 Den tilbagelagte afstand kan måles enten:

— så både fremadkørsel og bagudkørsel medregnes, eller

— så alene fremadkørsel medregnes.

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

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

— ± 1 % før montering,

— ± 2 % ved montering og periodisk eftersyn,

— ± 4 % under brug.

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

2.2. ***Hastighedsmåling***

024 Kontrolapparatet skal måle hastigheder fra 0 til 220 km/h.

025 For at sikre en højeste tolerance på den viste hastighed på ± 6 km/h under brug, og under hensyntagen til:

— a ± en tolerance på 2 km/h på variationer i inddata (dækvariationer, . . .),

— a ± en tolerance på 1 km/h på målinger udført under montering og periodiske eftersyn,

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

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

025a Inden for 2 sekunder efter afslutning af en hastighedsændring skal hastighedsmåling kunne foretages korrekt med de normale tolerancer, når hastighedsændringen er sket i et tempo på indtil 2 m/s^2.

026 Hastighedsmålingen skal have en opløsning på 1 km/h eller bedre.

3. **Tidsmåling**

027 Tidsmålefunktionen skal permanent og digitalt levere UTC-dato og -tid.

028 Til datering skal konsekvent anvendes UTC-dato og -tid i hele kontrolapparatet (registrering, udskrivning, dataoverførsel, skærm, . . .).

029 For at lokal tid kan vises, skal forskydningen af den viste tid kunne ændres i trin på en halv time.

030 Tidspunktdriften skal være inden for ± 2 sekunder i døgnet under typegodkendelsesomstændigheder.

031 Tidsmålingens opløsning skal være 1 sekund eller bedre.

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

4. **Overvågning af førerens aktiviteter**

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

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

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

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

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

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

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

040 Har der i et givet kalenderminut fundet KØRSEL sted, anses hele det pågældende minut for KØRSEL.

041 Har der for et givet kalenderminut fundet KØRSEL sted i både det umiddelbart foregående og umiddelbart efterfølgende minut, anses hele det pågældende minut for KØRSEL.

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

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

5. **Overvågning af førerstatus**

044 Denne funktion overvåger kørestatus permanent og automatisk.

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

6. **Manuel indlæsning foretaget af fører**

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

046 Denne funktion skal give mulighed for indlæsning af de steder, hvor den daglige arbejdstid begynder og/eller slutter for fører og/eller medchauffør.

047 Ved stedet forstås den pågældende stat samt, hvor det er relevant, region.

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

049 Kontrolapparatet skal tillade, at denne anmodning tilsidesættes.

050 Det skal være muligt at indlæse steder, hvor den daglige arbejdstid begynder og/eller slutter, uden kort eller på andre tidspunkter end ved isætning eller udtagning af kort.

6.2. ***Manuel indlæsning af førerens aktiviteter***

050a Ved isætning af førerkort (eller værkstedskort) på dette tidspunkt, og kun på dette tidspunkt, skal kontrolapparatet:

— oplyse kortindehaveren om dato og klokkeslæt for seneste udtagning af dennes kort og

— anmode kortindehaveren om at identificere sig, hvis den aktuelle isætning af kortet repræsenterer en fortsættelse af den aktuelle daglige arbejdstid.

Kontrolapparatet skal give kortindehaveren mulighed for at tilsidesætte spørgsmålet uden at svare, at svare bekræftende eller at svare benægtende:

— Tilsidesætter kortindehaveren spørgsmålet, skal kontrolapparatet anmode kortindehaveren om at angive et »sted, hvor den daglige arbejdstid begynder«. Kontrolapparatet skal tillade, at denne anmodning tilsidesættes. Indlæses der et sted, skal dette registreres i datalageret og på fartskriverkortet og knyttes sammen med kortisætningstidspunktet.

— Svares der benægtende eller bekræftende, skal kontrolapparatet anmode kortindehaveren om manuelt at indlæse aktiviteter med tilhørende start- og slutdato og -klokkeslæt, alene som ARBEJDE, RÅDIGHED eller PAUSE/HVILE, nøje indeholdt i perioden seneste kortudtagning — aktuel kortindsættelse, og uden at tillade overlapning mellem disse aktiviteter. Hertil skal anvendes følgende procedurer:

  — Svarer kortindehaveren bekræftende på spørgsmålet, skal kontrolapparatet anmode kortindehaveren om manuelt at indlæse aktiviteter i kronologisk rækkefølge for perioden seneste kortudtagning — aktuel kortisætning. Denne proces skal slutte, når sluttidspunktet for en manuelt indlæst aktivitet er lig kortisætningstidspunktet.

  — Svarer kortindehaveren benægtende på spørgsmålet, skal kontrolapparatet:

    — Anmode kortindehaveren om manuelt at indlæse aktiviteter i kronologisk rækkefølge fra kortisætningstidspunktet indtil sluttidspunktet for den tilknyttede daglige arbejdstid (eller, i tilfælde, hvor den daglige arbejdstid fortsætter på et diagramark, sluttidspunktet for aktiviteterne knyttet til det pågældende køretøj). Før kontrolapparatet lader kortindehaveren indlæse hver aktivitet manuelt, skal det derfor bede kortindehaveren angive, om sluttidspunktet for senest registrerede aktivitet repræsenterer slutningen af en foregående arbejdstid (se bemærkningen nedenfor).

      Bemærkning: Undlader kortindehaveren at angive sluttidspunkt for den foregående arbejdstid, og indlæser en aktivitet manuelt med et sluttidspunkt svarende til kortisætningstidspunktet, skal kontrolapparatet:

      — Antage, at den daglige arbejdstid sluttede ved begyndelsen af første periode efter kortudtagningen med HVILE (eller fortsat UKENDT), eller på kortudtagningstidspunktet hvis der ikke er indlæst en hvileperiode (og ingen periode fortsat er UKENDT),

      — antage, at starttidspunktet (se nedenfor) er lig kortindsætningstidspunktet,

      — gennemføre nedenstående trin.

    — Derefter, hvis sluttidspunktet for den tilknyttede arbejdstid er forskellig fra kortudtagningstidspunket, eller hvis der det pågældende tidspunkt ikke var indlæst et sted, hvor den daglige arbejdstid slutter, anmode kortindehaveren om at »bekræfte eller indlæse det sted, hvor den daglige arbejdstid sluttede« (kontrolapparatet skal tillade, at denne anmodning tilsidesættes). Indlæses der et sted, skal det kun registreres på fartskriverkortet, og kun hvis det er forskelligt fra det, der (i givet fald) blev indlæst ved udtagning af kortet, og skal knyttes til arbejdsperiodens sluttidspunkt,

    — derefter opfordre kortindehaveren til at »indlæse et starttidspunkt« på den aktuelle daglige arbejdstid (eller på aktiviteter vedrørende det aktuelle førerbevis når kortindehaveren tidligere anvendte et diagramark i denne periode), og bede kortindehaveren angive et »sted, hvor den daglige arbejdstid begynder« (kontrolapparatet skal tillade, at denne anmodning tilsidesættes). Indlæses der et sted, skal det gemmes på fartskriverkortet og knyttes til dette starttidspunkt. Er dette starttidspunkt lig kortisætningstidspunktet, skal stedet endvidere gemmes i datalageret,

    — er dette starttidspunkt forskelligt fra kortisætningstidspunktet, derefter opfordre kortindehaveren til manuelt at indlæse aktiviteterne i kronologisk orden fra dette starttidspunkt indtil kortisætningstidspunktet. Denne proces skal slutte, når sluttidspunktet for en manuelt indlæst aktivitet er lig kortisætningstidspunktet.

— Kontrolapparatet skal derefter give kortindehaveren mulighed for at ændre enhver manuelt indlæst aktivitet, indtil den gøres gyldig ved valg af en nærmere bestemt kommando, og derefter forbyde sådanne ændringer.

— Sådanne svar på det indledende spørgsmål efterfulgt af indlæsninger uden aktivitet skal af kontrolapparatet fortolkes som at kortindehaveren har tilsidesat spørgsmålet.

Under hele denne procedure skal kontrolapparatet ikke afvente indlæsning længere end svarende til følgende frister:

— hvis der ingen udveksling sker med apparatets person/maskine grænseflade inden for 1 minut (idet der afgives et visuelt, eventuelt også akustisk opmærksomhedssignal efter 30 sekunder), eller

— hvis kortet tages ud eller isættes der et andet førerkort (eller værkstedskort), eller

— så snart køretøjet sætter i bevægelse,

skal kontrolapparatet gøre eventuelle allerede foretagne indlæsninger gyldige.

6.3. ***Indlæsning af særlige omstændigheder***

050b Kontrolapparatet skal give føreren mulighed for tidstro indlæsning af følgende to særlige omstændigheder:

— »UDEN FOR GYLDIGHEDSOMRÅDE« (start, slut)

— »OVERFART MED FÆRGE/TOG«

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

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

7. **Styring af virksomhedslåse**

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

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

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

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

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

055a Hvis en virksomhed låser ind, hvor forudgående lås var for samme virksomhed, antages det, at forudgående lås ikke er låst »ud« og stadig er »ind«.

8. **Overvågning af kontrolaktiviteter**

056 Denne funktion skal overvåge de aktiviteter — VISNING PÅ SKÆRM, UDPRINTNING, UDLÆSNING på køretøjsenhed og kort — som finder sted i kontrolmåde.

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

9. **Detektion af hændelser og/eller fejl**

058 Denne funktion detekterer følgende hændelser og/eller fejl:

9.1. ***Hændelsen »isætning af ugyldigt kort«***

059 Denne hændelse skal udløses ved isætning af et vilkårligt ikke gyldigt kort og/eller ved udløb af et isat gyldigt kort.

9.2. ***Hændelsen »kortkonflikt«***

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

Kortkonflikt		Førerkortplads				
		Intet kort	Førerkort	Kontrolkort	Værkstedskort	Virksomhedskort
Kortplads f. medchauffør	Intet kort					
	Førerkort				X	
	Kontrolkort			X	X	X
	Værkstedskort		X	X	X	X
	Virksomheds-kort			X	X	X

9.3. ***Hændelsen »tidsoverlapning«***

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

9.4. ***Hændelsen »kørsel uden behørigt kort«***

062 Denne hændelse skal udløses for enhver af de kombinationer af fartskriverkort, som er angivet med X i følgende tabel, når føreraktiviteten skifter til KØRSEL, eller når der skiftes funktionsmåde mens føreraktiviteten er KØRSEL:

Kørsel uden behørigt kort		Førerkortplads				
		Intet (eller ugyldigt) kort	Førerkort	Kontrolkort	Værkstedskort	Virksomhedskort
Kortplads f. medchauffør	Intet (eller ugyldigt) kort	X		X		X
	Førerkort	X		X	X	X
	Kontrolkort	X	X	X	X	X
	Værkstedskort	X	X	X		X
	Virksomheds-kort	X	X	X	X	X

9.5. ***Hændelsen »isætning af kort under kørslen«***

063 Denne hændelse skal udløses, når der indsættes et fartskriverkort i en vilkårlig kortplads, mens føreraktiviteten er KØRSEL.

9.6. ***Hændelsen »sidste kortsession ikke korrekt afsluttet«***

064 Denne hændelse skal udløses, når kontrolapparatet ved indsætning af kortet konstaterer, at foregående kortsession trods bestemmelserne i kapitel III, punkt 1. ikke er blevet afsluttet korrekt (kortet er taget ud, før alle relevante data er blevet gemt på kortet). Denne hændelse er kun relevant for fører- og værkstedskort.

9.7. ***Hændelsen »overskridelse af tilladt hastighed«***

065 Denne hændelse skal udløses for hver overskridelse af tilladt hastighed.

9.8. ***Hændelsen »afbrydelse af strømforsyning«***

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

9.9. ***Hændelsen »fejl i køredata«***

067 Denne hændelse skal udløses ved afbrydelse af den normale dataudveksling mellem bevægelsesføler og køretøjsenhed og/eller ved fejl i dataintegritet eller -ægthedskontrol under dataudveksling mellem bevægelsesføler og køretøjsenhed.

9.10. ***Hændelsen »forsøg på sikkerhedsbrud«***

068 Denne hændelse skal udløses ved enhver anden hændelse, som berører sikkerheden af bevægelsesføler og/eller køretøjsenhed som angivet under fælles sikkerhedsmål for disse komponenter, og som ikke finder sted i kalibreringsmåde.

9.11. ***»Kort« fejl***

069 Denne fejl skal udløses, når der optræder fejl ved et fartskriverkort under driften.

9.12. ***»Fejl ved kontrolapparat«***

070 Denne fejl skal udløses, når et af nedenstående svigt forekommer, uden at apparatet er i kalibreringsmåde:

— Intern fejl i køretøjsenhed

— Printerfejl

— Skærmfejl

— Fejl ved dataoverførsel

— Fejl ved føler

10. **Indbyggede tests og selvtest**

071 Kontrolapparatet skal selvdetektere fejl gennem selvtests og indbyggede tests i overensstemmelse med følgende tabel:

Den testede underenhed	selvtest	Indbygget test
Programmel		Integritet
Datalager	Adgang	Adgang, dataintegritet
Kortlæseenheder	Adgang	Adgang
Tastatur		Manuelt eftersyn
Printer	(op til fabrikanten)	Udskrift
Skærmbillede		Visuelt eftersyn
Dataoverførsel (udføres kun under dataoverførsel)	Korrekt funktion	
Føler	Korrekt funktion	Korrekt funktion

11. **Læsning fra datalager**

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

12. **Registrering og lagring i datalageret**

Med henblik på bestemmelserne i dette afsnit forstås ved

— »365 dage«, 365 kalenderdage med en aktivitet i køretøjet svarende til gennemsnitsførerens. Den gennemsnitlige aktivitet pr. dag i et køretøj defineres som mindst 6 førere eller medchauffører, 6 cykluser med isætning/udtagning af kort samt 256 aktivitetsskift. »365 dage« omfatter således mindst 2 190 (med)chauffører, 2 190 cykluser med kortisætning og -udtagning samt 93 440 aktivitetsskift.

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

— kilometerstand registreres med en opløsning på en kilometer.

— hastigheder registreres med en opløsning på 1 km/h.

073 Data gemt i datalageret må under typegodkendelsesomstændigheder ikke kunne påvirkes af en afbrydelse i den eksterne strømforsyning af under tolv måneders varighed.

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

12.1. ***Identifikationsdata for apparat***

12.1.1. *Identifikationsdata for køretøjsenhed*

075 Kontrolapparatet skal i sit datalager kunne lagre følgende identifikationsdata for køretøjsenhed:

— fabrikantens navn,

— fabrikantens adresse,

— reservedelsnummer,

— serienummer,

— programmellets versionsnummer,

— installationsdato for den pågældende version af programmellet,

— apparatets produktionsår,

— godkendelsesnummer,

076 Køretøjsenhedens identifikationsnummer registreres og lagres én gang for alle af køretøjsenhedens fabrikant, bortset fra programmelrelaterede data og godkendelsesnummeret, som kan ændres ved eventuel opgradering af programmellet.

12.1.2. *Identifikationsdata for bevægelsesføler*

077 Bevægelsesføleren skal kunne gemme følgende identifikationsdata i sit lager:

— fabrikantens navn,

— reservedelsnummer,

— serienummer,

— godkendelsesnummer,

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

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

078 Identifikationsdata på bevægelsesføleren registreres og lagres én gang for alle i bevægelsesføleren af dennes fabrikant.

079 Kontrolapparatet skal kunne registrere og i sit datalager gemme følgende aktuelt parrede identifikationsdata for bevægelsesføler:

— Serienummer,

— godkendelsesnummer,

— dato for første parring,

12.2. ***Sikkerhedselementer***

080 Kontrolapparatet skal kunne lagre følgende sikkerhedselementer:

— Europæisk offentlig nøgle,

— attest fra medlemsstaten,

— attest for apparatet,

— privat nøgle for apparatet.

Kontrolapparatets sikkerhedselementer indsættes i apparatet af køretøjsenhedens fabrikant.

12.3. ***Data vedrørende isætning og udtagning af førerkort***

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

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

— kortnummer, udstedende medlemsstat og udløbsdato som lagret på kortet,

— isætningsdato og -klokkeslæt,

— køretøjets kilometerstand ved isætning af kortet,

— den kortplads, som kortet sidder i,

— dato og klokkeslæt for udtagning af kortet,

— køretøjets kilometerstand ved udtagning af kortet,

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

  — køretøjets registreringsnummer og den indregistrerende medlemsstat,

  — dato og klokkeslæt for udtagning af kortet,

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

082 Datalageret skal kunne opbevare disse data i mindst 365 dage.

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

12.4. ***Føreraktivitetsdata***

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

— kørestatus (FØRERHOLD, ÉN FØRER)

— kortplads (FØRER, MEDCHAUFFØR),

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

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

— dato og klokkeslæt for ændringen,

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

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

085 Datalageret skal kunne opbevare føreraktivitetsdata i mindst 365 dage.

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

12.5. ***Steder, hvor den daglige arbejdstid begynder og/eller slutter***

087 Følgende oplysninger skal af kontrolapparatet registreres og gemmes i datalageret, hver gang en fører eller medchauffør indlæser det sted, hvor den daglige arbejdstid begynder eller slutter:

— I givet fald, kortnummer for fører (medchauffør) samt kortudstedende medlemsstat,

— dato og klokkeslæt for indlæsningen (eller dato/klokkeslæt knyttet til indlæsningen, når indlæsning fandt sted manuelt),

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

— den indlæste stat og region,

— køretøjets kilometerstand.

088 Datalageret skal kunne opbevare data vedrørende den daglige arbejdstids start og/eller slutning i mindst 365 dage (idet det forudsættes, at én fører indlæser to poster dagligt).

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

12.6 ***Kilometerstand***

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

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

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

12.7. ***Detaljerede hastighedsdata***

093 Kontrolapparatet skal registrere og i sit datalager gemme køretøjets øjeblikkelige hastighed med tilhørende dato og klokkeslæt i hvert sekund i mindst de seneste 24 timer, køretøjet har været i bevægelse.

12.8. ***Data vedrørende hændelser***

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

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

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

Hændelse	Lagringsbestemmelse	Data som skal lagres for hver hændelse
Afbrydelse af strømforsyning ([2])	— den længstvarige hændelse for hver af de 10 seneste dage, den er forekommet, — de 5 længstvarige hændelser inden for de sidste 365 dage	— hændelsens startdato og -klokkeslæt, — hændelsens slutdato og -klokkeslæt, — korttype, -nummer og udstedende medlemsstat for ethvert kort, som er isat ved hændelsens start og/eller slutning, — antal tilsvarende hændelser samme dag
Fejl ved køredata	— den længstvarige hændelse for hver af de 10 seneste dage, den er forekommet, — de 5 længstvarige hændelser inden for de sidste 365 dage	— hændelsens startdato og -klokkeslæt, — hændelsens slutdato og -klokkeslæt, — korttype, -nummer og udstedende medlemsstat for ethvert kort, som er isat ved hændelsens start og/eller slutning, — antal tilsvarende hændelser samme dag
Forsøg på sikkerhedsbrud	— de 10 seneste hændelser for hver type hændelse	— hændelsens startdato og -klokkeslæt, — hændelsens slutdato og -klokkeslæt (hvis relevant), — korttype, -nummer og udstedende medlemsstat for ethvert kort, som er isat ved hændelsens start og/eller slutning, — hændelsens type

095 ([1]) Endvidere skal kontrolapparatet registrere følgende data og gemme dem i datalageret:
— dato og klokkeslæt for seneste KONTROL MED OVERSKRIDELSE AF TILLADT HASTIGHED,
— dato og klokkeslæt for den første overskridelse af tilladt hastighed efter denne KONTROL FOR OVERSKRIDELSE AF TILLADT HASTIGHED,
— antal hændelser med overskridelse af tilladt hastighed siden seneste KONTROL FOR OVERSKRIDELSE AF TILLADT HASTIGHED.

([2]) Det kan tillades, at disse data først registreres ved genetablering af strømforsyningen, og at tidspunktet er bestemt med en nøjagtighed på et minut.

12.9. ***Data vedrørende fejl***

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

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

Fejl	Lagringsbestemmelse	Data som skal gemmes for hver hændelse
Kortfejl	— de 10 seneste kortfejl for førerkortet	— startdato og -klokkeslæt for fejlen, — slutdato og -klokkeslæt for fejlen, — korttype, -nummer og udstedende medlemsstat
Fejl ved kontrolapparatet	— de 10 seneste fejl af hver type fejl, — den første fejl efter seneste kalibrering	— startdato og -klokkeslæt for fejlen, — slutdato og -klokkeslæt for fejlen, — fejlens type, — korttype, -nummer og udstedende medlemsstat for ethvert kort, som er isat ved fejlens start og/eller slutning

12.10. ***Kalibreringsdata***

097 Kontrolapparatet skal registrere og i datalageret gemme data vedrørende:

— kalibreringsparametre, som er kendte i aktiveringsøjeblikket,

— dets allerførste kalibrering efter aktivering,

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

— de 5 seneste kalibreringer (hvis der udføres flere kalibreringer samme kalenderdag, skal kun den sidste heraf gemmes).

098 Følgende data skal registreres for hver af disse kalibreringer:

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

— værkstedets navn og adresse,

— værkstedskortets nummer, den kortudstedende medlemsstat og kortets udløbsdato,

— køretøjets identifikation,

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

099 Bevægelsesføleren skal registrere og i sit datalager gemme følgende data vedrørende bevægelsesfølerens montering:

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

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

12.11. ***Tidsjusteringsdata***

100 Kontrolapparatet skal registrere og i sit datalager gemme data vedrørende:

— seneste justering af tidspunktet,

— de 5 største justeringer siden sidste kalibrering,

udført i kalibreringsmåde uden for rammerne af en sædvanlig kalibrering (def. f).

101 Følgende data skal registreres for hver af disse tidsjusteringer:

— dato og klokkeslæt, gammel værdi,

— dato og klokkeslæt, ny værdi,

— værkstedets navn og adresse,

— værkstedskortets nummer, den kortudstedende medlemsstat og kortets udløbsdato.

12.12. ***Data vedrørende kontrolaktivitet***

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

— dato og klokkeslæt for kontrollen,

— kontrolkortets nummer og den kortudstedende medlemsstat,

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

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

12.13. ***Data vedrørende virksomhedslåse***

104 Kontrolapparatet skal registrere og i datalageret gemme data vedrørende de 20 seneste virksomhedslåse:

— dato og klokkeslæt for lås-ind,

— dato og klokkeslæt for lås-ud,

— virksomhedskortets nummer og den kortudstedende medlemsstat,

— virksomhedens navn og adresse.

12.14. ***Data vedrørende dataoverførsel***

105 Kontrolapparatet skal registrere og i sit datalager gemme følgende data vedrørende den seneste dataoverførsel fra datalageret til eksterne medier, som fandt sted i virksomhedsmåde eller i kalibreringsmåde:

— dato og klokkeslæt for dataoverførslen,

— virksomheds- eller værkstedskortets nummer og den kortudstedende medlemsstat,

— virksomhedens eller værkstedets navn.

12.15. ***Data vedrørende særlige omstændigheder***

105a Kontrolapparatet skal registrere og i datalageret gemme følgende data vedrørende særlige omstændigheder:

— Indlæsningsdato og -klokkeslæt,

— Den særlige omstændigheds art.

105b Datalageret skal være i stand til at opbevare data vedrørende særlige omstændigheder i mindst 365 dage (idet det forudsættes, at der i gennemsnit åbnes og lukkes 1 omstændighed dagligt. Når lagerpladsen er opbrugt, skal nye data erstatte de ældste data.

13. **Læsning fra fartskriverkort**

106 Kontrolapparatet skal i givet fald kunne læse de data fra fartskriverkortene, som er nødvendige

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

— til kontrol af, at seneste kortsession blev afsluttet korrekt,

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

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

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

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

14. **Registrering og lagring på fartskriverkort**

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

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

109a Kontrolapparatet skal ajourføre de føreraktivitets- og steddata (som foreskrevet i kapitel IV, punkt 5.2.5 og 5.2.6), som er gemt på gyldige fører- og/eller værkstedskort, med de aktivitets- og steddata, som indlæses manuelt af kortindehaveren.

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

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

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

15. **Visning på skærm**

113 Skærmen skal have mindst 20 tegn.

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

114a Skærmen skal understøtte tegnsættene latin1 og græsk defineret ved ISO 8859 del 1 og 7, som foreskrevet i tillæg 1, kapitel 4 æt. Skærmen kan anvende forenklede tegn (f.eks. kan tegn med accent vises uden accent, eller små bogstaver kan vises som store).

115 Skærmen skal være forsynet med tilstrækkelig ikke blændende belysning.

116 Anvisningerne skal kunne ses udefra i forhold til kontrolapparatet.

117 Kontrolapparatet skal på skærmen kunne vise:

— automatisk valgte værdier,

— data vedrørende advarselssignaler,

— data vedrørende adgang via menu,

— andre data, som en bruger ønsker.

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

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

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

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

Skærmformatet er foreskrevet i tillæg 5.

15.1 ***Standardskærmbillede***

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

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

— funktionsmåde,

— aktuel føreraktivitet og aktuel medchaufføraktivitet,

— oplysninger vedrørende fører:

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

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

— oplysninger vedrørende medchauffør:

  — aktuel varighed af dennes aktivitet (siden den valgtes).

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

123 Giver skærmens bredde ikke mulighed for automatisk visning af funktionsmåde, skal kontrolapparatet kortvarigt vise den nye funktionsmåde, når den ændres.

124 Ved isætning af kort skal kontrolapparatet kortvarigt vise korthaverens navn.

124a Når omstændigheden »UDEN FOR GYLDIGHEDSOMRÅDE« åbnes, skal skærmen automatisk ved hjælp af det pågældende piktogram vise, at denne omstændighed er åbnet. (Det kan godtages, at den aktuelle føreraktivitet ikke nødvendigvis vises samtidigt).

15.2. ***Visning af oplysninger om advarselssignaler***

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

15.3. ***Adgang via menu***

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

15.4. ***Andre skærmbilleder***

127 På kommando skal skærmen selektivt kunne vise:

— UTC-dato and -klokkeslæt,

— funktionsmåde (hvis den ikke vises automatisk),

— førerens sammenhængende køretid og akkumulerede pausetid,

— medchaufførens sammenhængende køretid og akkumulerede pausetid,

— førerens akkumulerede køretid for den foregående og den aktuelle uge,

— medchaufførens akkumulerede køretid for den foregående og den aktuelle uge,

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

128 Visningen af udskriftens indhold skal være sekventiel, linje for linje. Er skærmen mindre end 24 tegn bred, skal brugeren have adgang til de fuldstændige oplysninger gennem en passende menu (flere linjer, rulning . . .). Udskriftslinjer, som er afsat til håndskrevne oplysninger, kan udelades på skærmen.

16. **Udskrivning**

129 Kontrolapparatet skal kunne udskrive oplysninger fra sit datalager og/eller fra fartskriverkort i henhold til nedenstående seks udskriftstyper:

— daglig udskrift af føreraktivitet fra kort,

— daglig udskrift af føreraktivitet fra køretøjsenhed,

— udskrift af hændelser og fejl fra kort,

— udskrift af hændelser og fejl fra køretøjsenhed,

— udskrift af tekniske data,

— udskrift af overskridelse af tilladt hastighed.

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

Yderligere data kan anføres sidst i udskrifterne

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

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

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

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

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

132 Printeren skal kunne udskrive 24 tegn pr. linje.

133 Den mindste tegnstørrelse er 2,1 mm i højden og 1,5 mm i bredden.

133a Printeren skal understøtte tegnsættene latin1 og græsk, defineret ved ISO 8859 del 1 og 7, som foreskrevet i tillæg 1, kapitel 4 »Tegnsæt«.

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

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

136 Papir, som skal anvendes af kontrolapparatet, skal være forsynet med det pågældende typegodkendelsesmærke og angivelse af de(n) type(r) kontrolapparat(er), det kan anvendes med. Udskrifterne skal forblive letlæselige og identificerbare under normale opbevaringsforhold mht. lysstyrke, fugtighed og temperatur i mindst et år.

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

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

17. **Advarselssignaler**

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

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

141 Kontrolapparatet skal advare føreren, når en sammenhængende køretid på 4 h. 30 min. overskrides, samt 15 minutter inden dette sker.

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

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

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

145 I sidstnævnte tilfælde skal de være forsynet med symbolet »T« og være gule eller orange.

146 Advarselssignaler skal have en varighed på mindst 30 sekunder, medmindre brugeren kvitterer ved at trykke på en vilkårlig knap i kontrolapparatet. Denne første kvittering må ikke slette det i næste afsnit omhandlede skærmbillede: Årsag til advarselssignal.

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

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

18. **Overførsel af data til eksterne medier**

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

150 Som en ikke obligatorisk facilitet kan kontrolapparatet desuden i enhver funktionsmåde gennem et andet stik overføre data til en virksomhed, hvis identitet er bekræftet gennem denne kanal. I så fald skal der for denne dataoverførsel gælde samme adgangsret til data som i virksomhedsmåde.

151 Overførslen må ikke ændre eller slette lagrede data.

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

Dataoverførselsprotokoller er specificeret i tillæg 7.

19. **Udlæsning af data til supplerende eksterne enheder**

152 Har kontrolapparatet ikke funktioner til visning af hastighed og/eller kilometerstand på skærmen, skal apparatet levere udgangssignal(er), der gør det muligt at vise køretøjets hastighed (speedometer) og/eller den samlede distance, køretøjet har tilbagelagt (kilometerstand).

153 Desuden skal køretøjsenheden kunne udlæse følgende data gennem en seriel dataforbindelse, som er uafhængig af en eventuel CAN-bus (ISO 11898 Road vehicles — Interchange of digital information — Controller Area Network (CAN) for high speed communication), således at disse data kan behandles af andre elektroniske enheder i køretøjet:

— Aktuel UTC-dato og -klokkeslæt,

— køretøjets hastighed,

— den samlede distance, som køretøjet har tilbagelagt (kilometerstand),

— aktuelt valgte aktivitet for fører og medchauffør,

— oplysninger om, hvorvidt der aktuelt er indsat et fartskriverkort i førerens kortplads og i medchaufførens kortplads og (i givet fald) oplysninger om identifikation af de tilsvarende kort (kortnummer og udstedende medlemsstat).

Andre data kan udlæses ud over disse mindstekrav.

Når køretøjets tænding er tilsluttet, skal disse data udsendes permanent. Når køretøjets tænding er afbrudt, skal i det mindste enhver ændring i førers eller medchaufførs aktivitet og/eller enhver isætning eller udtagning af et fartskriverkort medføre tilsvarende afsendelse af data. Er dataafsendelsen stillet i bero, mens køretøjets tænding er afbrudt, skal de pågældende data blive tilgængelige, når køretøjets tænding tilsluttes igen.

20. **Kalibrering**

154 Kalibreringsfunktionen skal give mulighed for:

— At bevægelsesføleren automatisk samparres med køretøjsenheden,

— at vejdrejetallet (k) digitalt tilpasses efter kontrolapparatets konstant (w) (køretøjer med to eller flere akseludvekslinger skal være forsynet med en omskifter, der automatisk bringer de forskellige reduktionsforhold i overensstemmelse med det, kontrolapparatet er blevet tilpasset til på køretøjet).

— at aktuelt klokkeslæt justeres (uden begrænsning),

— at aktuel kilometerstand justeres,

— at datalagerets identifikationsdata for bevægelsesføleren opdateres,

— at andre parametre, som kontrolapparatet har kendskab til, føres ajour eller bekræftes: Køretøjsidentifikation, w, l, dækstørrelse og, hvis relevant, fartbegrænserens indstilling.

155 Samparring af bevægelsesføler med køretøjsenhed skal i det mindste omfatte følgende:

— ajourføring af bevægelsesfølerens monteringsdata, som opbevares af bevægelsesføleren (efter behov),

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

156 Kalibreringsfunktionen skal kunne indlæse data gennem kalibrerings-/overførselsstikket i henhold til den i tillæg 8 fastlagte kalibreringsprotokol. Kalibreringsfunktionen kan derudover indlæse de nødvendige data gennem andre stik.

21. **Tidsjustering**

157 Tidsjusteringsfunktionen skal give mulighed for justering af aktuelt klokkeslæt i trin på højst 1 minut med intervaller på mindst 7 dage.

158 I kalibreringsmåde skal tidsjusteringsfunktionen give mulighed for justering af aktuelt klokkeslæt uden begrænsning.

22. **Funktionsspecifikationer**

159 Køretøjsenheden skal være fuldt funktionsdygtig i temperaturområdet – 20 °C til 70 °C, og bevægelsesføleren i temperaturområdet – 40 °C til 135 °C. Indholdet af datalageret skal bevares ved temperaturer ned til – 40 °C.

160 Kontrolapparatet skal være fuldt funktionsdygtigt i fugtighedsintervallet 10 % til 90 %.

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

162 Kontrolapparatet skal være i overensstemmelse med Kommissionens direktiv 95/54/EF ([1]) om tilpasning til den tekniske udvikling af Rådets direktiv 72/245/EØF om elektromagnetisk kompatibilitet, og skal være beskyttet mod elektrostatiske udladninger og spændingsvariationer.

23. **Materialer**

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

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

165 Køretøjsenheden skal opfylde beskyttelsesgrad IP 40, og bevægelsesføleren skal opfylde beskyttelsesgrad IP 64 i henhold til standard IEC 529.

166 Kontrolapparatet skal opfylde de pågældende tekniske forskrifter for ergonomisk udformning.

167 Kontrolapparatet skal være beskyttet mod hændelig beskadigelse.

24. **Mærkning**

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

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

([1]) EFT L 266 af 8.11.1995, s. 1.

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

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

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

— navn og adresse på fabrikanten af apparatet,

— fabrikantens reservedelsnummer og apparatets fremstillingsår,

— apparatets serienummer,

— kontrolapparattypens godkendelsesmærke.

170 Når der ikke er tilstrækkelig plads til at angive alle ovenstående enkeltheder, skal skiltet i det mindste angive: Fabrikantens navn eller mærke, og apparatets reservedelsnummer.

IV. KONSTRUKTIONS- OG FUNKTIONSKRAV TIL FARTSKRIVERKORT

1. **Synlige data**

Forsiden indeholder:

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

172 de samme ord på de andre fællesskabssprog, trykt sådan, at de danner baggrunden på kortet:

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 DEL CENTRO DI PROVA	CARTA DELL'AZIENDA
NL	BESTUURDERS KAART	CONTROLEKAART	CONTROLESTATION KAART	BEDRIJFSKAART
PT	CARTÃO DE CONDUTOR	CARTÃO DE CONTROLO	CARTÃO DO CENTRO DE ENSAIO	CARTÃO DE EMPRESA
FIN	KULJETTAJA KORTTILLA	VALVONTA KORTILLA	TESTAUSASEMA KORTILLA	YRITYSKORTILLA
SV	FÖRARKORT	KONTROLLKORT	VERKSTADSKORT	FÖRETAGSKORT

173 navnet på den medlemsstat, der har udstedt kortet (ikke obligatorisk);

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

B Belgien

DK Danmark

D Tyskland

GR Grækenland

E Spanien

F Frankrig

IRL Irland

I Italien

L Luxembourg

NL Nederlandene

A Østrig

P Portugal

FIN Finland

S Sverige

UK Det Forenede Kongerige

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

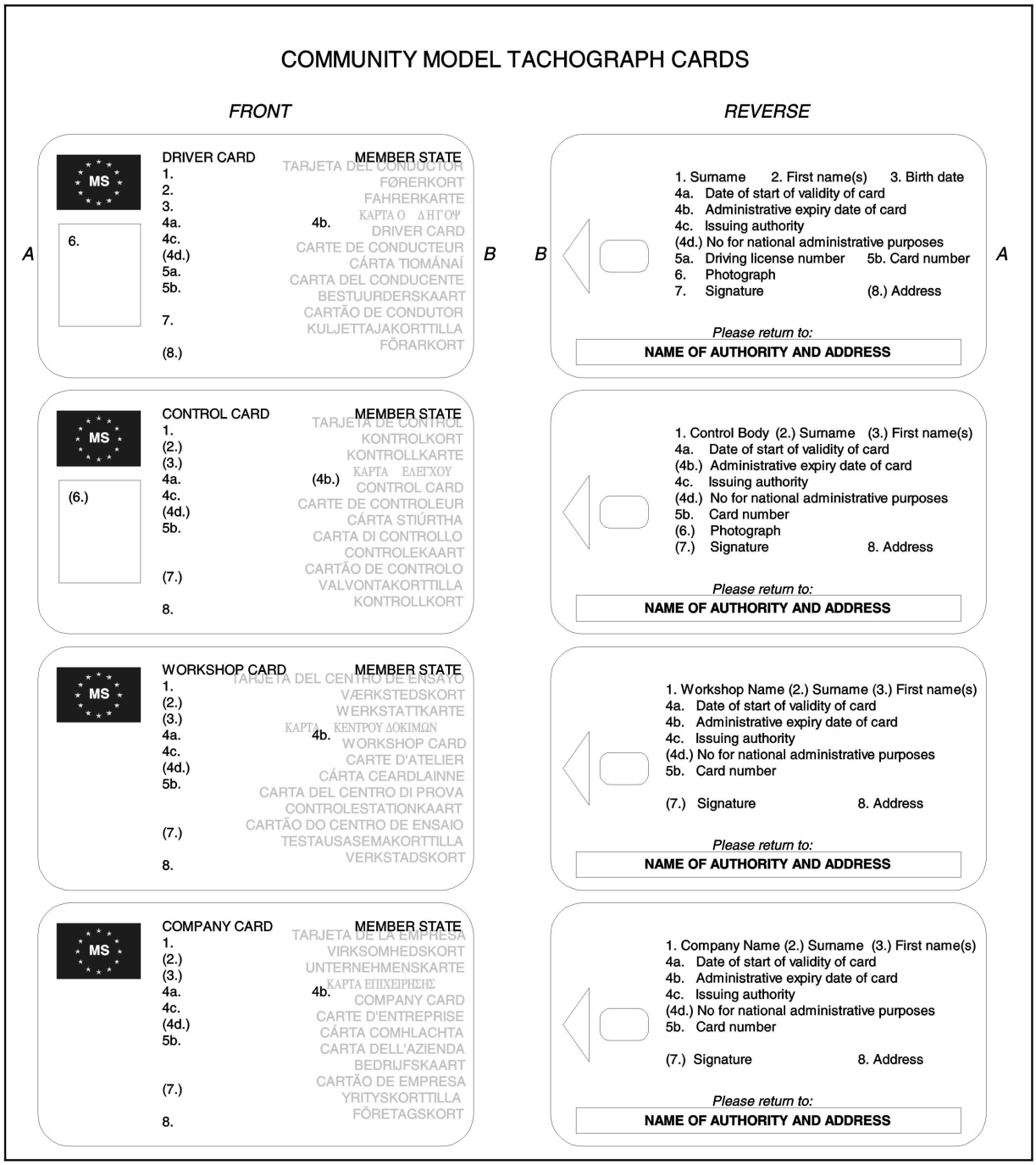
	Førerkort	Kontrolkort	Virksomheds- eller værkstedskort
1.	førerens efternavn	kontrolmyndighedens navn	virksomhedens eller værkstedets navn
2.	førerens fornavn(e)	den tilsynsførendes efternavn (hvis relevant)	kortindehaverens efternavn (hvis relevant)
3.	førerens fødselsdato	den tilsynsførendes fornavn(e) (hvis relevant)	kortindehaverens fornavn(e) (hvis relevant)
4.(a)	første dato i kortets gyldighedsperiode		
(b)	eventuel udløbsdato for kortet		
(c)	udstedende myndighed (kan være trykt på side 2)		
(d)	(evt.) nummer, der er forskelligt fra nummeret under punkt 5, til administrative formål		
5.(a)	Kørekortets nummer (på udstedelsesdatoen for førerkortet)	—	—
5.(b)	Kortnummer		
6.	Fotografi af føreren	(evt.) fotografi af den tilsynsførende	—
7.	Førerens underskrift	(evt.) indehaverens underskrift	
8.	(Evt.) førerens sædvanlige bopæl eller postadresse	Kontrolinstansens postadresse	firmaets eller værkstedets postadresse

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

Bagsiden indeholder:

177 En forklaring til de nummererede punkter på kortets forside;

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



179 Fartskriverkort skal være trykt med følgende dominerende baggrundsfarve:

— førerkort: hvid,

— kontrolkort: blå,

— værkstedskort rød,

— virksomhedskort: gul.

180 Fartskriverkort skal have mindst følgende egenskaber til beskyttelse mod forfalskning og indgreb fra uvedkommende:

— sikkerhedsbaggrund med fint slangeornament og regnbuetryk,

— i fotografiets område skal sikkerhedsbaggrund og fotografi overlappe,

— mindst én tofarvet mikroprintlinie.

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

2. **Sikkerhed**

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

182 Af hensyn til systemets sikkerhed skal fartskriverkortene opfylde sikkerhedsforskrifterne i de fælles sikkerhedsmål for fartskriverkort (tillæg 10).

183 Fartskriverkort skal kunne læses med andet udstyr som f.eks. PC'ere.

3. **Standarder**

184 Fartskriverkort skal være i overensstemmelse med følgende standarder:

— ISO/IEC 7810 Identification cards — Physical characteristics,

— ISO/IEC 7816 Identification cards — Integrated circuits with contacts:

  — Part 1: Physical characteristics,

  — Part 2: Dimensions and location of the contacts,

  — Part 3: Electronic signals and transmission protocols,

  — Part 4: Inter-industry commands for interchange,

  — Part 8: Security related inter-industry commands,

— ISO/IEC 10373 Identification cards — Test methods,

4. **Miljømæssige og elektriske specifikationer**

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

186 Fartskriverkort skal kunne fungere korrekt i fugtighedsintervallet 10 % til 90 %.

187 Fartskriverkort skal kunne fungere korrekt i fem år, hvis de anvendes i overensstemmelse med de miljømæssige og elektriske specifikationer.

188 Fartskriverkort skal under drift være i overensstemmelse med Kommissionens direktiv 95/54/EF af 31. oktober 1995 [1] om elektromagnetisk kompatibilitet, og skal være beskyttet mod elektrostatiske udladninger.

5. **Datalagring**

Med henblik på bestemmelserne i dette afsnit skal

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

— kilometerstand registreres med en opløsning på en kilometer,

— hastighed registreres med en opløsning på 1 km/h.

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

---

[1] EFT L 266 af 8.11.1995, s. 1.

189 I dette afsnit fastsættes tilladelig mindste lagerkapacitet til applikationens forskellige datafiler. Fartskriverkortene skal til kontrolapparatet kunne angive den faktiske lagerkapacitet til disse datafiler.

Skal kortet herudover benyttes til lagring af andre data vedrørende andre applikationer, som kortet understøtter, skal disse lagres i overensstemmelse med direktiv 95/46/EF [1].

5.1. ***Data vedrørende kortidentifikation og -sikkerhed***

5.1.1. *Identifikation af applikation*

190 Fartskriverkort skal kunne lagre følgende data til identifikation af applikationen:

— identifikation af fartskriverapplikation,

— identifikation af fartskriverkortets type.

5.1.2. *Identifikation af chip*

191 Fartskriverkort skal kunne lagre følgende data til identifikation af IC (IC = integreret kreds):

— IC-serienummer,

— IC-produktionshenvisninger.

5.1.3. *Identifikation af IC-kort*

192 Fartskriverkort skal kunne lagre følgende data til identifikation af chipkort:

— kortets serienummer (herunder produktionshenvisninger),

— kortets typegodkendelsesnummer,

— identifikation af kortnavn (ID),

— indlejrer-ID,

— IC-navn

5.1.4. *Sikkerhedselementer*

193 Fartskriverkort skal kunne lagre følgende data vedrørende sikkerhedselementer:

— Europæisk offentlig nøgle,

— Attest fra medlemsstaten,

— kortattest,

— privat kodenøgle for kortet.

5.2. ***Førerkort***

5.2.1. *Identifikation af kort*

194 Førerkortet skal kunne lagre følgende data til identifikation af kortet:

— kortnummer,

— udstedende medlemsstat, navn på udstedende myndighed, udstedelsesdato,

— startdato på kortets gyldighedsperiode, kortets udløbsdato.

5.2.2. *Identifikation af kortindehaver*

195 Førerkortet skal kunne lagre følgende data til identifikation af kortindehaver:

— indehaverens efternavn,

— indehaverens fornavn(e),

---

[1] EFT L 281 af 23.11.1995, s. 31.

— fødselsdato,

— foretrukket sprog.

5.2.3. *Oplysninger om førerbevis*

196 Førerkortet skal kunne lagre følgende data vedrørende førerbevis:

— udstedende medlemsstat, navn på udstedende myndighed,

— førerbevisets nummer (på kortets udstedelsesdato),

5.2.4. *Data vedrørende anvendte køretøjer*

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

— dato og klokkeslæt for første anvendelse af køretøjet (dvs. første kortisætning til denne anvendelsesperiode for køretøjet, eller 00h00 hvis det pågældende tidspunkt er inden for anvendelsesperioden),

— køretøjets kilometerstand på det pågældende tidspunkt,

— dato og klokkeslæt for seneste anvendelse af køretøjet (dvs. første kortudtagning med henblik på denne anvendelsesperiode for køretøjet, eller 23h59 hvis det pågældende tidspunkt er inden for anvendelsesperioden),

— køretøjets kilometerstand på det pågældende tidspunkt,

— køretøjets registreringsnummer og den indregistrerende medlemsstat,

198 Førerkortet skal kunne lagre mindst 84 sådanne poster.

5.2.5. *Føreraktivitetsdata*

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

— dato,

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

— førerstatus kl. 00.00,

— samlet distance tilbagelagt af føreren den pågældende dag,

— hver gang føreren har skiftet aktivitet og/eller kørestatus og/eller har isat eller udtaget sit kort:

  — kørestatus (FØRERHOLD, ÉN FØRER),

  — kortplads (FØRER, MEDCHAUFFØR),

  — kortstatus (ISAT, IKKE ISAT),

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

  — tidspunkt for ændringen.

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

201 De under forskrift 197 og 199 angivne data skal opbevares på en måde, som giver mulighed for at hente aktiviteterne i den rækkefølge, de har fundet sted, også når der er tidsmæssig overlapning.

5.2.6. *Steder, hvor den daglige arbejdstid begynder og/eller slutter*

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

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

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

— den indlæste stat og region,

— køretøjets kilometerstand.

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

5.2.7. *Data vedrørende hændelser*

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

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

— Tidsoverlapning (når kortet er årsag til denne hændelse),

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

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

— Afbrydelse i strømforsyningen,

— Fejl i køredata,

— Forsøg på sikkerhedsbrud.

205 Førerkortet skal kunne lagre følgende data vedrørende disse hændelser:

— Hændelseskode,

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

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

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

Bemærkning: For hændelsen »tidsoverlapning«:

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

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

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

Bemærkning: For hændelsen »Seneste kortsession ikke korrekt afsluttet«

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

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

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

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

5.2.8. *Data vedrørende fejl*

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

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

— Kortfejl (når kortet er genstand for hændelsen),

— Fejl ved kontrolapparatet.

208 Førerkortet skal kunne lagre følgende data vedrørende disse hændelser:

— Fejlkode,

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

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

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

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

5.2.9. *Data vedrørende kontrolaktivitet*

210 Førerkortet skal kunne lagre følgende data vedrørende kontrolaktiviteter:

— kontroldato og -klokkeslæt,

— kontrolkortets nummer og den kortudstedende medlemsstat,

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

— Ved dataoverførsel, den overførte periode,

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

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

211 Førerkortet skal kunne opbevare én sådan post.

5.2.10. *Kortsessionsdata*

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

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

— køretøjets registreringsnummer og den indregistrerende medlemsstat.

5.2.11. *Data vedrørende særlige omstændigheder*

212a Førerkortet skal kunne opbevare følgende data vedrørende særlige omstændigheder, som er indlæst, mens kortet var isat (uanset i hvilken kortplads):

— Indlæsningsdato og -klokkeslæt,

— Den særlige omstændigheds art.

212b Førerkortet skal kunne lagre mindst 56 sådanne poster.

5.3. ***Værkstedskort***

5.3.1. *Sikkerhedselementer*

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

214 Værkstedskortet skal kunne lagre de kryptografiske nøgler, som er nødvendige for at samparre bevægelsesfølere med køretøjsenheder.

5.3.2. *Identifikation af kort*

215 Værkstedskortet skal kunne lagre følgende data til kortidentifikation:

— kortnummer,

— udstedende medlemsstat, navn på udstedende myndighed, udstedelsesdato,

— startdato på kortets gyldighedsperiode, kortets udløbsdato.

5.3.3. *Identifikation af kortindehaver*

216 Værkstedskortet skal kunne lagre følgende data til identifikation af kortindehaver:

— værkstedets navn,

— værkstedets adresse,

— indehaverens efternavn,

— indehaverens fornavn(e),

— foretrukket sprog.

5.3.4. *Data vedrørende anvendte køretøjer*

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

218 Værkstedskortet skal kunne lagre mindst 4 sådanne poster.

5.3.5. *Føreraktivitetsdata*

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

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

5.3.6. *Data vedrørende steder, hvor den daglige arbejdstid begynder og/eller slutter*

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

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

5.3.7. *Data vedrørende hændelser og fejl*

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

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

5.3.8. *Data vedrørende kontrolaktivitet*

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

5.3.9. *Kalibrerings- og tidsjusteringsdata*

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

227 Hver kalibreringspost skal kunne indeholde følgende data:

— Kalibreringens formål (første montering, montering, periodisk eftersyn),

— Identifikation af køretøjet,

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

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

228 Værkstedskortet skal kunne lagre mindst 88 sådanne poster.

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

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

5.3.10. *Data vedrørende særlige omstændigheder*

230a Værkstedskortet skal kunne lagre data vedrørende særlige omstændigheder på samme måde som et førerkort. Værkstedskortet skal kunne opbevare 2 sådanne poster.

5.4. ***Kontrolkort***

5.4.1. *Identifikation af kort*

231 Kontrolkortet skal kunne lagre følgende data til kortidentifikation:

— kortnummer,

— udstedende medlemsstat, navn på udstedende myndighed, udstedelsesdato,

— startdato på kortets gyldighedsperiode, kortets eventuelle udløbsdato.

5.4.2. *Identifikation af kortindehaver*

232 Kontrolkortet skal kunne lagre følgende data til identifikation af kortindehaveren:

— kontrolinstansens navn,

— kontrolinstansens adresse,

— indehaverens efternavn,

— indehaverens fornavn(e),

— foretrukket sprog.

5.4.3. *Data vedrørende kontrolaktivitet*

233 Kontrolkortet skal kunne lagre følgende data vedrørende kontrolaktivitet:

— kontroldato og -klokkeslæt,

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

— eventuel periode, som er overført,

— Køretøjets registreringsnummer og den indregistrerende myndighed i det kontrollerede køretøj,

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

234 Kontrolkortet skal kunne lagre mindst 230 sådanne poster.

5.5. ***Virksomhedskort***

5.5.1. *Identifikation af kort*

235 Virksomhedskortet skal kunne lagre følgende data til kortidentifikation:

— kortnummer,

— udstedende medlemsstat, navn på udstedende myndighed, udstedelsesdato,

— startdato på kortets gyldighedsperiode, kortets eventuelle udløbsdato.

5.5.2. *Identifikation af kortindehaver*

236 Virksomhedskortet skal kunne lagre følgende data til identifikation af kortindehaveren:

— virksomhedens navn,

— virksomhedens adresse.

5.5.3. *Virksomhedsaktivitetsdata*

237 Virksomhedskortet skal kunne lagre følgende virksomhedsaktivitetsdata:

— dato og klokkeslæt for aktiviteten,

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

— eventuel periode, som er overført,

— Køretøjets registreringsnummer og den myndighed, som har registreret det,

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

238 Virksomhedskortet skal kunne opbevare mindst 230 sådanne poster.

V. MONTERING AF KONTROLAPPARATET

1. **Montering**

239 Nye kontrolapparater skal leveres i ikke-aktiveret stand til installatører eller køretøjsfabrikanter, med alle de i kapitel III.20 opregnede kalibreringsparametre sat til hensigtsmæssige og gyldige standardværdier. Når ingen særlig værdi er passende, sættes strengparametre til værdien »?« og talparametre til »0«.

240 Inden kontrolapparatet er aktiveret, skal kontrolapparatet give adgang til kalibreringsfunktionen, også når det ikke er i kalibreringsmåde.

241 Før kontrolapparatet er aktiveret, må det hverken registrere eller lagre de i III.12.3. til III.12.9. og III.12.12 til III.12.14. inkl. omhandlede data.

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

243 Køretøjsfabrikant eller installatør skal aktivere det monterede kontrolapparat, før køretøjet forlader de lokaler, hvor monteringen fandt sted.

244 Kontrolapparatet skal automatisk aktiveres ved første indsætning af et værkstedskort i en af dets kortlæsere.

245 Eventuelle nødvendige særlige samparringsprocedurer mellem bevægelsesføler og køretøjsenhed skal udføres automatisk før eller under aktivering.

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

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

248 Monteringen skal efterfølges af en kalibrering. Køretøjets registreringsnummer indlæses ved den første kalibrering, som finder sted inden for to uger efter denne montering, dog senest to uger efter tildeling af registreringsnummer, hvis denne finder sted senere end monteringen.

248a Kontrolapparatet skal være anbragt på en sådan måde i køretøjet, at føreren har adgang til de nødvendige funktioner fra førersædet.

2. **Installationsplade**

249 Når apparatet er blevet kontrolleret efter monteringen, anbringes en monteringsplade klart synligt og lettilgængeligt på eller ved siden af apparatet. Efter ethvert indgreb foretaget af en autoriseret installatør eller et autoriseret værksted skal installationspladen udskiftes med en ny plade.

250 Pladen skal være forsynet med mindst følgende oplysninger:

— Den autoriserede installatørs eller det autoriserede værksteds navn og adresse eller firmanavn,

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

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

— Effektiv dækperiferi i formen »l = . . . mm«,

— Dækstørrelse,

— Datoen for bestemmelse af køretøjets vejdrejetal og måling af dets effektive dækperiferi,

— Køretøjets identifikationsnummer.

3. **Plombering**

251 Følgende dele skal være plomberet:

— Tilslutninger, hvis afbrydelse medfører uopdagede ændringer eller uopdaget tab af data;

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

252 Ovennævnte plomberinger kan brydes:

— I nødstilfælde,

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

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

VI. KONTROL, EFTERSYN OG REPARATIONER

Kapitel V, punkt 3 i dette bilag indeholder bestemmelser for, under hvilke omstændigheder plomber må fjernes som omhandlet i artikel 12, stk. 5 af forordning (EØF) nr. 3821/85, senest ændret ved forordning (EF) nr. 2135/98.

1. **Autorisering af installatører eller værksteder**

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

— montering,

— eftersyn,

— kontrol,

— reparationer.

I rammerne af artikel 12, stk. 1 i denne forordning vil værkstedskort alene blive udstedt til installatører og/eller værksteder, som er godkendt til aktivering og/eller kalibrering af kontrolapparater i overensstemmelse med dette bilag, og som, medmindre det behørigt begrundes:

— ikke er berettiget til et virksomhedskort;

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

2. **Kontrol af nye eller reparerede instrumenter**

254 For hver enkelt ny eller repareret anordning kontrolleres den korrekte funktion og nøjagtigheden af angivelser og optegnelser inden for de i kapitel III, punkt 2.1. og 2.2 fastlagte grænser ved plombering i henhold til kapitel V, punkt 3, og kalibrering.

3. **Monteringseftersyn**

255 Ved monteringen i et køretøj skal apparatet og hele installationen opfylde bestemmelserne i kapitel III, punkt 2.1 og 2.2 vedrørende maksimale tolerancer.

4. **Periodiske eftersyn**

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

257 Disse eftersyn skal omfatte følgende kontroller:

— at kontrolapparatet fungerer korrekt, herunder også lagring af data på fartskriverkortet,

— at overholdelse af bestemmelserne i kapitel III, punkt 2.1 og 2.2 om maksimale tolerancer ved monteringen er sikret,

— at kontrolapparatet er forsynet med typegodkendelsesmærke,

— at monteringspladen er anbragt,

— at plomberne på apparatet og på anlæggets øvrige dele er intakte,

— dækstørrelsen og den faktiske dækperiferi.

258 Disse eftersyn skal omfatte en kalibrering.

5. **Måling af fejl**

259 Måling af fejl, som opstår under montering og drift, udføres under følgende betingelser, der skal betragtes som normale prøvebetingelser:

— ubelastet køretøj i køreklar stand,

— dæktryk i overensstemmelse med fabrikantens angivelser,

— dækslitage inden for de ved national lov givne grænser,

— køretøjets bevægelse:

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

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

6. **Reparationer**

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

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

VII. UDSTEDELSE AF KORT

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

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

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

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

265 Et fartskriverkort, som udstedes til erstatning for et eksisterende fartskriverkort, skal have samme udløbsdato som det erstattede.

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

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

268 »Kortindehavers efternavn« skal for ikke personlige værksteds- eller kontrolkort udfyldes med værkstedets eller kontrolinstansens navn.

VIII. TYPEGODKENDELSE AF KONTROLAPPARATUR OG FARTSKRIVERKORT

1. **Generelt**

I dette afsnit forstås ved »kontrolapparat«, »kontrolapparatet eller dets komponenter«. Der kræves ingen typegodkendelse af de(t) kabel (kabler), som forbinder bevægelsesføler med køretøjsenhed. Det papir, som skal anvendes af kontrolapparatet, anses for en komponent i kontrolapparatet.

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

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

271 Medlemsstaternes typegodkendelsesmyndigheder udsteder ikke typegodkendelsesattest i overensstemmelse med artikel 5 i denne forordning, medmindre de er i besiddelse af:

— en sikkerhedsattest,

— en funktionsattest,

— og en interoperabilitetsattest

for det kontrolapparat eller det fartskriverkort, som typegodkendelsesansøgningen omfatter.

272 Enhver ændring af en af apparatets komponenter eller af arten af de til dets fremstilling anvendte materialer skal, inden apparatet tages i brug, anmeldes til den myndighed, som har typegodkendt apparatet. Denne myndighed skal over for fabrikanten bekræfte udvidelsen af typegodkendelsen eller kan kræve opdatering eller bekræftelse af de relevante funktions-, sikkerheds- og/eller interoperabilitetsattester.

273 Procedurer til opgradering af programmel i allerede monteret kontrolapparat skal være godkendt af den myndighed, som meddelte typegodkendelse af kontrolapparatet. Opgradering af programmel må ikke ændre eller slette føreraktivitetsdata, som er gemt i kontrolapparatet. Programmel må kun opgraderes under ansvar af kontrolapparatets fabrikant.

2. **Sikkerhedsattest**

274 Sikkerhedsattesten udstedes i overensstemmelse med bestemmelserne i tillæg 10 til dette bilag.

3. **Funktionsattest**

275 Ansøgere til typegodkendelse skal forsyne medlemsstatens typegodkendelsesmyndigheder med alt det materiale og al den dokumentation, som myndigheden anser for nødvendigt.

276 Der må ikke udstedes en funktionsattest til fabrikanten, før mindst alle de i tillæg 9 foreskrevne funktionsprøver er udført med tilfredsstillende resultat.

277 Funktionsattesten udstedes af typegodkendelsesmyndigheden. Denne attest skal ud over navnet på modtageren og identifikation af modellen indeholde en specificeret liste over de udførte prøver og resultaterne heraf.

4. **Interoperabilitetsattest**

278 Interoperabilitetsprøver udføres af ét enkelt laboratorium under Europa-Kommissionens myndighed og ansvar.

279 Laboratoriet registrerer de af fabrikanterne indgivne anmodninger om interoperabilitetsprøver i den kronologiske rækkefølge, de modtages.

280 Anmodningerne vil først blive officielt registreret, når laboratoriet er i besiddelse af:

— det fuldstændige sæt materiale og dokumenter, som er nødvendige til sådanne interoperabilitetsprøver,

— den tilsvarende sikkerhedsattest,

— den tilsvarende funktionsattest,

Fabrikanten underrettes om datoen for registreringen.

281 Laboratoriet udfører ikke interoperabilitetsprøvning af kontrolapparater eller fartskriverkort, for hvilke der ikke er udstedt en sikkerhedsattest og en funktionsattest.

282 Enhver fabrikant, som anmoder om interoperabilitetsprøver, forpligter sig til at overlade hele det sæt materiale og dokumenter, som han har fremskaffet med henblik på udførelse af prøverne, til det laboratorium, som forestår prøverne.

283 Interoperabilitetsprøver skal udføres i overensstemmelse med bestemmelserne i punkt 5 i bilag 9 til dette bilag, og i prøverne skal henholdsvis indgå alle de typer kontrolapparater og fartskriverkort:

— for hvilke typegodkendelsen stadig er gyldig eller,

— for hvilke typegodkendelsen er under behandling, og for hvilke der foreligger en gyldig interoperabilitetsattest.

284 Der må ikke udstedes en interoperabilitetsattest til fabrikanten, før mindst alle de foreskrevne interoperabilitetsprøver er udført med tilfredsstillende resultat.

285 Giver interoperabilitetsprøverne ikke tilfredsstillende resultat med en (et) eller flere af kontrolapparaterne eller fartskriverkortene som foreskrevet i krav 283, vil interoperabilitetsattesten ikke blive udstedt, før den anmodende fabrikant har gennemført de nødvendige ændringer og interoperabilitetsprøverne har givet tilfredsstillende resultat. Laboratoriet skal udfinde årsagen til problemet med assistance fra de fabrikanter, der berøres af denne interoperabilitetsmangel og skal søge at bistå den anmodende producent med at finde en teknisk løsning. I tilfælde, hvor fabrikanten har ændret sit produkt, påhviler det fabrikanten at søge de pågældende myndigheders bekræftelse på, at sikkerhedsattest og funktionsattest stadig er gyldige.

286 Interoperabilitetsattesten er gyldig i seks måneder. Efter slutningen af denne periode ophæves den, hvis fabrikanten ikke har modtaget en tilsvarende typegodkendelsesattest. Den fremsendes af fabrikanten til den typegodkendende myndighed i den medlemsstat, som har udstedt funktionsattesten.

287 Intet element, som kan tænkes at give anledning til en interoperabilitetsmangel, må anvendes til at opnå fortjeneste eller til at opnå en dominerende stilling.

5. **Typegodkendelsesattest**

288 Den typegodkendende myndighed i medlemsstaten kan udstede typegodkendelsesattesten, så snart den er i besiddelse af de nødvendige tre attester.

289 Typegodkendelsesattesten kopieres af den typegodkendende myndighed til det laboratorium, som forestår interoperabilitetsprøverne, på det tidspunkt hvor den udstedes til fabrikanten.

290 Det laboratorium, som forestår interoperabilitetsprøverne, skal have et offentligt web-sted med en opdateret liste over de kontrolapparat- eller fartskrivermodeller,

— for hvilke der er registreret en anmodning om interoperabilitetsprøver,

— for hvilke der er udstedt en interoperabilitetsattest (også selv om den er foreløbig),

— for hvilke der er udstedt en typegodkendelsesattest.

6. **Undtagelsesprocedure: Indledende interoperabilitetsattester**

291 I en periode på fire måneder efter at et første sammenhørende sæt kontrolapparat og tilhørende fartskriverkort (fører-, værksteds-, kontrol- og virksomhedskort) er attesteret som interoperabelt, anses en eventuelt udstedt interoperabilitetsattest (herunder også denne allerførste attest) vedrørende anmodninger registreret i denne periode, for foreløbig.

292 Anses alle de omhandlede produkter efter slutningen af denne periode for indbyrdes interoperable, bliver alle tilsvarende interoperabilitetsattester endelige.

293 Findes der i løbet af denne periode interoperabilitetsmangel, skal det laboratorium, som forestår interoperabilitetsprøverne, finde årsagerne til problemerne med assistance fra alle de berørte fabrikanter og opfordre dem til at gennemføre de nødvendige ændringer.

294 Tilbagestår der efter slutningen af denne periode interoperabilitetsproblemer, skal det laboratorium, som forestår interoperabilitetsprøverne, i samarbejde med de pågældende fabrikanter og med de typegodkendelsesmyndigheder, som udstedte de tilsvarende funktionsattester, finde årsagen til interoperabilitetsmanglerne og fastlægge, hvilke ændringer hver af de pågældende fabrikanter bør foretage. Søgningen efter tekniske løsninger må vare højst to måneder; findes der derved ingen fælles løsning, tager Kommissionen efter samråd med det laboratorium, som forestår interoperabilitetsprøverne, stilling til, hvilke(t) apparat(er) og kort, der skal udstedes en endelig interoperabilitetsattest for, og angiver begrundelse herfor.

295 Eventuelle anmodninger om interoperabilitetstests, som af laboratoriet registreres i perioden fra fire måneder efter udstedelse af den første foreløbige interoperabilitetsattest til datoen for den i krav 294 omhandlede Kommissionsbeslutning, stilles i bero, til de første interoperabilitetsproblemer er løst. Disse anmodninger behandles derefter i samme kronologiske rækkefølge, som de er registreret.

Tillæg 1

DATAORDLISTE

1. INDLEDNING

Dette tillæg fastlægger de dataformater, dataelementer og datastrukturer, som skal anvendes i kontrolapparater og fartskriverkort.

1.1. **Fremgangsmåde anvendt ved definition af datatyper**

Til definition af datatyperne i dette tillæg er anvendt Abstract Syntax Notation One (ASN.1). På denne måde kan der defineres enkle og strukturerede data, uden at dette forudsætter en nærmere bestemt overføringssyntaks (kodningsregler), som vil være applikations- og miljøafhængig.

ASN.1 typebenævnelser er tildelt efter ISO/IEC 8824-1. Dette indebærer:

— at datatypens betydning, hvor det er muligt, er givet gennem de valgte navne,

— at når en datatype er sammensat af andre datatyper, består datatypens navn stadig af én enkelt sekvens af alfabetiske tegn med stort begyndelsesbogstav, dog anvendes store bogstaver inde i navnet til at angive den tilsvarende betydning.

— at datatypernes navne sædvanligvis hænger sammen med navnet på de datatyper, de er opbygget af, det udstyr, data bliver lagret på, og den funktion, der knytter sig til de pågældende data.

Er en ASN.1 type i forvejen defineret som del af en anden standard og relevant til brug i kontrolapparatet, vil den pågældende ASN.1 type være defineret i dette tillæg.

For at give mulighed for forskellige typer kodningsregler er visse ASN.1 typer i dette tillæg begrænset ved identifikatorer for værdiområdet. Identifikatorerne for værdiområde er definereret i punkt 3.

1.2. **Referencer**

I dette tillæg henvises til følgende referencer:

ISO 639	Code for the representation of names of languages. First Edition: 1988.
EN 726-3	Identification cards systems — Telecommunications integrated circuit(s) cards and terminals — Part 3: Application independent card requirements. December 1994.
ISO 3779	Road vehicles — Vehicle identification number (VIN) — Content and structure. Edition 3: 1983.
ISO/IEC 7816-5	Information technology — Identification cards — Integrated circuit(s) cards with contacts — Part 5: Numbering system and registration procedure for application identifiers. First edition: 1994 + Amendment 1: 1996.
ISO/IEC 8824-1	Information technology — Abstract Syntax Notation 1 (ASN.1): Specification of basic notation. Edition 2: 1998.
ISO/IEC 8825-2	Information technology — ASN.1 encoding rules: Specification of Packed Encoding Rules (PER). Edition 2: 1998.
ISO/IEC 8859-1	Information technology — 8 bit single-byte coded graphic character sets — Part 1: Latin alphabet No.1. First edition: 1998.
ISO/IEC 8859-7	Information technology — 8 bit single-byte coded graphic character sets — Part 7: Latin/Greek alphabet. First edition: 1987.
ISO 16844-3	Road vehicles — Tachograph systems — Motion Sensor Interface. WD 3-20/05/99.

2. DEFINITIONER AF DATATYPER

For nedenstående datatyper vil datafeltet som standardværdi for »ukendt« eller »ikke relevant« indhold være udfyldt med sideskiftbyte.

2.1. **ActivityChangeInfo**

Med denne datatype kan der inden for et to byte stort ord kodes skift af kortlæserstatus kl. 00:00 og/eller førerstatus kl. 00:00 og/eller skift af aktivitet og/eller skift af kørestatus og/eller skift af kortstatus for en fører eller medchauffør. Denne datatype er knyttet til krav 084, 109a, 199 og 219.

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

Tilordnet værdi — Oktet udsluttet: `'scpaatttttttttt'B` (16 Bit)

Til registrering i datalager (eller kortlæserstatus):

`'s'B` Kortplads:

`'0'B`: FØRER,

`'1'B`: MEDCHAUFFØR,

`'c'B` Kørestatus:

`'0'B`: ÉN FØRER,

`'1'B`: FØRERHOLD,

`'p'B` Status for fører- (eller værksteds-) kortet i den pågældende kortplads:

`'0'B`: ISAT, der er isat et kort,

`'1'B`: IKKE ISAT, kort er ikke isat (eller er taget ud),

`'aa'B` Aktivitet:

`'00'B`: PAUSE/HVILE,

`'01'B`: RÅDIGHED,

`'10'B`: ARBEJDE,

`'11'B`: KØRSEL,

`'ttttttttttt'B` Klokkeslæt for skiftet: Antal minutter siden 00h00 det pågældende døgn.

For registrering med fører- eller værkstedskort (og førerstatus):

`'s'B` Kortplads (ikke relevant når 'p' = 1, se dog bemærkning nedenfor):

`'0'B`: FØRER,

`'1'B`: MEDCHAUFFØR,

`'c'B` Kørestatus (tilfældet 'p' = 0) eller Efterfølgende aktivitetsstatus (tilfældet 'p' = 1):

`'0'B`: ÉN FØRER `'0'B`: UKENDT

`'1'B`: FØRERHOLD, `'1'B`: KENDT (= manuelt indlæst)

`'p'B` Kortstatus:

`'0'B`: ISAT, kortet er sat i et kontrolapparat,

`'1'B`: IKKE ISAT, kortet er ikke isat (eller er taget ud),

'aa'B Aktivitet (ikke relevant når 'p' = 1 og 'c' = 0, se dog bemærkning nedenfor):

'00'B: PAUSE/HVILE,

'01'B: RÅDIGHED,

'10'B: ARBEJDE,

'11'B: KØRSEL,

'ttttttttttt'B Klokkeslæt for ændringen: Antal minutter siden 00h00 det pågældende døgn.

Bemærkning vedrørende tilfældet »udtagning af kort«:

Når kortet er taget ud:

— 's' er relevant og angiver den kortplads, kortet er fjernet fra,

— 'c' skal være sat til 0,

— 'p' skal være sat til 1,

— 'aa' skal kode den aktuelle aktivitet, som er valgt på det pågældende tidspunkt,

Bit 'c' og 'aa' i ordet (gemt på et kort) kan ved senere manuel indlæsning overskrives svarende til indlæsningen.

2.2. **Address**

En adresse.

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

codePage angiver den del af ISO/IEC 8859, som er anvendt til at kode adressen,

address er en adresse, som er kodet i henhold til ISO/IEC 8859-codePage.

2.3. **BCDString**

BCDString anvendes til at fremstille decimaltal ved binær kode (BCD). Denne datatype anvendes til at fremstille ét decimalciffer ved én semioktet (4 bit). BCDString er baseret på ISO/IEC 8824-1 »'CharacterStringType'«.

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

BCDString anvender »hstring« notation. Det hexadecimale tegn længst til venstre skal være mest betydende semioktet i første oktet. Til frembringelse af flere oktetter indsættes efter behov foranstillede nul-semioktetter fra semioktetpositionen længst til venstre i den første oktet.

De tilladte cifre er: 0, 1, . . . 9.

2.4. **CalibrationPurpose**

Kode, som forklarer hvorfor der blev registreret et sæt kalibreringsparametre. Denne datatype er knyttet til krav 097 og 098.

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

Tilordnet værdi:

'00'H reserveret værdi,

'01'H aktivering: Registrering af de kalibreringsparametre, som er kendt i det øjeblik, hvor køretøjsenheden aktiveres,

'02'H første installation: Første kalibrering af køretøjsenheden efter at den er aktiveret,

'03'H installation: Første kalibrering af køretøjsenheden i det aktuelle køretøj,

'04'H periodisk eftersyn.

2.5. **CardActivityDailyRecord**

Oplysninger, gemt på kortet, vedrørende føreraktiviteterne for en given kalenderdag. Denne datatype er knyttet til krav 199 og 219.

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

activityPreviousRecordLength er den totale længde i byte af den foregående døgnpost. Maksimumværdien er givet ved længden af den OCTET STRING, som indeholder disse poster (se CardActivityLengthRange punkt 3). Når denne post er den ældste døgnpost, skal activityPreviousRecordLength sættes til værdien 0.

activityRecordLength er den totale længde i byte af denne post. Maksimumværdien er givet ved længden af den OCTET STRING, som indeholder disse poster.

activityRecord Date er postens dato.

activityDailyPresenceCounter er tælleren for daglig tilstedeværelse det pågældende døgn.

activityDayDistance er den totale distance, som er tilbagelagt det pågældende døgn.

activityChangeInfo er datasættet ActivityChangeInfo for føreren det pågældende døgn. Det kan indeholde indtil 1 440 værdier (ét aktivitetsskift pr. minut). Dette datasæt indeholder altid ActivityChangeInfo med kode for førerstatus kl. 00:00.

2.6. **CardActivityLengthRange**

Antal bytes, som i et fører- eller værkstedskort er til rådighed for lagring af poster vedrørende føreraktivitet.

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

Tilordnet værdi: Se punkt 3.

2.7. **CardApprovalNumber**

Kortets typegodkendelsesnummer.

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

Tilordnet værdi: Uspecificeret.

2.8. **CardCertificate**

Certifikat for et korts offentlige nøgle.

```
CardCertificate ::= Certificate
```

2.9. **CardChipIdentification**

Oplysninger, gemt på et kort, vedrørende identifikation af kortets integrerede kreds (IC) (krav 191).

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

icSerialNumber er serienummeret på den integrerede kreds som defineret i EN 726-3.

icManufacturingReferences er datanavnet for producenten af den integrerede kreds og produktionsdataelementer som defineret i EN 726-3.

2.10. **CardConsecutiveIndex**

Et fortløbende kortindeks (definition h)).

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

Tilordnet værdi: (Se kapitel VII i dette bilag)

Rækkefølge af forøgelse: '0, . . ., 9, A, . . ., Z, a, . . . , z'

2.11. **CardControlActivityDataRecord**

Oplysninger, gemt på et fører- eller værkstedskort, vedrørende den seneste kontrol, som føreren har været genstand for (krav 210 og 225).

```
CardControlActivityDataRecord ::= SEQUENCE {
   controlType                          ControlType,
   controlTime                          TimeReal,
   controlCardNumber                    FullCardNumber,
   controlVehicleRegistration           VehicleRegistrationIdentification,
   controlDownloadPeriodBegin           TimeReal,
   controlDownloadPeriodEnd             TimeReal
}
```

controlType er kontrollens type.

controlTime er dato og klokkeslæt for kontrollen.

controlCardNumber er FullCardNumber for den kontrollør, som har foretaget kontrollen.

controlVehicleRegistration er indregistreringsnummer og registrerende medlemsstat for det køretøj, i hvilket kontrollen fandt sted.

controlDownloadPeriodBegin og **controlDownloadPeriodEnd** angiver, ved dataoverførsel, den periode, for hvilken dataoverførsel har fundet sted.

2.12. **CardCurrentUse**

Oplysninger om kortets aktuelle anvendelse (krav 212).

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

sessionOpenTime er det tidspunkt, hvor kortet er indsat med henblik på den aktuelle anvendelse. Dette dataelement sættes til nul, når kortet tages ud.

sessionOpenVehicle er identifikationen af det aktuelt anvendte køretøj og bliver sat ved isætning af kortet. Dette dataelement sættes til nul, når kortet tages ud.

2.13. **CardDriverActivity**

Oplysninger, gemt på et fører- eller værkstedskort, vedrørende førerens aktiviteter (krav 199 og 219).

```
CardDriverActivity ::= SEQUENCE {
   activityPointerOldestDayRecord       INTEGER(0..CardActivityLengthRange-1),
   activityPointerNewestRecord          INTEGER(0..CardActivityLengthRange-1),
   activityDailyRecords                 OCTET STRING
                                        (SIZE(CardActivityLengthRange))
}
```

activityPointerOldestDayRecord angiver begyndelsen på lagerpladsen (antal byte fra strengens begyndelse) for den ældste fuldstændige døgnpost i activityDailyRecords strengen. Maksimumværdien er givet ved længden af strengen.

activityPointerNewestRecord angiver begyndelsen på lagerpladsen (antal byte fra strengens begyndelse) for den seneste døgnpost i activityDailyRecords strengen. Maksimumværdien er givet ved længden af strengen.

activityDailyRecords er den plads, der er til rådighed til lagring af føreraktivitetsdata (datastruktur: CardActivityDailyRecord) for hver kalenderdag, kortet har været benyttet.

Tilordnet værdi: Denne oktetstreng bliver cyklisk fyldt op med poster vedrørende CardActivityDailyRecord. Ved første gangs brug begynder lagringen ved strengens første byte. Alle nye poster bliver hæftet til slutningen af den foregående. Når strengen er fuld, fortsætter lagringen ved strengens første byte uafhængigt af, om der eventuelt er en afbrydelse inde i et dataelement. Før nye aktivitetsdata placeres i strengen (ved at den aktuelle activityDailyRecord bliver større, eller ved at der indsættes en ny activityDailyRecord) som erstatning for ældre aktivitetsdata, skal activityPointerOldestDayRecord opdateres svarende til den nye placering af den ældste fuldstændige døgnpost, og activityPreviousRecordLength for denne (nye) ældste fuldstændige døgnpost skal stilles tilbage på 0.

2.14. **CardDrivingLicenceInformation**

Oplysninger, gemt på et førerkort, vedrørende kortindehaverens licensdata (krav 196).

```
CardDrivingLicenceInformation ::= SEQUENCE {
   drivingLicenceIssuingAuthority         Name,
   drivingLicenceIssuingNation            NationNumeric,
   drivingLicenceNumber                   IA5String(SIZE(16))
}
```

drivingLicenceIssuingAuthority er den myndighed, som er ansvarlig for udstedelse af førerbeviset.

drivingLicenceIssuingNation er nationaliteten af den myndighed, som har udstedt førerbeviset.

drivingLicenceNumber er førerbevisets nummer.

2.15. **CardEventData**

Oplysninger, gemt på et fører- eller værkstedskort, vedrørende hændelser knyttet til kortindehaveren (krav 204 og 223).

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

CardEventData er en sekvens af cardEventRecords, ordnet efter stigende EventFaultType, (bortset fra poster vedrørende forsøg på sikkerhedsbrud, som er samlet i sekvensens sidste mængde).

cardEventRecords er en mængde af hændelsesposter af en given hændelsestype (eller kategori ved hændelser bestående i forsøg på sikkerhedsbrud).

2.16. **CardEventRecord**

Oplysninger, gemt på et fører- eller værkstedskort, vedrørende en hændelse knyttet til kortindehaveren (krav 205 og 223).

```
CardEventRecord ::= SEQUENCE {
   eventType                              EventFaultType,
   eventBeginTime                         TimeReal,
   eventEndTime                           TimeReal,
   eventVehicleRegistration               VehicleRegistrationIdentification
}
```

eventType er hændelsens type.

eventBeginTime er hændelsens startdato og -klokkeslæt.

eventEndTime er hændelsens slutdato og -klokkeslæt.

eventVehicleRegistration er indregistreringsnummer og registrerende medlemsstat for det køretøj, hvor hændelsen er indtruffet.

2.17. **CardFaultData**

Oplysninger, gemt på et fører- eller værkstedskort, vedrørende fejl knyttet til kortindehaveren (krav 207 og 223).

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

CardFaultData er en sekvens af poster vedrørende fejl ved kontrolapparatet, efterfulgt af en mængde af poster vedrørende kortfejl.

cardFaultRecords er en mængde af fejlposter af en given fejlkategori (kontrolapparat eller kort).

2.18. **CardFaultRecord**

Oplysninger, gemt på et fører- eller værkstedskort, vedrørende en fejl knyttet til kortindehaveren (krav 208 og 223).

```
CardFaultRecord ::= SEQUENCE {
   faultType                           EventFaultType,
   faultBeginTime                      TimeReal,
   faultEndTime                        TimeReal,
   faultVehicleRegistration            VehicleRegistrationIdentification
}
```

faultType er fejlens type.

faultBeginTime er fejlens startdato og -klokkeslæt.

faultEndTime er fejlens slutdato og -klokkeslæt.

faultVehicleRegistration er indregistreringsnummer og registrerende medlemsstat for det køretøj, hvor fejlen er indtruffet.

2.19. **CardIccIdentification**

Oplysninger, gemt på et kort, vedrørende identifikation af kortet med integreret kreds (IC) (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 er klokstop-mode som defineret i EN 726-3.

cardExtendedSerialNumber er IC-kortets serienummer og IC-kortets fabrikationshenvisning som defineret i EN 726-3 og som videre angivet ved datatypen af det pågældende ExtendedSerialNumber.

cardApprovalNumber er kortets typegodkendelsesnummer.

cardPersonaliserID er kortets person-ID som defineret i EN 726-3.

embedderIcAssemblerId er datanavnet på embedder/IC assembler som defineret i EN 726-3.

icIdentifier er datanavnet for kortets IC og IC-fabrikant som defineret i EN 726-3.

2.20. **CardIdentification**

Oplysninger, gemt på et kort, vedrørende identifikation af kortet (krav 194, 215, 231, 235).

```
CardIdentification ::= SEQUENCE {
   cardIssuingMemberState                NationNumeric,
   cardNumber                            CardNumber,
   cardIssuingAuthorityName              Name,
   cardIssueDate                         TimeReal,
   cardValidityBegin                     TimeReal,
   cardExpiryDate                        TimeReal
}
```

cardIssuingMemberState er koden på den medlemsstat, som har udstedt kortet.

cardNumber er kortets nummer.

cardIssuingAuthorityName er navnet på den myndighed, der har udstedt kortet.

cardIssueDate er datoen for udstedelse af kortet til den nuværende indehaver.

cardValidityBegin er kortets første gyldighedsdato.

cardExpiryDate er kortets udløbsdato.

2.21. **CardNumber**

Et kortnummer er defineret ved definition g).

```
CardNumber ::= CHOICE {
   SEQUENCE {
      driverIdentification               IA5String(SIZE(14)),
      cardReplacementIndex               CardReplacementIndex,
      cardRenewalIndex                   CardRenewalIndex
   },
   SEQUENCE {
      ownerIdentification                IA5String(SIZE(13)),
      cardConsecutiveIndex               CardConsecutiveIndex,
      cardReplacementIndex               CardReplacementIndex,
      cardRenewalIndex                   CardRenewalIndex
   }
}
```

driverIdentification er den entydige identifikation af en fører i en medlemsstat.

ownerIdentification er den entydige identifikation af en virksomhed, et værksted eller et kontrolorgan i en medlemsstat.

cardConsecutiveIndex er kortets fortløbende indeks.

cardReplacementIndex er kortets udskiftningsindeks.

cardRenewalIndex er kortets fornyelsesindeks.

Den første sekvens af valget er egnet til kodning af et førerkortnummer, den anden sekvens af valget er egnet til kodning af værksteds- kontrol- og virksomhedskortnummer.

2.22. **CardPlaceDailyWorkPeriod**

Oplysninger, gemt på et fører- eller værkstedskort, vedrørende de steder, hvor den daglige arbejdstid begynder og/eller slutter (krav 202 og 221).

```
CardPlaceDailyWorkPeriod ::= SEQUENCE {
   placePointerNewestRecord          INTEGER(0..NoOfCardPlaceRecords-1),
   placeRecords                      SET SIZE(NoOfCardPlaceRecords) OF PlaceRecord
}
```

placePointerNewestRecord er index for den senest opdaterede stedpost.

Tilordnet værdi: Tal svarende til tælleren i stedposten, begyndende med '0' for den første forekomst af stedposterne i strukturen.

placeRecords er den mængde poster, der indeholder oplysninger vedrørende de indlæste steder.

2.23. **CardPrivateKey**

Et korts private nøgle.

```
CardPrivateKey ::= RSAKeyPrivateExponent
```

2.24. **CardPublicKey**

Et korts offentlige nøgle.

```
CardPublicKey ::= PublicKey
```

2.25. **CardRenewalIndex**

Et kortfornyelsesindeks (definition i)).

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

Tilordnet værdi: (Se kapitel VII i dette bilag).

`'19'` Første udstedelse.

Rækkefølge af forøgelse: '0, . . ., 9, A, . . ., Z'

2.26. **CardReplacementIndex**

Et korterstatningsindeks (definition j)).

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

Tilordnet værdi: (Se kapitel VII i dette bilag).

`'19'` Oprindeligt kort.

Rækkefølge af forøgelse: '0, . . ., 9, A, . . ., Z'

2.27. **CardSlotNumber**

Kode, som anvendes til at skelne mellem de to kortpladser i en køretøjsenhed.

```
CardSlotNumber ::= INTEGER {
   driverSlot                        (0),
   co-driverSlot                     (1)
}
```

Tilordnet værdi: Ikke yderligere angivet.

2.28. **CardSlotsStatus**

Kode, som angiver den type kort, der sidder i køretøjsenhedens to kortpladser.

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

Tilordnet værdi — Oktet udsluttet: `'ccccdddd'B`:

`'cccc'B` Identifikation af den type kort, der sidder i medchaufførens kortplads,

`'dddd'B` Identifikation af den type kort, der sidder i førerens kortplads,

med følgende identifikationskoder:

`'0000'B` intet kort isat,

`'0001'B` et førerkort isat,

`'0010'B` et værkstedskort isat,

`'0011'B` et kontrolkort isat,

`'0100'B` et virksomhedskort isat.

2.29. **CardStructureVersion**

Kode, som angiver versionen af den struktur, der er implementeret i et fartskriverkort.

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

Tilordnet værdi: `'aabb'H`:

`'aa'H` Indeks for ændringer af strukturen,

`'bb'H` Indeks for ændringer vedrørende brug af de dataelementer, der er defineret for strukturen, er givet ved det høje byte.

2.30. **CardVehicleRecord**

Oplysninger, gemt på et fører- eller værkstedskort, vedrørende en anvendelsesperiode for et køretøj på en kalenderdag (krav 197 og 217).

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

vehicleOdometerBegin er køretøjets kilometerstand ved begyndelsen af anvendelsesperioden for køretøjet.

vehicleOdometerEnd er køretøjets kilometerstand ved slutningen af anvendelsesperioden for køretøjet.

vehicleFirstUse er startdato og -klokkeslæt for anvendelsesperioden for køretøjet.

vehicleLastUse er slutdato og -klokkeslæt for anvendelsen af køretøjet.

vehicleRegistration er indregistreringsnummer og registrerende medlemsstat for køretøjet.

vuDataBlockCounter er værdien af VuDataBlockCounter ved sidste uddragning af køretøjets anvendelsesperiode.

2.31. **CardVehiclesUsed**

Oplysninger, gemt på et fører- eller værkstedskort, vedrørende de køretøjer, der er anvendt af kortindehaveren (krav 197 og 217).

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

vehiclePointerNewestRecord er indekset på senest opdaterede køretøjspost.

Tilordnet værdi: Tal svarende til tælleren i køretøjsposten, begyndende med '0' for den første forekomst af køretøjsposterne i strukturen.

cardVehicleRecords cardVehicleRecords er den mængde poster, der indeholder oplysninger om de anvendte køretøjer.

2.32. **Certifikat**

Certifikatet for en offentlig nøgle, udstedt af et certificeringsorgan.

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

Tilordnet værdi: Digital underskrift med delvis genfinding af et CertificateContent i henhold til tillæg 11 fælles sikkerhedsmekanismer: Signature (128 byte) || Public Key remainder (58 byte) || Certification Authority Reference (8 byte).

2.33. **CertificateContent**

Det (tydelige) indhold af certifikatet for en offentlig nøgle, som fremgår af tillæg 11, fælles sikkerhedsmekanismer.

```
CertificateContent ::= SEQUENCE {
   certificateProfileIdentifier          INTEGER(0..255),
   certificationAuthorityReference       KeyIdentifier,
   certificateHolderAuthorisation        CertificateHolderAuthorisation,
   certificateEndOfValidity              TimeReal,
   certificateHolderReference            KeyIdentifier,
   publicKey                             PublicKey
}
```

certificateProfileIdentifier er den pågældende version af det tilsvarende certifikat.

Tilordnet værdi: '01h' for denne version.

certificationAuthorityReference angiver den certificeringsmyndighed, som udsteder certifikatet. Den angiver desuden denne certificeringsmyndigheds offentlige nøgle.

certificateHolderAuthorisation identificerer certifikatindehaverens rettigheder.

certificateEndOfValidity er den dato, hvor certifikatet udløber administrativt.

certificateHolderReference identificerer certifikatindehaveren. Den henviser desuden til hans offentlige nøgle.

publicKey er den offentlige nøgle, som er certificeret ved det pågældende certifikat.

2.34. **CertificateHolderAuthorisation**

Identifikation af en certifikatindehavers rettigheder.

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

tachographApplicationID er datanavnet for fartskriverapplikationen.

Tilordnet værdi: 'FFh' '54h' '41h' '43h' '48h' '4Fh'. Denne AID er et beskyttet, ikke registreret applikationsdatanavn i henhold til ISO/IEC 7816-5.

equipmentType er identifikationen af den type udstyr, som certifikatet er bestemt til.

Tilordnet værdi: I overensstemmelse med EquipmentType datatype. 0 hvis certifikatet er fra en medlemsstat.

2.35. **CertificateRequestID**

Entydig identifikation af en anmodning om certifikat. Den kan også benyttes som datanavn for et køretøjs offentlige nøgle, hvis serienummeret på den køretøjsenhed, som nøglen er bestemt for, ikke kendes på udfærdigelsestidspunktet for certifikatet.

```
CertificateRequestID ::= SEQUENCE {
   requestSerialNumber                    INTEGER(0..2^32-1)
   requestMonthYear                       BCDString(SIZE(2))
   crIdentifier                           OCTET STRING(SIZE(1))
   manufacturerCode                       ManufacturerCode

}
```

requestSerialNumber er et serienummer på anmodningen om certifikatet. Den er entydig for fabrikanten og for måneden nedenfor.

requestMonthYear identificerer måned og år for anmodningen om certifikatet.

Tilordnet værdi: BCD-kodning af måned (to cifre) og år (to sidste cifre).

crIdentifier: Et datanavn, som har til formål at skelne en anmodning om certifikat fra et udvidet serienummer.

Tilordnet værdi: 'FFh'.

manufacturerCode: Den numeriske kode for den producent, der anmoder om certifikatet.

2.36. **CertificationAuthorityKID**

Datanavn for den offentlige nøgle tilhørende en certificeringsmyndighed (en medlemsstat eller den europæiske certificeringsmyndighed).

```
CertificationAuthorityKID ::= SEQUENCE {
   nationNumeric                          NationNumeric
   nationAlpha                            NationAlpha
   keySerialNumber                        INTEGER(0..255)
   additionalInfo                         OCTET STRING(SIZE(2))
   caIdentifier                           OCTET STRING(SIZE(1))
}
```

nationNumeric er den numeriske kode for certificeringsmyndigheden.

nationAlpha er den alfanumeriske nationskode for certificeringsmyndigheden.

keySerialNumber er et serienummer, som er bestemt til at skelne mellem certificeringsmyndighedens forskellige nøgler i tilfælde, hvor der skiftes nøgle.

additionalInfo er et felt på to byte til supplerende kodning (specifik for certificeringsmyndigheden).

caIdentifier er et datanavn, som har til formål at skelne datanavnet for en certificeringsmyndigheds nøgle fra andre nøgledatanavne.

Tilordnet værdi: '01h'.

2.37. **CompanyActivityData**

Oplysninger, gemt på et virksomhedskort, vedrørende de aktiviteter, der udføres 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 er indekset på senest opdaterede companyActivityRecord.

Tilordnet værdi: Tal svarende til tælleren i virksomhedsaktivitetsposten, begyndende med »0« for første forekomst af virksomhedsaktivitetsposten i strukturen.

companyActivityRecords er mængden af alle virksomhedsaktivitetsposter.

companyActivityRecord er sekvensen af oplysninger vedrørende én virksomhedsaktivitet.

companyActivityType er virksomhedsaktivitetens type.

companyActivityTime er klokkeslæt og dato for virksomhedsaktiviteten.

cardNumberInformation er kortnummer og kortudstedende medlemsstat for det kort, hvis data er blevet overført (i givet fald).

vehicleRegistrationInformation er indregistreringsnummer og registrerende medlemsstat for det køretøj, hvis data er blevet overført, eller som er blevet låst ind eller ud.

downloadPeriodBegin og **downloadPeriodEnd** angiver den periode, hvor eventuel overførsel af data fra køretøjsenheden har fundet sted.

2.38. **CompanyActivityType**

Kode, som angiver en aktivitet udøvet af en virksomhed, som benytter sit virksomhedskort.

```
CompanyActivityType ::= INTEGER {
   dataoverførsel af kort                (1),
   dataoverførsel for køretøjsenhed      (2),
   låse køretøjsenhed ind                (3),
   låse køretøjsenhed ud                 (4)
}
```

2.39. **CompanyCardApplicationIdentification**

Oplysninger, gemt på kortet, vedrørende identifikation af kortets applikation (krav 190).

```
CompanyCardApplicationIdentification ::= SEQUENCE {
   typeOfTachographCardId                EquipmentType,
   cardStructureVersion                  CardStructureVersion,
   noOfCompanyActivityRecords            NoOfCompanyActivityRecords
}
```

typeOfTachographCardId specificerer den implementerede korttype.

cardStructureVersion specificerer den version af strukturen, som er implementeret i kortet.

noOfCompanyActivityRecords er det antal virksomhedsaktivitetsposter, som kortet kan opbevare.

2.40. **CompanyCardHolderIdentification**

Oplysninger, gemt på et virksomhedskort, vedrørende identifikation af kortindehaveren (krav 236).

```
CompanyCardHolderIdentification ::= SEQUENCE {
   companyName                           Name,
   companyAddress                        Address,
   cardHolderPreferredLanguage           Language
}
```

companyName er navnet på den virksomhed, der er indehaver af kortet.

companyAddress er adressen på den virksomhed, der er indehaver af kortet.

cardHolderPreferredLanguage er det af kortindehaveren foretrukne sprog.

2.41. **ControlCardApplicationIdentification**

Oplysninger, gemt på et kontrolkort, vedrørende identifikation af kortets applikation (krav 190).

```
ControlCardApplicationIdentification ::= SEQUENCE {
   typeOfTachographCardId                EquipmentType,
   cardStructureVersion                  CardStructureVersion,
   noOfControlActivityRecords            NoOfControlActivityRecords
}
```

typeOfTachographCardId specificerer den implementerede korttype.

cardStructureVersion specificerer den version af strukturen, som er implementeret i kortet.

noOfControlActivityRecords er det antal kontrolaktivitetsposter, som kortet kan opbevare.

2.42. **ControlCardControlActivityData**

Oplysninger, gemt på et kontrolkort, vedrørende de aktiviteter, der er udført 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 er indekset på senest opdaterede kontrolaktivitetspost.

Tilordnet værdi: Tal svarende til tælleren i køretøjsposten, begyndende med '0' for første forekomst af kontrolaktivitetsposten i strukturen.

controlActivityRecords er det fuldstændige sæt kontrolaktivitetsposter.

controlActivityRecord er sekvensen af oplysninger vedrørende én kontrol.

controlType er kontrollens type.

controlTime er dato og klokkeslæt for kontrollen.

controlledCardNumber er kortnummer og kortudstedende medlemsstat for det kort, som kontrolleres.

controlledVehicleRegistration er indregistreringsnummer og registrerende medlemsstat for det køretøj, i hvilket kontrollen fandt sted.

controlDownloadPeriodBegin og **controlDownloadPeriodEnd** angiver den periode, for hvilken data derefter er blevet overført.

2.43. **ControlCardHolderIdentification**

Oplysninger, gemt på et kontrolkort, vedrørende identifikation af kortindehaveren (krav 232).

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

controlBodyName er navnet på kortindehaverens kontrolorgan.

controlBodyAddress er adressen på kortindehaverens kontrolorgan.

cardHolderName er efternavn og fornavn(e) på kontrolkortets indehaver.

cardHolderPreferredLanguage er det af kortindehaveren foretrukne sprog.

2.44. **ControlType**

Kode, som angiver de aktiviteter, som udføres under en kontrol. Denne datatype er knyttet til krav 102, 210 og 225.

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

Tilordnet værdi — Oktet udsluttet: `'cvpdxxxx'B` (8 bit)

`'c'B` dataoverførsel for kort:

`'0'B`: Kortets data er ikke overført under denne kontrolaktivitet,

`'1'B`: Kortets data er overført under denne kontrolaktivitet

`'v'B` dataoverførsel for køretøjsenhed:

`'0'B`: Køretøjsenhedens data er ikke blevet overført under denne kontrolaktivitet,

`'1'B`: Køretøjsenhedens data er blevet overført under denne kontrolaktivitet,

`'p'B` udprintning:

`'0'B`: Der er ikke udprintet under denne kontrolaktivitet,

`'1'B`: Der er udprintet under denne kontrolaktivitet,

`'d'B` visning på skærm:

`'0'B`: Der er ikke anvendt visning på skærm under denne kontrolaktivitet,

`'1'B`: Der er anvendt visning på skærm under denne kontrolaktivitet,

`'xxxx'B` Ikke anvendt.

2.45. **CurrentDateTime**

Kontrolapparatets aktuelle klokkeslæt og dato.

```
CurrentDateTime ::= TimeReal
```

Tilordnet værdi: Ikke yderligere angivet.

2.46. **DailyPresenceCounter**

En tæller, som er gemt på et fører- eller værkstedskort, og hvis værdi øges med én for hver kalenderdag, kortet har været indsat i en køretøjsenhed. Denne datatype er knyttet til krav 199 og 219.

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

Tilordnet værdi: Fortløbende nummer med maksimumværdi = 9 999, hvorefter der tælles forfra fra 0. Ved første udstedelse af kortet stilles tælleren på nul.

2.47. **Datef**

Dato, angivet i numerisk, let printbart format.

```
Datef ::= SEQUENCE {
   year       BCDString(SIZE(2)),
   month      BCDString(SIZE(1)),
   day        BCDString(SIZE(1))
}
```

Tilordnet værdi:

yyyy	Year
mm	Month
dd	Day
'00000000'H	datoangivelse udtrykkelig udeladt.

2.48. **Distance**

En tilbagelagt distance (resultat af beregning af forskellen mellem to værdier af køretøjets kilometerstand).

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

Tilordnet værdi: Binær uden fortegn. Værdi i km med området 0 til 9 999 km.

2.49. **DriverCardApplicationIdentification**

Oplysninger, gemt på et førerkort, vedrørende identifikation af kortets applikation (krav 190).

```
DriverCardApplicationIdentification ::= SEQUENCE {
   typeOfTachographCardId                EquipmentType,
   cardStructureVersion                  CardStructureVersion,
   noOfEventsPerType                     NoOfEventsPerType,
   noOfFaultsPerType                     NoOfFaultsPerType,
   activityStructureLength               CardActivityLengthRange,
   noOfCardVehicleRecords                NoOfCardVehicleRecords,
   noOfCardPlaceRecords                  NoOfCardPlaceRecords
}
```

typeOfTachographCardId angiver den implementerede korttype.

cardStructureVersion angiver den version af strukturen, som er implementeret i kortet.

noOfEventsPerType er antal hændelser af hver hændelsestype, som kortet kan opbevare.

noOfFaultsPerType er antal fejl af hver fejltype, som kortet kan opbevare.

activityStructureLength angiver antal byte, som er til rådighed til opbevaring af aktivitetsposter.

noOfCardVehicleRecords er antal køretøjsposter, som kortet kan opbevare.

noOfCardPlaceRecords er antal steder, som kortet kan opbevare.

2.50. **DriverCardHolderIdentification**

Oplysninger, gemt på et førerkort, vedrørende identifikation af kortindehaveren (krav 195).

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

cardHolderName er efternavn og fornavn(e) på førerkortets indehaver.

cardHolderBirthDate er fødselsdato for førerkortets indehaver.

cardHolderPreferredLanguage er det af kortindehaveren foretrukne sprog.

2.51. **EntryTypeDailyWorkPeriod**

Kode, der benyttes til at skelne mellem start og slut på det indlæste sted for den daglige arbejdstid og omstændigheden ved indlæsning.

```
EntryTypeDailyWorkPeriod ::= INTEGER
   Begin,  tilknyttet tid = tidspunkt for isætning af kort eller tidspunkt for
           indlæsning                                                    (0),
   End,    tilknyttet tid = tidspunkt for udtagning af kort eller tidspunkt for
           indlæsning                                                    (1),
   Begin,  tilknyttet tid indlæst manuelt (starttidspunkt)               (2),
   End,    tilknyttet tid indlæst manuelt (slutning på arbejdsperiode)   (3),
   Begin,  tilknyttet tid, som registreres af køretøjsenheden            (4),
   End,    tilknyttet tid, som registreres af køretøjsenheden            (5)
}
```

Tilordnet værd: I henhold til ISO/IEC8824-1.

2.52. **EquipmentType**

Kode, som benyttes til at skelne mellem forskellige typer udstyr til fartskriverapplikationen.

```
EquipmentType ::= INTEGER(0..255)
- - Reserveret                          (0),
- - Førerkort                           (1),
- - Værkstedskort                       (2),
- - Kontrolkort                         (3),
- - Virksomhedskort                     (4),
- - Fabrikationskort                    (5),
- - Køretøjsenhed                       (6),
- - Bevægelsesføler                     (7),
- - Reserveret fremtidig anvendelse     (8..255)
```

Tilordnet værdi: I henhold til ISO/IEC8824-1.

Værdien 0 er reserveret til at angive en medlemsstat eller EU i CHA-feltet i certifikaterne.

2.53. **EuropeanPublicKey**

Den europæiske offentlige nøgle.

```
EuropeanPublicKey ::= PublicKey
```

2.54. **EventFaultType**

Kode, som bestemmer en hændelse eller en fejl.

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

Tilordnet værdi:

'0x'H	Generelle hændelser,
'00'H	Ingen yderligere detaljer,
'01'H	Isætning af ugyldigt kort,
'02'H	Kortkonflikt,
'03'H	Tidsoverlapning,
'04'H	Kørsel uden behørigt kort,
'05'H	Isætning af kort under kørslen,
'06'H	Seneste kortsession ikke korrekt afsluttet,
'07'H	Overskridelse af tilladt hastighed,

'08'H	Afbrydelse i strømforsyningen,
'09'H	Fejl i bevægelsesdata,
'0A'H .. '0F'H	Reserveret fremtidig anvendelse,
'1x'H	Hændelser, som er knyttet til køretøjsenheden og består i forsøg på sikkerhedsbrud,
'10'H	Ingen yderligere detaljer,
'11'H	Ægthedsbekræftelse for bevægelsesføler ikke lykkedes,
'12'H	Ægthedsbekræftelse for fartskriverkort ikke lykkedes,
'13'H	Ubeføjet ændring af bevægelsesføler,
'14'H	Integritetsfejl på indlæste kortdata
'15'H	Integritetsfejl på lagrede brugerdata,
'16'H	Fejl ved intern dataoverførsel,
'17'H	Ubehørig åbning af hus,
'18'H	Hardware-sabotage
'19'H .. '1F'H	Reserveret fremtidig anvendelse,
'2x'H	Hændelser, som knyttet til føleren og består i forsøg på sikkerhedsbrud,
'20'H	Ingen yderligere detaljer,
'21'H	Ægthedskontrol ikke lykkedes,
'22'H	Integritetsfejl på lagrede data,
'23'H	Fejl ved intern dataoverførsel,
'24'H	Ubehørig åbning af hus,
'25'H	Hardware-sabotage
'26'H .. '2F'H	Reserveret fremtidig anvendelse,
'3x'H	Fejl ved kontrolapparat,
'30'H	Ingen yderligere detaljer,
'31'H	Intern fejl i køretøjsenhed,
'32'H	Printerfejl,
'33'H	Displayfejl,
'34'H	Dataoverførselsfejl,
'35'H	Følerfejl,
'36'H .. '3F'H	Reserveret fremtidig anvendelse,
'4x'H	Kortfejl,
'40'H	Ingen yderligere detaljer,
'41'H .. '4F'H	Reserveret fremtidig anvendelse,
'50'H .. '7F'H	Reserveret fremtidig anvendelse,
'80'H .. 'FF'H	Fabrikantspecifik.

2.55. **EventFaultRecordPurpose**

Kode, som forklarer, hvorfor en hændelse eller en fejl er blevet registreret.

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

Tilordnet værdi:

'00'H	en af de 10 seneste hændelser eller fejl
'01'H	den længstvarende hændelse for en af de 10 seneste dage, den er forekommet,
'02'H	en af de 5 længstvarende hændelser inden for de sidste 365 dage
'03'H	den seneste hændelse for en af de 10 seneste dage, den er forekommet
'04'H	den alvorligste hændelse for en af de 10 seneste dage, den er forekommet
'05'H	en af de 5 alvorligste hændelser inden for de sidste 365 dage
'06'H	den første hændelse eller fejl, som er forekommet efter sidste kalibrering
'07'H	en aktiv/igangværende hændelse eller fejl
'08'H . til '7F'H	Reserveret fremtidig anvendelse
'80'H .. 'FF'H	fabrikantspecifik

2.56. **ExtendedSerialNumber**

Entydig identifikation af et stykke udstyr. Kan desuden bruge som datanavn for en offentlig nøgle for udstyr.

```
ExtendedSerialNumber ::= SEQUENCE {
   serialNumber                    INTEGER(0..2^32-1)
   monthYear                       BCDString(SIZE(2))
   type                            OCTET STRING(SIZE(1))
   manufacturerCode                ManufacturerCode
}
```

serialNumber er et serienummer på udstyret. Det er entydigt for udstyret, entydigt for fabrikanten, udstyrets type og måneden nedenfor.

monthYear er identifikationen af fabrikationsmåned og -år (eller af tildelingen af serienummer).

Tilordnet værdi: Binær kodet decimaltal for måned (to cifre) og år (to sidste cifre).

type er et datanavn for udstyrets type.

Tilordnet værdi: Fabrikantspecifik, med 'FFh' reserveret værdi.

manufacturerCode: Den numeriske kode for producenten af udstyret.

2.57. **FullCardNumber**

Kode, som fuldstændig identificerer et fartskriverkort.

```
FullCardNumber ::= SEQUENCE {
   cardType                        EquipmentType,
   cardIssuingMemberState          NationNumeric,
   cardNumber                      CardNumber
}
```

cardType er fartskriverkortets type.

cardIssuingMemberState er koden på den medlemsstat, der har udstedt kortet.

cardNumber er kortnummeret.

2.58. **HighResOdometer**

Køretøjets kilometerstand: Samlet distance tilbagelagt af køretøjet i dettes driftstid.

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

Tilordnet værdi: Binær uden fortegn. Talværdi i 1/200 km med området 0 to 21 055 406 km.

2.59. **HighResTripDistance**

En distance, som er tilbagelagt i løbet af en hel tur eller en del heraf.

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

Tilordnet værdi: Binær uden fortegn. Talværdi i 1/200 km med området 0 to 21 055 406 km.

2.60. **HolderName**

En kortindehavers efternavn og fornavn(e).

```
HolderName ::= SEQUENCE {
   holderSurname                   Name,
   holderFirstNames                Name
}
```

holderSurname er indehaverens efternavn. Titler indgår ikke i efternavnet.

Tilordnet værdi: Når et kort ikke er personligt, indeholder holderSurname samme oplysninger som et companyName eller workshopName eller controlBodyName.

holderFirstNames er indehaverens fornavn(e) og forbogstaver.

2.61. **K-ConstantOfRecordingEquipment**

Kontrolapparatets konstant (definition m)).

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

Tilordnet værdi: Impulser pr. kilometer med området 0 til 64 255 impulser/km.

2.62. **KeyIdentifier**

Et entydigt datanavn for en offentlig nøgle. Benyttes til at henvise til og vælge nøgle. Den identificerer desuden indehaveren af nøglen.

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

Det første valg er egnet til henvisning til den offentlige nøgle for et køretøj eller for et fartskriverkort.

Det andet valg er egnet til henvisning til den offentlige nøgle for en køretøjsenhed (når køretøjets serienummer ikke kan oplyses på tidspunktet for udfærdigelse af certifikatet).

Det tredje valg er egnet til henvisning til den offentlige nøgle for en medlemsstat.

2.63. **L-TyreCircumference**

Effektiv dækperiferi (definition u)).

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

Tilordnet værdi: Binær uden fortegn, værdi i 1/8 mm med området 0 til 8 031 mm.

2.64. **Language**

Kode, som identificerer et sprog.

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

Tilordnet værdi: En kode bestående af to minuskler i overensstemmelse med ISO 639.

2.65. **LastCardDownload**

Dato og klokkeslæt, gemt på førerkortet, for seneste dataoverførsel af kort (til andre formål end kontrol). Denne dato kan ajourføres af en køretøjsenhed eller enhver kortlæser.

```
Last card download ::= TimeReal
```

Tilordnet værdi: Ikke yderligere specificeret.

2.66. **ManualInputFlag**

Kode, som fastslår, om en kortindehaver manuelt har eller ikke har indlæst føreraktiviteter ved isætning af kort (krav 081).

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

Tilordnet værdi: Ikke yderligere angivet.

2.67. **ManufacturerCode**

Kode, som identificerer en fabrikant.

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

Tilordnet værdi:

'00'H	Ingen oplysninger foreligger
'01'H	Reserveret værdi
'02'H .. '0F'H	Reserveret til fremtidig brug
'10'H	ACTIA
'11'H .. '17'H	Reserveret fabrikanter, hvis navn begynder med 'A'
'18'H .. '1F'H	Reserveret fabrikanter, hvis navn begynder med 'B'
'20'H .. '27'H	Reserveret fabrikanter, hvis navn begynder med 'C'
'28'H .. '2F'H	Reserveret fabrikanter, hvis navn begynder med 'D'
'30'H .. '37'H	Reserveret fabrikanter, hvis navn begynder med 'E'
'38'H .. '3F'H	Reserveret fabrikanter, hvis navn begynder med 'F'
'40'H	Giesecke & Devrient GmbH
'41'H	GEM plus
'42'H .. '47'H	Reserveret fabrikanter, hvis navn begynder med 'G'
'48'H .. '4F'H	Reserveret fabrikanter, hvis navn begynder med 'H'
'50'H .. '57'H	Reserveret fabrikanter, hvis navn begynder med 'I'
'58'H .. '5F'H	Reserveret fabrikanter, hvis navn begynder med 'J'
'60'H .. '67'H	Reserveret fabrikanter, hvis navn begynder med 'K'
'68'H .. '6F'H	Reserveret fabrikanter, hvis navn begynder med 'L'
'70'H .. '77'H	Reserveret fabrikanter, hvis navn begynder med 'M'
'78'H .. '7F'H	Reserveret fabrikanter, hvis navn begynder med 'N'
'80'H	OSCARD
'81'H .. '87'H	Reserveret fabrikanter, hvis navn begynder med 'O'
'88'H .. '8F'H	Reserveret fabrikanter, hvis navn begynder med 'P'
'90'H .. '97'H	Reserveret fabrikanter, hvis navn begynder med 'Q'
'98'H .. '9F'H	Reserveret fabrikanter, hvis navn begynder med 'R'
'A0'H	SETEC
'A1'H	Siemens VDO
'A2'H	Stoneridge
'A3'H .. 'A7'H	Reserveret fabrikanter, hvis navn begynder med 'S'
'AA'H	TACHOCONTROL
'AB'H .. 'AF'H	Reserveret fabrikanter, hvis navn begynder med 'T'
'B0'H .. 'B7'H	Reserveret fabrikanter, hvis navn begynder med 'U'
'B8'H .. 'BF'H	Reserveret fabrikanter, hvis navn begynder med 'V'
'C0'H .. 'C7'H	Reserveret fabrikanter, hvis navn begynder med 'W'
'C8'H .. 'CF'H	Reserveret fabrikanter, hvis navn begynder med 'X'
'D0'H .. 'D7'H	Reserveret fabrikanter, hvis navn begynder med 'Y'
'D8'H .. 'DF'H	Reserveret fabrikanter, hvis navn begynder med 'Z'

2.68. **MemberStateCertificate**

Certifikat for en medlemsstats offentlige nøgle, udstedt af den europæiske certificeringsmyndighed.

```
MemberStateCertificate ::= Certificate
```

2.69. **MemberStatePublicKey**

En medlemsstats offentlige nøgle.

```
MemberStatePublicKey ::= PublicKey
```

2.70. **Name**

Et navn.

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

codePage angiver den del af ISO/IEC 8859, som er anvendt til at kode navnet,

name er et navn, som er kodet i henhold til ISO/IEC 8859-codePage.

2.71. **NationAlpha**

Alfabetisk henvisning til en stat i overensstemmelse med sædvanlige kendingsbogstaver på biler og/eller som anvendt på internationalt harmoniserede forsikringsbeviser (grønne kort).

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

Tilordnet værdi:

' '	Ingen oplysninger foreligger,
'A '	Østrig,
'AL '	Albanien,
'AND'	Andorra,
'ARM'	Armenien,
'AZ '	Aserbajdsjan,
'B '	Belgien,
'BG '	Bulgarien,
'BIH'	Bosnien-Hercegovina,
'BY '	Belarus,
'CH '	Schweiz,
'CY '	Cypern,
'CZ '	Tjekkiet,
'D '	Tyskland,
'DK '	Danmark,
'E '	Spanien,
'EST'	Estland,
'F '	Frankrig,
'FIN'	Finland,
'FL '	Liechtenstein
'FR '	Færøerne,
'UK '	Det Forenede Kongerige, Alderney, Guernsey, Jersey, Isle of Man, Gibraltar,
'GE '	Georgien,
'GR '	Grækenland,
'H '	Ungarn,
'HR '	Kroatien,
'I '	Italien,
'IRL'	Irland,
'IS '	Island,
'KZ '	Kasakhstan,
'L '	Luxembourg,
'LT '	Litauen,
'LV '	Letland,
'M '	Malta,
'MC '	Monaco,

'MD '	Moldova,
'MK '	Makedonien,
'N '	Norge,
'NL '	Nederlandene,
'P '	Portugal,
'PL '	Polen,
'RO '	Rumænien,
'RSM'	San Marino,
'RUS'	Den Russiske Føderation,
'S '	Sverige,
'SK '	Slovakiet,
'SLO'	Slovenien,
'TM '	Turkmenistan,
'TR '	Tyrkiet,
'UA '	Ukraine,
'V '	Vatikanstaten,
'YU '	Jugoslavien,
'UNK'	Ukendt,
'EC '	Det Europæiske Fællesskab,
'EUR'	Det øvrige Europa,
'WLD'	Den øvrige verden.

2.72. **NationNumeric**

Numerisk henvisning til en stat.

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

Tilordnet værdi:

--	Ingen oplysninger foreligger	(00)H,
--	Østrig	(01)H,
--	Albanien	(02)H,
--	Andorra	(03)H,
--	Armenien	(04)H,
--	Aserbajdsjan	(05)H,
--	Belgien	(06)H,
--	Bulgarien	(07)H,
--	Bosnien-Hercegovina	(08)H,
--	Belarus	(09)H,
--	Schweiz	(0A)H,
--	Cypern	(0B)H,
--	Tjekkiet	(0C)H,
--	Tyskland	(0D)H,
--	Danmark	(0E)H,
--	Spanien	(0F)H,
--	Estland	(10)H,
--	Frankrig	(11)H,
--	Finland	(12)H,
--	Liechtenstein	(13)H,
--	Færøerne	(14)H,
--	Det Forenede Kongerige	(15)H,
--	Georgien	(16)H,
--	Grækenland	(17)H,
--	Ungarn	(18)H,
--	Kroatien	(19)H,
--	Italien	(1A)H,
--	Irland	(1B)H,
--	Island	(1C)H,
--	Kasakhstan	(1D)H,
--	Luxembourg	(1E)H,
--	Litauen	(1F)H,
--	Letland	(20)H,

-- Malta (21)H,
-- Monaco (22)H,
-- Moldova (23)H,
-- Makedonien (24)H,
-- Norge (25)H,
-- Nederlandene (26)H,
-- Portugal (27)H,
-- Polen (28)H,
-- Rumænien (29)H,
-- San Marino (2A)H,
-- Den Russiske Føderation (2B)H,
-- Sverige (2C)H,
-- Slovakiet (2D)H,
-- Slovenien (2E)H,
-- Turkmenistan (2F)H,
-- Tyrkiet (30)H,
-- Ukraine (31)H,
-- Vatikanstaten (32)H,
-- Jugoslavien (33)H,
-- Reserveret fremtidig anvendelse (34 .. FC)H,
-- Det Europæiske Fællesskab (FD)H,
-- Det øvrige Europa (FE)H,
-- Den øvrige verden (FF)H

2.73. **NoOfCalibrationRecords**

Antal kalibreringsposter, som kan gemmes på et værkstedskort.

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

Tilordnet værdi: Se punkt 3.

2.74. **NoOfCalibrationsSinceDownload**

Tæller, som angiver det samlede antal kalibreringer, der er udført med et værkstedskort siden sidste dataoverførsel for kortet (krav 230).

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

Tilordnet værdi: Ikke yderligere angivet.

2.75. **NoOfCardPlaceRecords**

Antal stedposter, som kan gemmes på et fører- eller værkstedskort.

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

Tilordnet værdi: Se punkt 3.

2.76. **NoOfCardVehicleRecords**

Antal anvendte køretøjer, som kan gemmes på et fører- eller værkstedskort.

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

Tilordnet værdi: Se punkt 3.

2.77. **NoOfCompanyActivityRecords**

Antal virksomhedsaktivitetsposter, som kan gemmes på et virksomhedskort.

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

Tilordnet værdi: Se punkt 3.

2.78. **NoOfControlActivityRecords**

Antal kontrolaktivitetsposter, som kan gemmes på et kontrolkort.

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

Tilordnet værdi: Se punkt 3.

2.79. **NoOfEventsPerType**

Antal hændelser af hver hændelsestype, som kan gemmes på et kort.

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

Tilordnet værdi: Se punkt 3.

2.80. **NoOfFaultsPerType**

Antal fejl af hver fejltype, som kan gemmes på et kort.

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

Tilordnet værdi: Se punkt 3.

2.81. **OdometerValueMidnight**

Køretøjets kilometerstand ved midnat i et givet døgn (krav 090).

```
OdometerValueMidnight ::= OdometerShort
```

Tilordnet værdi: Ikke yderligere angivet.

2.82. **OdometerShort**

Køretøjets kilometerstand i kortform.

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

Tilordnet værdi: Binær uden fortegn. Værdi i km i området 0 til 9 999 999 km.

2.83. **OverspeedNumber**

Antal hændelser med overskridelse af tilladt hastighed siden seneste kontrol for overskridelse af tilladt hastighed.

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

Tilordnet værdi: 0 betyder, at der ikke er forekommet hændelser med overskridelse af tilladt hastighed siden seneste kontrol for overskridelse af tilladt hastighed, 1 betyder, at der har været én hændelse med overskridelse af tilladt hastighed siden seneste kontrol for overskridelse af tilladt hastighed, ... 255 betyder, at der har varet 255 eller flere hændelser med overskridelse af tilladt hastighed siden seneste kontrol for overskridelse af tilladt hastighed.

2.84. **PlaceRecord**

Oplysninger vedrørende et sted, hvor en daglig arbejdsperiode begynder eller slutter (krav 087, 202, 221).

```
PlaceRecord ::= SEQUENCE {
   entryTime                        TimeReal,
   entryTypeDailyWorkPeriod         EntryTypeDailyWorkPeriod,
   dailyWorkPeriodCountry           NationNumeric,
   dailyWorkPeriodRegion            RegionNumeric,
   vehicleOdometerValue             OdometerShort
}
```

entryTime er en dato og et klokkeslæt knyttet til indlæsningen.

entryTypeDailyWorkPeriod er indlæsningens type.

dailyWorkPeriodCountry er den indlæste stat.

dailyWorkPeriodRegion er den indlæste region.

vehicleOdometerValue er kilometerstanden på tidspunktet for indlæsning af stedet.

2.85. **PreviousVehicleInfo**

Oplysninger vedrørende det foregående køretøj, som føreren anvendte, da han satte sit kort i en køretøjsenhed (krav 081).

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

vehicleRegistrationIdentification er indregistreringsnummer og registrerende medlemsstat for køretøjet.

cardWithdrawalTime er dato og klokkeslæt for udtagning af kortet.

2.86. **PublicKey**

En offentlig RSA-nøgle.

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

rsaKeyModulus er nøgleparrets modulus.

rsaKeyPublicExponent er nøgleparrets offentlige eksponent.

2.87. **RegionAlpha**

Alfabetisk henvisning til en region i en given stat.

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

Tilordnet værdi:

`'  '`	Ingen oplysninger foreligger,

Spanien:

`'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 henvisning til en region i en given stat.

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

Tilordnet værdi:

'00'H	Ingen oplysninger foreligger,
Spanien:	
'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 for et RSA-nøglepar.

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

Tilordnet værdi: Uspecificeret.

2.90. **RSAKeyPrivateExponent**

Den private eksponent for et RSA-nøglepar.

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

Tilordnet værdi: Uspecificeret.

2.91. **RSAKeyPublicExponent**

Den offentlige eksponent for et RSA-nøglepar.

```
RSAKeyPublicExponent ::= OCTET STRING (SIZE(20))
```

Tilordnet værdi: Uspecificeret.

2.92. **SensorApprovalNumber**

Følerens typegodkendelsesnummer.

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

Tilordnet værdi:: Uspecificeret.

2.93. **SensorIdentification**

Oplysninger, gemt på en bevægelsesføler, vedrørende identifikation af bevægelsesføleren (krav 077).

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

sensorSerialNumber er det udvidede serienummer på bevægelsesføleren (hvori reservedelsnummer og fabrikantkode indgår).

sensorApprovalNumber er godkendelsesnummeret på bevægelsesføleren.

sensorSCIdentifier er datanavnet på bevægelsesfølerens sikkerhedskomponent.

sensorOSIdentifier er datanavnet på bevægelsesfølerens styresystem.

2.94. **SensorInstallation**

Oplysninger, gemt på en bevægelsesføler, vedrørende bevægelsesfølerens montering (krav 099).

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

sensorPairingDateFirst er datoen for første samparring af bevægelsesføleren med en køretøjsenhed.

firstVuApprovalNumber er godkendelsesnummeret på den første køretøjsenhed, som er samparret med bevægelsesføleren.

firstVuSerialNumber er serienummeret på den første køretøjsenhed, som er samparret med bevægelsesføleren.

sensorPairingDateCurrent er datoen for den aktuelle samparring af bevægelsesføleren med en køretøjsenhed.

currentVuApprovalNumber er godkendelsesnummeret på den køretøjsenhed, som aktuelt er samparret med bevægelsesføleren.

currentVUSerialNumber er serienummeret på den køretøjsenhed, som aktuelt er samparret med bevægelsesføleren.

2.95. **SensorInstallationSecData**

Oplysninger, gemt på et værkstedskort, vedrørende sikkerhedsdata, som er nødvendige til samparring af bevægelsesfølere med køretøjsenheder (krav 214).

```
SensorInstallationSecData ::= TDesSessionKey
```

Tilordnet værdi: I henhold til ISO 16844-3.

2.96. **SensorOSIdentifier**

Datanavn på bevægelsesfølerens styresystem.

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

Tilordnet værdi: Fabrikantspecifik.

2.97. **SensorPaired**

Oplysninger, gemt på en køretøjsenhed, vedrørende identifikation af den bevægelsesføler, som er samparret med køretøjsenheden (krav 079).

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

sensorSerialNumber er serienummeret på den bevægelsesføler, som aktuelt er samparret med køretøjsenheden.

sensorApprovalNumber er godkendelsesnummeret på den bevægelsesføler, som aktuelt er samparret med køretøjsenheden.

sensorPairingDateFirst er datoen for første samparring mellem en køretøjsenhed og den bevægelsesføler, som aktuelt er samparret med køretøjsenheden.

2.98. **SensorPairingDate**

Datoen for samparring af bevægelsesføleren med en køretøjsenhed.

```
SensorPairingDate ::= TimeReal
```

Tilordnet værdi: Uspecificeret.

2.99. **SensorSerialNumber**

Serienummeret på bevægelsesføleren.

```
SensorSerialNumber ::= ExtendedSerialNumber
```

2.100. **SensorSCIdentifier**

Datanavnet på bevægelsesfølerens sikkerhedskomponent.

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

Tilordnet værdi: Specifik for komponentfabrikanten.

2.101. **Signature**

En digital underskrift.

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

Tilordnet værdi: I overensstemmelse med Tillæg 11 (fælles sikkerhedsmekanismer).

2.102. **SimilarEventsNumber**

Antal tilsvarende hændelser for ét givet døgn (krav 094).

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

Tilordnet værdi: 0 anvendes ikke, 1 betyder, at der det pågældende døgn kun er indtruffet og registreret én hændelse af den pågældende type, 2 betyder, at der er registreret to hændelser af den pågældende type (kun én er registreret), . . . 255 betyder, at der er registreret 255 eller flere hændelser af den pågældende type den pågældende dag.

2.103. **SpecificConditionType**

Kode, som identificerer en særlig omstændighed (krav 050b, 105a, 212a og 230a).

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

Tilordnet værdi:

'00'H	Reserveret fremtidig anvendelse
'01'H	Out of scope — Begin
'02'H	Out of scope — End
'03'H	Overfart med færge/tog
'04'H .. 'FF'H	Reserveret fremtidig anvendelse

2.104. **SpecificConditionRecord**

Oplysninger, som er gemt på et førerkort, et værkstedskort eller en køretøjsenhed og vedrører en særlig omstændighed (krav 105a, 212a og 230a).

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

entryTime er dato og klokkeslæt for indlæsningen.

specificConditionType er den kode, som identificerer den særlige omstændighed.

2.105. **Speed**

Køretøjets hastighed (km/h).

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

Tilordnet værdi: Kilometer i timen, med området 0 til 220 km/h.

2.106. **SpeedAuthorised**

Tilladelig maksimal hastighed for køretøjet (definition bb)).

```
SpeedAuthorised ::= Speed
```

2.107. **SpeedAverage**

Gennemsnitshastighed i en forud fastlagt periode (km/h).

```
SpeedAverage ::= Speed
```

2.108. **SpeedMax**

Maksimumhastighed målt i et forud fastlagt tidsrum.

```
SpeedMax ::= Speed
```

2.109. **TDesSessionKey**

En tredobbelt DES-sessionsnøgle.

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

Tilordnet værdi: Ikke yderligere angivet.

2.110. **TimeReal**

Kode for et kombineret dato- og klokkeslætfelt, hvor dato og klokkeslæt er angivet som sekunder siden 00h.00m.00s. den 1. januar 1970 GMT.

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

Tilordnet værdi — Oktet udsluttet: Antal sekunder siden midnat den 1. januar 1970 GMT.

Den maksimale værdi af dato/klokkeslæt er året 2106.

2.111. **TyreSize**

Dækdimensionsbetegnelser.

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

Tilordnet værdi: I henhold til direktiv 92/23/EØF af 31.3.1992, EFT L 129, s. 95.

2.112. **VehicleIdentificationNumber**

Køretøjets identifikationsnummer med henvisning til køretøjet som helhed, normalt chassisnummeret.

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

Tilordnet værdi: Som defineret i ISO 3779.

2.113. **VehicleRegistrationIdentification**

Identifikation af et køretøj, entydig for Europa (indregistreringsnummer og medlemsstat).

```
VehicleRegistrationIdentification ::= SEQUENCE {
   vehicleRegistrationNation              NationNumeric,
   vehicleRegistrationNumber              VehicleRegistrationNumber
}
```

vehicleRegistrationNation er den stat, hvor køretøjet er indregistreret.

vehicleRegistrationNumber er køretøjets indregistreringsnummer.

2.114. **VehicleRegistrationNumber**

Køretøjets indregistreringsnummer. Indregistreringsnummeret tildeles af registreringsmyndigheden.

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

codePage angiver den del af ISO/IEC 8859, som anvendes til at kode vehicleRegnNumber,

vehicleRegNumber er et køretøjsregistreringsnummer, som er kodet i henhold til ISO/IEC 8859-codePage.

Tilordnet værdi: Statsspecifik.

2.115. **VuActivityDailyData**

Oplysninger, gemt på en køretøjsenhed, vedrørende skift af aktivitet og/eller skift af kørestatus og/eller skift af kortstatus for en given kalenderdag (krav 084), samt kortlæserstatus kl. 00:00 den pågældende dag.

```
VuActivityDailyData ::= SEQUENCE {
   noOfActivityChanges                    INTEGER SIZE(0..1440),
   activityChangeInfos                    SET SIZE(noOfActivityChanges) OF
                                          ActivityChangeInfo
}
```

noOfActivityChanges er antal ord vedrørende ActivityChangeInfo i mængden activityChangeInfos.

activityChangeInfos er den mængde af ord vedrørende ActivityChangeInfo, som for det pågældende døgn er gemt i køretøjsenheden. Den omfatter altid to ActivityChangeInfo ord, som angiver status af de to kortlæsere kl. 00:00 den pågældende dag.

2.116. **VuApprovalNumber**

Køretøjsenhedens typegodkendelsesnummer.

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

Tilordnet værdi: Uspecificeret.

2.117. **VuCalibrationData**

Oplysninger, gemt på en køretøjsenhed, vedrørende kalibreringerne af kontrolapparatet (krav 098).

```
VuCalibrationData ::= SEQUENCE {
   noOfVuCalibrationRecords               INTEGER(0..255),
   vuCalibrationRecords                   SET SIZE(noOfVuCalibrationRecords) OF
                                          VuCalibrationRecord
}
```

noOfVuCalibrationRecords er antal poster indeholdt i mængden vuCalibrationRecords.

vuCalibrationRecords er mængden af kalibreringsposter.

2.118. **VuCalibrationRecord**

Oplysninger, gemt på en køretøjsenhed, vedrørende en kalibrering af kontrolapparatet (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 er formålet med kalibreringen.

workshopName, workshopAddress er værkstedets navn og adresse.

workshopCardNumber identificerer det værkstedskort, der er anvendt ved kalibreringen.

workshopCardExpiryDate er kortets udløbsdato.

vehicleIdentificationNumber er køretøjets identifikationsnummer.

vehicleRegistrationIdentification indeholder køretøjets indregistreringsnummer og den indregistrerende medlemsstat.

wVehicleCharacteristicConstant er køretøjets vejdrejetal.

kConstantOfRecordingEquipment er kontrolapparatets konstant.

lTyreCircumference er den effektive dækperiferi.

tyreSize er dækdimensionsbetegnelsen for de dæk, der er monteret på køretøjet

authorisedSpeed er køretøjets tilladte hastighed.

oldOdometerValue, newOdometerValue er gammel og ny kilometerstand.

oldTimeValue, newTimeValue er gammel og ny værdi af dato og klokkeslæt.

nextCalibrationDate er datoen for næste kalibrering af den type, som i CalibrationPurpose foreskrives at skulle udføres af kontrolmyndigheden.

2.119. **VuCardIWData**

Oplysninger, gemt på en køretøjsenhed, vedrørende cyklusser med isætning/udtagning af førerkort eller værkstedskort i køretøjsenheden (krav 081).

```
VuCardIWData ::= SEQUENCE {
   noOfIWRecords                         INTEGER(0..2^16-1),
   vuCardIWRecords                       SET SIZE(noOfIWRecords) OF
                                         VuCardIWRecord
}
```

noOfIWRecords er antal poster i mængden af vuCalibrationRecords.

vuCardIWRecords er en mængde af poster, som vedrører cyklusser med isætning/udtagning af kort.

2.120. **VuCardIWRecord**

Oplysninger, gemt på en køretøjsenhed, vedrørende cyklusser med isætning/udtagning af førerkort eller værkstedskort i køretøjsenheden (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 er kortindehaverens efternavn og fornavn(e), som gemt på kortet.

fullCardNumber er kortets type, den medlemsstat, som har udstedt kortet, samt kortets nummer, som gemt på kortet.

cardExpiryDate er kortets udløbsdato, som gemt på kortet.

cardInsertionTime er isætningsdato og -klokkeslæt.

vehicleOdometerValueAtInsertion er køretøjets kilometerstand ved isætning af kortet.

cardSlotNumber er den kortplads, som kortet sidder i.

cardWithdrawalTime er dato og klokkeslæt for udtagning af kortet.

vehicleOdometerValueAtWithdrawal er køretøjets kilometerstand ved udtagning af kortet.

previousVehicleInfo indeholder oplysninger om det foregående køretøj, føreren har anvendt, som gemt på kortet.

manualInputFlag er et flag, som angiver, om kortindehaveren manuelt har eller ikke har indlæst føreraktiviteter ved isætning af kortet.

2.121. **VuCertificate**

Certifikat for en køretøjsenheds offentlige nøgle.

```
VuCertificate ::= Certificate
```

2.122. **VuCompanyLocksData**

Oplysninger, som er gemt på en køretøjsenhed og vedrører virksomhedslåse (krav 104).

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

noOfLocks er antal låse, som er opført i vuCompanyLocksRecords.

vuCompanyLocksRecords er mængden af poster vedrørende virksomhedslåse.

2.123. **VuCompanyLocksRecord**

Oplysninger, gemt på en køretøjsenhed, vedrørende én virksomhedslås (krav 104).

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

lockInTime, lockOutTime er dato og klokkeslæt for lås-ind og lås-ud.

companyName, companyAddress er navn og adresse på den virksomhed, der er knyttet til den pågældende lås-ind.

companyCardNumber identificerer det kort, der er anvendt ved lås-ind.

2.124. **VuControlActivityData**

Oplysninger, gemt på en køretøjsenhed, vedrørende kontroller foretaget ved hjælp af denne køretøjsenhed (krav 102).

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

noOfControls er antal kontroller, som er opført i vuControlActivityRecords.

vuControlActivityRecords er mængden af kontrolaktivitetsposter.

2.125. **VuControlActivityRecord**

Oplysninger, gemt på en køretøjsenhed, vedrørende kontroller foretaget ved hjælp af denne køretøjsenhed (krav 102).

```
VuControlActivityRecord ::= SEQUENCE {
   controlType                         ControlType,
   controlTime                         TimeReal,
   controlCardNumber                   FullCardNumber,
   downloadPeriodBeginTime             TimeReal,
   downloadPeriodEndTime               TimeReal
}
```

controlType er kontrollens type.

controlTime er dato og klokkeslæt for kontrollen.

ControlCardNumber identificerer det kontrolkort, som er anvendt til kontrollen.

downloadPeriodBeginTime er begyndelsestidspunktet for dataoverførsel, når en sådan har fundet sted.

downloadPeriodEndTime er sluttidspunktet for dataoverførsel, når en sådan har fundet sted.

2.126. **VuDataBlockCounter**

Tæller, som er gemt på et kort, og som sekventielt identificerer cyklusserne med isætning/udtagning af kortet i køretøjsenheder.

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

Tilordnet værdi: Fortløbende nummer, som, efter at have nået maksimumværdien 9 999, begynder forfra fra 0.

2.127. **VuDetailedSpeedBlock**

Oplysninger, som er gemt på en køretøjsenhed og detaljeret angiver køretøjets hastighed i et minut, i hvilket køretøjet har bevæget sig (krav 093).

```
VuDetailedSpeedBlock ::= SEQUENCE {
   speedBlockBeginDate                    TimeReal,
   speedsPerSecond                        SEQUENCE SIZE(60) OF Speed
}
```

speedBlockBeginDate er dato og klokkeslæt for den første hastighedsværdi inden for blokken.

speedsPerSecond er den kronologiske sekvens af målte hastigheder hvert sekund for det minut, der begynder på speedBlockBeginDate (inklusive).

2.128. **VuDetailedSpeedData**

Oplysninger, gemt på en køretøjsenhed, vedrørende køretøjets detaljerede hastighed.

```
VuDetailedSpeedData ::= SEQUENCE {
   noOfSpeedBlocks                        INTEGER(0.2^16-1),
   vuDetailedSpeedBlocks                  SET SIZE(noOfSpeedBlocks) OF
                                          VuDetailedSpeedBlock
}
```

noOfSpeedBlocks er antal hastighedsblokke i mængden vuDetailedSpeedBlocks.

vuDetailedSpeedBlocks er mængden af detaljerede hastighedsblokke.

2.129. **VuDownloadablePeriod**

Ældste og nyeste dato, for hvilke en køretøjsenhed opbevarer data vedrørende førerens aktiviteter (krav 081, 084 eller 087).

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

minDownloadableTime er ældste dato og klokkeslæt, som i køretøjsenheden er gemt vedrørende isætning af kort, aktivitetsskift eller indlæsning af sted.

maxDownloadableTime er nyeste dato og klokkeslæt, som i køretøjsenheden er gemt vedrørende udtagning af kort, aktivitetsskift eller indlæsning af sted.

2.130. **VuDownloadActivityData**

Oplysninger, gemt på en køretøjsenhed, vedrørende dens seneste dataoverførsel (krav 105).

```
VuDownloadActivityData ::= SEQUENCE {
   downloadingTime                        TimeReal,
   fullCardNumber                         FullCardNumber,
   companyOrWorkshopName                  Name
}
```

downloadingTime er dato og klokkeslæt for dataoverførslen.

fullCardNumber identificerer det kort, der er anvendt til at muliggøre dataoverførslen.

companyOrWorkshopName er virksomhedens eller værkstedets navn.

2.131. **VuEventData**

Oplysninger, gemt på en køretøjsenhed, vedrørende hændelser (krav 094 bortset fra overskridelser af tilladt hastighed).

```
VuEventData ::= SEQUENCE {
   noOfVuEvents                           INTEGER(0..255),
   vuEventRecords                         SET SIZE(noOfVuEvents) OF VuEventRecord
}
```

noOfVuEvents er antal hændelser på listen over hændelser i mængden vuEventRecords.

vuEventRecords er en mængde af hændelsesposter.

2.132. **VuEventRecord**

Oplysninger, gemt på en køretøjsenhed, vedrørende en hændelse (krav 094 bortset fra overskridelse af tilladt hastighed).

```
VuEventRecord ::= SEQUENCE {
   eventType                          EventFaultType,
   eventRecordPurpose                 EventFaultRecordPurpose,
   eventBeginTime                     TimeReal,
   eventEndTime                       TimeReal,
   cardNumberDriverSlotBegin          FullCardNumber,
   cardNumberCodriverSlotBegin        FullCardNumber,
   cardNumberDriverSlotEnd            FullCardNumber,
   cardNumberCodriverSlotEnd          FullCardNumber,
   similarEventsNumber                SimilarEventsNumber
}
```

eventType er hændelsens type.

eventRecordPurpose er det formål, hændelsen er blevet registreret til.

eventBeginTime er hændelsens startdato og -klokkeslæt.

eventEndTime er hændelsens slutdato og -klokkeslæt.

cardNumberDriverSlotBegin identificerer det kort, der sad i førerens kortplads ved hændelsens start.

cardNumberCodriverSlotBegin identificerer det kort, der sad i medchaufførens kortplads ved hændelsens start.

cardNumberDriverSlotEnd identificerer det kort, der sad i førerens kortplads ved hændelsens slutning.

cardNumberCodriverSlotEnd identificerer det kort, der sad i medchaufførens kortplads ved hændelsens slutning.

similarEventsNumber er antal tilsvarende hændelser samme dag.

Denne sekvens kan anvendes til alle hændelser bortset fra overskridelser af tilladt hastighed.

2.133. **VuFaultData**

Oplysninger, gemt på en køretøjsenhed, vedrørende fejl (krav 096).

```
VuFaultData ::= SEQUENCE {
   noOfVuFaults                       INTEGER(0..255),
   vuFaultRecords                     SET SIZE(noOfVuFaults) OF VuFaultRecord
}
```

noOfVuFaults er antal fejl opført i mængden vuFaultRecords.

vuFaultRecords er en mængde af fejlposter.

2.134. **VuFaultRecord**

Oplysninger, gemt på en køretøjsenhed, vedrørende en fejl (krav 096).

```
VuFaultRecord ::= SEQUENCE {
   faultType                          EventFaultType,
   faultRecordPurpose                 EventFaultRecordPurpose,
   faultBeginTime                     TimeReal,
   faultEndTime                       TimeReal,
   cardNumberDriverSlotBegin          FullCardNumber,
   cardNumberCodriverSlotBegin        FullCardNumber,
   cardNumberDriverSlotEnd            FullCardNumber,
   cardNumberCodriverSlotEnd          FullCardNumber
}
```

faultType er typen af den pågældende fejl ved kontrolapparatet.

faultRecordPurpose er det formål, til hvilket fejlen er blevet registreret.

faultBeginTime er fejlens startdato og -klokkeslæt.

faultEndTime er fejlens slutdato og -klokkeslæt.

cardNumberDriverSlotBegin identificerer det kort, der sad i førerens kortplads ved fejlens begyndelse.

cardNumberCodriverSlotBegin identificerer det kort, der sad i medchaufførens kortplads ved fejlens begyndelse.

cardNumberDriverSlotEnd identificerer det kort, der sad i førerens kortplads ved fejlens slutning.

cardNumberCodriverSlotEnd identificerer det kort, der sad i medchaufførens kortplads ved fejlens slutning.

2.135. **VuIdentification**

Oplysninger, gemt på en køretøjsenhed, vedrørende identifikation af denne (krav 075).

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

vuManufacturerName er navnet på fabrikanten af køretøjsenheden.

vuManufacturerAddress er adressen på fabrikanten af køretøjsenheden.

vuPartNumber er reservedelsnummeret på køretøjsenheden.

vuSerialNumber er serienummeret på køretøjsenheden.

vuSoftwareIdentification identificerer det programmel, der anvendes i køretøjsenheden.

vuManufacturingDate er køretøjsenhedens fabrikationsdato.

vuApprovalNumber er køretøjsenhedens typegodkendelsesnummer.

2.136. **VuManufacturerAddress**

Adressen på fabrikanten af køretøjsenheden.

```
VuManufacturerAddress ::= Address
```

Tilordnet værdi: Uspecificeret.

2.137. **VuManufacturerName**

Navnet på fabrikanten af køretøjsenheden.

```
VuManufacturerName ::= Name
```

Tilordnet værdi: Uspecificeret.

2.138. **VuManufacturingDate**

Fabrikationsdatoen for køretøjsenheden.

```
VuManufacturingDate ::= TimeReal
```

Tilordnet værdi: Uspecificeret.

2.139. **VuOverSpeedingControlData**

Oplysninger, gemt på en køretøjsenhed, vedrørende de overskridelser af tilladt hastighed, som har fundet sted siden seneste kontrol med overskridelse af tilladt hastighed (krav 095).

```
VuOverSpeedingControlData ::= SEQUENCE {
   lastOverspeedControlTime              TimeReal,
   firstOverspeedSince                   TimeReal,
   numberOfOverspeedSince                OverspeedNumber
}
```

lastOverspeedControlTime er dato og klokkeslæt for seneste kontrol for overskridelse af tilladt hastighed.

firstOverspeedSince er dato og klokkeslæt for første overskridelse af tilladt hastighed siden denne kontrol for overskridelse af tilladt hastighed.

numberOfOverspeedSince er antal hændelser med overskridelse af tilladt hastighed siden seneste kontrol for overskridelse af tilladt hastighed.

2.140. **VuOverSpeedingEventData**

Oplysninger, gemt på en køretøjsenhed, vedrørende hændelser med overskridelse af tilladt hastighed (krav 094).

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

noOfVuOverSpeedingEvents er antal hændelser opført i listen over hændelser i mængden vuOverSpeedingEventRecords.

vuOverSpeedingEventRecords er en mængde af poster vedrørende hændelser med overskridelse af tilladt hastighed.

2.141. **VuOverSpeedingEventRecord**

Oplysninger, gemt på en køretøjsenhed, vedrørende hændelser med overskridelse af tilladt hastighed (krav 094).

```
VuOverSpeedingEventRecord ::= SEQUENCE {
   eventType                             EventFaultType,
   eventRecordPurpose                    EventFaultRecordPurpose,
   eventBeginTime                        TimeReal,
   eventEndTime                          TimeReal,
   maxSpeedValue                         SpeedMax,
   averageSpeedValue                     SpeedAverage,
   cardNumberDriverSlotBegin             FullCardNumber,
   similarEventsNumber                   SimilarEventsNumber
}
```

eventType er hændelsens type.

eventRecordPurpose er det formål, hændelsen er registreret til.

eventBeginTime er hændelsens startdato og -klokkeslæt.

eventEndTime er hændelsens slutdato og -klokkeslæt.

maxSpeedValue er den højeste hastighed målt under hændelsen.

averageSpeedValue er den aritmetiske gennemsnitshastighed målt under hændelsen.

cardNumberDriverSlotBegin identificerer det kort, der er sat i førerens kortplads ved hændelsens start.

similarEventsNumber er antal tilsvarende hændelser samme døgn.

2.142. **VuPartNumber**

Serienummeret på køretøjsenheden.

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

Tilordnet værdi: Specifik for fabrikanten af køretøjsenheden.

2.143. **VuPlaceDailyWorkPeriodData**

Oplysninger, gemt på en køretøjsenhed, vedrørende de steder, hvor føreren begynder eller afslutter den daglige arbejdstid (krav 087).

```
VuPlaceDailyWorkPeriodData ::= SEQUENCE {
   noOfPlaceRecords                        INTEGER(0..255),
   vuPlaceDailyWorkPeriodRecords           SET SIZE(noOfPlaceRecords) OF
                                           VuPlaceDailyWorkPeriodRecord
}
```

noOfPlaceRecords er antal poster i mængden vuPlaceDailyWorkPeriodRecords.

vuPlaceDailyWorkPeriodRecords er en mængde af poster vedrørende steder.

2.144. **VuPlaceDailyWorkPeriodRecord**

Oplysninger, gemt på en køretøjsenhed, vedrørende de steder, hvor føreren begynder eller afslutter den daglige arbejdstid (krav 087).

```
VuPlaceDailyWorkPeriodRecord ::= SEQUENCE {
   fullCardNumber                          FullCardNumber,
   placeRecord                             PlaceRecord
}
```

fullCardNumber er førerens korttype, den kortudstedende medlemsstat og kortets nummer.

placeRecord indeholder oplysningerne om det indlæste sted.

2.145. **VuPrivateKey**

Køretøjsenhedens private nøgle.

```
VuPrivateKey ::= RSAKeyPrivateExponent
```

2.146. **VuPublicKey**

Køretøjsenhedens offentlige nøgle.

```
VuPublicKey ::= PublicKey
```

2.147. **VuSerialNumber**

Køretøjsenhedens serienummer (krav 075).

```
VuSerialNumber ::= ExtendedSerialNumber
```

2.148. **VuSoftInstallationDate**

Dato for installation af den programmelversion, som anvendes i køretøjsenheden.

```
VuSoftInstallationDate ::= TimeReal
```

Tilordnet værdi: Uspecificeret.

2.149. **VuSoftwareIdentification**

Oplysninger, gemt på en køretøjsenhed, vedrørende det installerede programmel.

```
VuSoftwareIdentification ::= SEQUENCE {
   vuSoftwareVersion                       VuSoftwareVersion,
   vuSoftInstallationDate                  VuSoftInstallationDate
}
```

vuSoftwareVersion er versionsnummeret på det programmel, der anvendes i køretøjsenheden.

vuSoftInstallationDate er datoen for installation af den pågældende version af programmellet.

2.150. **VuSoftwareVersion**

Versionsnummeret på det programmel, der anvendes i køretøjsenheden.

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

Tilordnet værdi: Uspecificeret.

2.151. **VuSpecificConditionData**

Oplysninger, gemt på en køretøjsenhed, vedrørende særlige omstændigheder.

```
VuSpecificConditionData ::= SEQUENCE {
   noOfSpecificConditionRecords          INTEGER(0..2^16-1)
   specificConditionRecords              SET SIZE (noOfSpecificConditionRecords)
                                         OF SpecificConditionRecord
}
```

noOfSpecificConditionRecords er det antal poster, som er indeholdt i mængden specificConditionRecords.

specificConditionRecords er en mængde af poster vedrørende særlige omstændigheder.

2.152. **VuTimeAdjustmentData**

Oplysninger, gemt på en køretøjsenhed, vedrørende tidsjusteringer, som har fundet sted uden for rammerne af en planmæssig kalibrering (krav 101).

```
VuTimeAdjustmentData ::= SEQUENCE {
   noOfVuTimeAdjRecords                  INTEGER(0..6),
   vuTimeAdjustmentRecords               SET SIZE(noOfVuTimeAdjRecords) OF
                                         VuTimeAdjustmentRecord
}
```

noOfVuTimeAdjRecords er antal poster i mængden vuTimeAdjustmentRecords.

vuTimeAdjustmentRecords er en mængde af tidsjusteringsposter.

2.153. **VuTimeAdjustmentRecord**

Oplysninger, gemt på en køretøjsenhed, vedrørende tidsjustering, som har fundet sted uden for rammerne af en planmæssig kalibrering (krav 101).

```
VuTimeAdjustmentRecord ::= SEQUENCE {
   oldTimeValue                          TimeReal,
   newTimeValue                          TimeReal,
   workshopName                          Name,
   workshopAddress                       Address,
   workshopCardNumber                    FullCardNumber
}
```

oldTimeValue, newTimeValue er gammel og ny værdi af dato og klokkeslæt.

workshopName, workshopAddress er værkstedets navn og adresse.

workshopCardNumber identificerer det værkstedskort, der er brugt til at foretage tidsjustering.

2.154. **W-VehicleCharacteristicConstant**

Køretøjets vejdrejetal (definition k)).

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

Tilordnet værdi: Impulser pr. kilometer med området 0 til 64 255 impulser/km.

2.155. **WorkshopCardApplicationIdentification**

Oplysninger, gemt på et værkstedskort, vedrørende identifikation af kortets applikation (krav 190).

```
WorkshopCardApplicationIdentification ::= SEQUENCE {
   typeOfTachographCardId                EquipmentType,
   cardStructureVersion                  CardStructureVersion,
   noOfEventsPerType                     NoOfEventsPerType,
   noOfFaultsPerType                     NoOfFaultsPerType,
   activityStructureLength               CardActivityLengthRange,
   noOfCardVehicleRecords                NoOfCardVehicleRecords,
   noOfCardPlaceRecords                  NoOfCardPlaceRecords,
   noOfCalibrationRecords                NoOfCalibrationRecords
}
```

typeOfTachographCardId angiver den implementerede korttype.

cardStructureVersion angiver den version af strukturen, som er implementeret i kortet.

noOfEventsPerType er antal hændelser af hver hændelsestype, som kan gemmes på kortet.

noOfFaultsPerType er antal fejl af hver fejltype, som kan gemmes på kortet.

activityStructureLength angiver antal byte til rådighed til lagring af aktivitetsposter.

noOfCardVehicleRecords er antal køretøjsposter, som kan gemmes på kortet.

noOfCardPlaceRecords er antal steder, som kan gemmes på kortet.

noOfCalibrationRecords er det antal kalibreringsposter, som kan gemmes på kortet.

2.156. **WorkshopCardCalibrationData**

Oplysninger, gemt på et værkstedskort, vedrørende de aktiviteter, der er udført med kortet (krav 227 og 229).

```
WorkshopCardCalibrationData ::= SEQUENCE {
   calibrationTotalNumber                INTEGER(0..2^16-1),
   calibrationPointerNewestRecord        INTEGER(0..NoOfCalibrationRecords-1),
   calibrationRecords                    SET SIZE(NoOfCalibrationRecords) OF
                                         WorkshopCardCalibrationRecord
}
```

calibrationTotalNumber er det samlede antal kalibreringer, som er udført med kortet.

calibrationPointerNewestRecord er indekset på senest opdaterede kalibreringspost.

Tilordnet værdi: Tal svarende til tælleren i kalibreringsposten, begyndende med '0' for den første forekomst af kalibreringsposterne i strukturen.

calibrationRecords er den mængde poster, der indeholder oplysninger vedrørende kalibrering og/eller tidsjustering.

2.157. **WorkshopCardCalibrationRecord**

Oplysninger, gemt på et værkstedskort, vedrørende den kalibrering, der er udført 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 er formålet med kalibreringen.

vehicleIdentificationNumber is the VIN.

vehicleRegistration indeholder køretøjets indregistreringsnummer og den indregistrerende medlemsstat.

wVehicleCharacteristicConstant er køretøjets vejdrejetal.

kConstantOfRecordingEquipment er kontrolapparatets konstant.

lTyreCircumference er den effektive dækperiferi.

tyreSize er dækdimensionsbetegnelsen for de dæk, der er monteret på køretøjet.

authorisedSpeed er køretøjets tilladte hastighed.

oldOdometerValue, newOdometerValue er gammel og ny kilometerstand.

oldTimeValue, newTimeValue er gammel og ny værdi af dato og klokkeslæt.

nextCalibrationDate er datoen for næste kalibrering af den type, som i CalibrationPurpose foreskrives at skulle udføres af kontrolmyndigheden.

vuPartNumber, vuSerialNumber and **sensorSerialNumber** er de dataelementer, som identificerer kontrolapparatet.

2.158. **WorkshopCardHolderIdentification**

Oplysninger, gemt på et værkstedskort, vedrørende identifikation af kortindehaveren (krav 216).

```
WorkshopCardHolderIdentification ::= SEQUENCE {
   workshopName                     Name,
   workshopAddress                  Address,
   cardHolderName                   HolderName,
   cardHolderPreferredLanguage      Language
}
```

workshopName er navnet på kortindehaverens værksted.

workshopAddress er adressen på kortindehaverens værksted.

cardHolderName er efternavn og fornavn(e) på indehaveren (f.eks navnet på mekanikeren).

cardHolderPreferredLanguage er det af kortindehaveren foretrukne sprog.

2.159. **mWorkshopCardPIN**

Det personlige identifikationsnummer på værkstedskortet (krav 213).

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

Tilordnet værdi: Den PIN-kode, som kendes af kortindehaveren, udfyldt mod højre med sideskiftbyte indtil 8 byte.

3. DEFINITIONER AF VÆRDI- OG STØRRELSESOMRÅDE

Definition af de variabelværdier, der er anvendt til definitionerne i punkt 2.

`TimeRealRange ::= 2^32-1`

3.1. **Definitioner til førerkortet:**

Navn på variabelværdi	Min	Max
`CardActivityLengthRange`	5 544 bytes (28 døgn med 93 aktivitetsskift i døgnet)	13 776 bytes (28 døgn med 240 aktivitetsskift i døgnet)
`NoOfCardPlaceRecords`	84	112
`NoOfCardVehicleRecords`	84	200
`NoOfEventsPerType`	6	12
`NoOfFaultsPerType`	12	24

3.2. **Definitioner til værkstedskortet:**

Navn på variabelværdi	Min	Max
`CardActivityLengthRange`	198 byte (1 døgn med 93 aktivitetsskift)	492 byte (1 døgn med 240 aktivitetsskift)
`NoOfCardPlaceRecords`	6	8
`NoOfCardVehicleRecords`	4	8
`NoOfEventsPerType`	3	3
`NoOfFaultsPerType`	6	6
`NoOfCalibrationRecords`	88	255

3.3. **Definitioner til kontrolkortet:**

Navn på variabelværdi	Min	Max
`NoOfControlActivityRecords`	230	520

3.4. **Definitioner til virksomhedskortet:**

Navn på variabelværdi	Min	Max
`NoOfCompanyActivityRecords`	230	520

4. CHARACTER SETS

Til IA5Strings anvendes ASCII-tegnsættet som defineret i ISO/IEC 8824-1. Af hensyn til letlæselighed og overskuelighed er de tilordnede værdier gengivet nedenfor. Ved eventuel uoverensstemmelse har ISO/IEC 8824-1 forrang for denne bemærkning.

```
 ! " # $ % & ' ( ) * + , - . / 0 1 2 3 4 5 6 7 8 9 : ; < = > ?
@ A B C D E F G H I J K L M N O P Q R S T U V W X Y Z [ \ ] ^ _
` a b c d e f g h i j k l m n o p q r s t u v w x y z { | } ~
```

I andre tegnstrenge (Address, Name, VehicleRegistrationNumber) anvendes herudover de tegn, der er fastlagt ved kode 192 til 255 af ISO/IEC 8859-1 (tegnsættet Latin 1) eller ISO/IEC 8859-7 (det græske tegnsæt).

5. KODNING

Ved kodning efter ASN.1 kodningsreglerne skal alle de definerede datatyper være kodet i overensstemmelse med ISO/IEC 8825-2, justeret variant.

Tillæg 2

SPECIFIKATION AF FARTSKRIVERKORT

1. INDLEDNING

1.1. **Forkortelser**

I dette tillæg anvendes følgende forkortelser:

AC	Adgangsbetingelser (Access conditions)
AID	Applikationsnavn (Application identifier)
ALW	Altid (Always)
APDU	Dataenhed i applikationsprotokol (struktur i kommando) (Application protocol data unit)
ATR	Svar på nulstilling (Answer to reset)
AUT	Identitetsbekræftet (Authenticated)
C6, C7	Kortets kontakt nr. 6 og 7 som beskrevet i ISO/IEC 7816-2
cc	klokcyklusser (clock cycles)
CHV	Information til verifikation af kortindehaver (Card holder verification information)
CLA	Klassebyte i APDU-kommando (Class byte of an APDU command)
DF	Dedikeret fil. En DF kan indeholde andre filer (EF eller DF)
EF	Elementærfil
ENC	Krypteret (Encrypted): Adgang kun mulig med krypteringsdata.
etu	Elementær tidsenhed (elementary time unit)
IC	Integreret kreds (Integrated circuit)
ICC	Chipkort (Integrated circuit card)
ID	Identifikator
IFD	Kortlæser (Interface device)
IFS	Længde af informationsfelt (Information field size)
IFSC	Længde af informationsfelt til kort (Information field size for the card)
IFSD	Informationsfeltlængde for kortlæser (Information field size device)
INS	Ordrebyte i APDU-kommando (Instruction byte)
Lc	Længde af inddata til APDU-kommando
Le	Længde af forventede data (uddata til en kommando)
MF	Hovedfil (dedikeret rodfil) (Master file)
P1-P2	Parameterbytes
NAD	Knudepunktadresse i en T=1 protokol (Node address)
NEV	Aldrig (Never)
PIN	Personligt identifikationsnummer
PRO SM	Beskyttet med sikker meddelelsesoverførsel (Protected with secure messaging)
PTS	Valgt transmissionsprotokol (Protocol transmission selection)
RFU	Forbeholdt fremtidig brug (Reserved for future use)

RST	Nulstilling (af et kort) (Reset)
SM	Sikker overførsel af meddelelser (Secure messaging)
SW1-SW2	Statusbytes
TS	Initialt tegn i ATR (svar på nulstilling)
VPP	Programmeringsspænding
XXh	Størrelsen XX i hexadecimal notation
||	Sammenkædningssymbol 03||04=0304

1.2. **Henvisninger**

I dette tillæg henvises til følgende referencer:

EN 726-3	Identification cards systems — Telecommunications integrated circuit(s) cards and terminals — Part 3: Application independent card requirements. December 1994.
ISO/IEC 7816-2	Information technology — Identification cards — Integrated circuit(s) cards with contacts — Part 2: Dimensions and location of the contacts. First edition: 1999.
ISO/IEC 7816-3	Information technology — Identification cards — Integrated circuit(s) cards with contacts — Part 3: Electronic signals and transmission protocol. Edition 2: 1997.
ISO/IEC 7816-4	Information technology — Identification cards — Integrated circuit(s) cards with contacts — Part 4: Interindustry commands for interexchange. First edition: 1995 + Amendment 1: 1997.
ISO/IEC 7816-6	Information technology — Identification cards — Integrated circuit(s) cards with contacts — Part 6: Interindustry data elements. First Edition: 1996 + Cor 1: 1998.
ISO/IEC 7816-8	Information technology — Identification cards — Integrated circuit(s) cards with contacts — Part 8: Security related interindustry commands. First Edition: 1999.
ISO/IEC 9797	Information technology — Security techniques — Data integrity mechanism using a cryptographic check function employing a block cipher algorithm. Edition 2: 1994.

2. ELEKTRISKE OG FYSISKE EGENSKABER

TCS_200 Alle elektroniske signaler skal overholde ISO/IEC 7816-3, medmindre andet er angivet.

TCS_201 Placering og dimensioner af kortets kontakter skal være i overensstemmelse med ISO/IEC 7816-2.

2.1. **Forsyningsspænding og strømforbrug**

TCS_202 Kortet skal fungere i henhold til specifikationerne inden for de forbrugsgrænser, der foreskrives i ISO/IEC 7816-3.

TCS_203 Kortet skal fungere med V_{cc} = 3 V (+/- 0,3 V) eller V_{cc} = 5 V (+/- 0,5 V).

Valg af spænding skal ske i overensstemmelse med ISO/IEC 7816-3.

2.2. **Programmeringsspænding V_{pp}**

TCS_204 Kortet må ikke kræve programmeringsspænding ved klemme C6. Det forventes at klemme C6 ikke tilsluttes en kortlæser. Kontakt C6 kan være tilsluttet V_{cc} i kortet men må ikke stelforbindes. Denne spænding må ikke i noget tilfælde tolkes.

2.3. **Klokgenerering og -frekvens**

TCS_205 Kortet skal arbejde i et frekvensområde fra 1 til 5 MHz. Inden for én kortsession kan klokfrekvensen variere ± 2 %. Klokfrekvensen genereres af køretøjsenheden, ikke af kortet selv. Arbejdscyklussen kan variere mellem 40 og 60 %.

TCS_206 Under de betingelser, der er indeholdt i kortfilen EF_{ICC}, kan den eksterne klokke standses. Den første byte i kroppen af filen EF_{ICC} koder for betingelserne i klokstop-funktionsmåde (for nærmere oplysninger henvises til EN 726-3):

Lav	Høj		
Bit 3	Bit 2	Bit 1	
0	0	1	Klokstop tilladt, intet foretrukket niveau
0	1	1	Klokstop tilladt, højt niveau foretrukket
1	0	1	Klokstop tilladt, lavt niveau foretrukket
0	0	0	Klokstop ikke tilladt
0	1	0	Klokstop kun tilladt på højt niveau
1	0	0	Klokstop kun tilladt på lavt niveau

Bit 4 til 8 ubenyttet.

2.4. **I/O-kontakt**

TCS_207 TCS_207 I/O-kontakten C7 anvendes til at modtage og overføre data fra og til kortlæseren. Under funktion må kun enten kortet eller kortlæseren være i dataoverførselsmåde. Hvis begge enheder er i overførselsmåde, må det ikke kunne medføre skade på kortet. Medmindre kortet overfører data, skal det skifte til modtagemåde.

2.5. **Kortets tilstande**

TCS_208 Kortet arbejder i to tilstande, mens forsyningsspændingen tilføres:

— i driftstilstand mens det udfører kommandoer eller er koblet til den digitale enhed,

— i hviletilstand på alle andre tidspunkter; i denne tilstand skal alle data ligge på kortet.

3. HARDWARE OG KOMMUNIKATION

3.1. **Indledning**

Dette afsnit beskriver de funktioner, der som minimum kræves af fartskriverkort og køretøjsenheder for at sikre korrekt funktion og interoperabilitet.

Fartskriverkort opfylder så vidt muligt de foreliggende gældende ISO/IEC normer (specielt ISO/IEC 7816). Dog beskrives kommandoer og protokoller fuldt ud for at specificere visse indskrænkninger i brugen eller visse forskelle, når sådanne findes. De foreskrevne kommandoer er fuldt forenelige med de anførte normer, medmindre andet er angivet.

3.2. **Transmissionsprotokol**

TCS_300 Transmissionsprotokollen skal være i overensstemmelse med ISO/IEC 7816-3. Specielt skal køretøjsenheden anerkende udvidelser af ventetid, som sendes af kortet.

3.2.1. ***Protokoller***

TCS_301 Kortet skal give mulighed både for protokol T=0 og protokol T=1.

TCS_302 T=0 er standardprotokol, hvorfor der kræves en PTS-kommando for at ændre protokol til T=1.

TCS_303 Enheder skal understøtte direkte konvention i begge protokoller: Den direkte konvention er følgelig påbudt for kortet.

TCS_304 Feltstørrelsesbyten skal placeres i karakter TA3 i ATR (svar på reset). Denne værdi skal være mindst 'F0h' (= 240 bytes).

For protokollerne gælder følgende begrænsninger:

TCS_305 T=0

— Kortlæseren skal understøtte et svar på I/O efter begyndelsen af signalet på nulstilling fra 400 cc.

— Kortlæseren skal kunne læse tegn, som er adskilt af 12 etu.

— Kortlæseren skal læse en forkert karakter og dens gentagelse, hvis de er adskilt af 13 etu. Hvis der registreres en forkert karakter, kan fejlsignalet på I/O optræde mellem 1 etu og 2 etu. Kortlæseren skal understøtte en forsinkelse på 1 etu.

— Kortlæseren skal acceptere et svar på nulstilling (ATR) på 33 bytes (TS+32).

— Hvis det pågældende ATR indeholder et TC1, skal den ekstra beskyttelsestid gælde for tegn sendt af kortlæseren, dog kan tegn sendt af kortet stadig være adskilt af 12 etu. Dette gælder også for ACK-tegnet sendt af kortet efter, at der er afgivet et P3-tegn af kortlæseren.

— Kortlæseren skal tage hensyn til et NUL-tegn afsendt fra kortet.

— Kortlæseren skal acceptere den supplerende funktionsmåde for ACK.

— Kommandoen GET RESPONSE kan ikke bruges i kædningsfunktion til at hente data, hvis længde eventuelt er over 255 bytes.

TCS_306 T=1

— NAD-byte: Ikke anvendt (NAD skal sættes til '00').

— S-block ABORT: Ikke anvendt.

— S-block VPP state error: Ikke anvendt.

— Den totale kædningslængde for et datafelt er ikke over 255 bytes (skal sikres af kortlæseren).

— Informationsfeltstørrelse for kortlæser (IFSD) skal angives af kortlæseren umiddelbart efter svar på nulstilling: Kortlæseren skal overføre S-blokkens IFS-forespørgsel efter svar på nulstilling (ATR), og kortet skal tilbagemelde S-blokkens IFS. Den anbefalede værdi for IFSD er 254 bytes.

— Kortet anmoder ikke om efterjustering af IFS.

3.2.2. ***ATR***

TCS_307 Korlæseren kontrollerer ATR-bytes (svar på nulstilling) i henhold til ISO/IEC 7816-3. Der skal ikke foretages kontrol af historiske ATR-tegn.

Eksempel på grundlæggende biprotokollær ATR i henhold til ISO/IEC 7816-3

Tegn	Værdi	Bemærkninger
TS	'3Bh'	Angiver direkte konvention
T0	'85h'	TD1 foreligger; 5 historiske bytes til stede
TD1	'80h'	TD2 foreligger; T=0 skal anvendes
TD2	'11h'	TA3 foreligger; T=1 skal anvendes
TA3	'XXh' (mindst 'F0h')	Størrelse af informationsfelt på kort (IFSC)
TH1 til TH5	'XXh'	Historiske tegn
TCK	'XXh'	Kontroltegn (eksklusiv OR)

TCS_308 Efter svar på nulstilling (ATR) er hovedfilen (MF) valgt automatisk og bliver aktuel mappe.

3.2.3. ***PTS***

TCS_309 Standardprotokollen er T=0. For at vælge protokol T=1 skal der sendes en PTS (også benævnt PPS) til kortet fra kortlæseren.

TCS_310 Da protokollerne T=0 og T=1 begge er påbudte for kortet, er det grundlæggende valg af transmissionsprotokol (PTS) for protokolskift påbudt for kortet.

Som angivet i ISO/IEC 7816-3 kan PTS benyttes til at skifte til en højere transmissionshastighed end den standardhastighed, som vælges af kortet i svar på nulstilling (ATR) hvis der er nogen (TA(1)) byte tilstede.

Højere tranmissionshastigheder er valgfri for kortet.

TCS_311 Hvis ingen anden transmissionshastighed end standardhastigheden understøttes (eller den valgte transmissionshastighed ikke understøttes), skal kortet svare korrekt på protokoltranmissionsvalget (PTS) i henhold til ISO/IEC 7816-3 ved at udelade PPS1-byten.

Følgende er eksempler på grundlæggende PTS til protokolvalg:

Tegn	Værdi	Bemærkninger
PPSS	'FFh'	Starttegn
PPS0	'00h' or '01h'	PPS1 til PPS3 findes ikke; '00h' for at vælge T0, '01h' for at vælge T1
PK	'XXh'	Kontroltegn: 'XXh' = 'FFh' hvis PPS0 = '00h', 'XXh' = 'FEh' hvis PPS0 = '01h'

3.3. **Adgangsbetingelser (AC)**

Adgangsbetingelserne (AC) for kommandoerne UPDATE BINARY og READ BINARY er defineret for hver elementærfil.

TCS_312 Adgangsbetingelserne (AC) for den aktuelle fil skal være opfyldt, før man kan få adgang til filen med disse kommandoer.

Definitionerne på de foreliggende adgangsbetingelser er følgende:

— ALW: Operationen er altid mulig og kan udføres uden begrænsning.

— NEV: Operationen er aldrig mulig.

— AUT: Rettighederne svarende til vellykket ekstern ægthedsbekræftelse skal åbnes (fås med kommandoen EXTERNAL AUTHENTICATE).

— PRO SM: Kommandoen skal overføres med en kryptografisk kontrolsum med sikkert meddelelsessystem (se tillæg 11).

— AUT og PRO SM (kombineret)

På databehandlingskommandoerne (UPDATE BINARY og READ BINARY) kan der sættes følgende adgangsbetingelser i kortet:

	UPDATE BINARY	READ BINARY
ALW	Ja	Ja
NEV	Ja	Ja
AUT	Ja	Ja
PRO SM	Ja	Nej
AUT og PRO SM	Ja	Nej

Adgangsbetingelsen PRO SM er ikke til rådighed for READ BINARY kommandoen. Dette indebærer, at der aldrig er påbudt en kryptografisk kontrolsum for en READ kommando. Ved at bruge værdien af 'OC' for klassen kan man bruge kommandoen READ BINARY med sikker meddelelsesoverførsel som beskrevet i punkt 3.6.2.

3.4. **Datakryptering**

Når data i en fil skal være fortrolige, mærkes filen »Encrypted«. Kryptering sker ved hjælp af sikker meddelelsesoverførsel (se tillæg 11).

3.5. **Oversigt over kommandoer og fejlkoder**

Kommandoer og filorganisation er afledt af og i overensstemmelse med ISO/IEC 7816-4.

TCS_313 I dette afsnit beskrives følgende par APDU kommando-svar:

Kommando	INS
SELECT FILE	A4
READ BINARY	B0
UPDATE BINARY	D6
GET CHALLENGE	84
VERIFY	20
GET RESPONSE	C0
PERFORM SECURITY OPERATION: VERIFY CERTIFICATE COMPUTE DIGITAL SIGNATURE VERIFY DIGITAL SIGNATURE HASH	2A
INTERNAL AUTHENTICATE	88
EXTERNAL AUTHENTICATE	82
MANAGE SECURITY ENVIRONMENT: SETTING A KEY	22
PERFORM HASH OF FILE	2A

TCS_314 Statusordet SW1 SW2 tilbagemeldes sammen med enhver svarmeddelelse og angiver behandlingsstatus for kommandoen.

SW1	SW2	Betydning
90	00	Normal behandling af data
61	XX	Normal behandling af data. XX = antal svarbytes til rådighed
62	81	Advarselsbehandling. En del af svardata kan være beskadiget
63	CX	Forkert CHV (kortindehaververifikation, PIN). Indholdet i tæller for resterende forsøg tilbagemeldes med 'X'
64	00	Kørselsfejl — Status af ikke-flygtigt lager uændret. Integritetsfejl
65	00	Kørselsfejl — Status af ikke-flygtigt lager ændret
65	81	Kørselsfejl — Status af ikke-flygtigt lager ændret. Hukommelsesfejl
66	88	Sikkerhedsfejl: Forkert kryptografisk kontrolsum (ved sikker meddelelsesoverførsel) eller forkert certifikat (ved verifikation af certifikat) eller forkert kryptogram (ved ekstern ægthedsbekræftelse) eller forkert underskrift (ved verifikation af underskrift)
67	00	Forkert længde (forkert Lc eller Le)
69	00	Forbudt kommando (intet svar foreligger i T=0)
69	82	Sikkerhedsstatus ikke tilfredsstillet
69	83	Ægthedsbekræftelse blokeret
69	85	Betingelser for anvendelse ikke opfyldt
69	86	Kommando ikke tilladt (ingen aktuel elementærfil)
69	87	Forventede dataobjekter for sikker meddelelsesoverførsel mangler
69	88	Ukorrekte dataobjekter for sikker meddelelsesoverførsel
6A	82	Filer ikke fundet
6A	86	Forkerte parametre P1-P2
6A	88	De adresserede data kunne ikke findes
6B	00	Forkerte parametre (adressetillæg uden for elementærfil)

SW1	SW2	Betydning
6C	XX	Forkert længde, SW2 angiver eksakt længde. Intet datafelt tilbagemeldes
6D	00	Operationskode ikke understøttet eller ugyldig
6E	00	Klasse ikke understøttet
6F	00	Andre kontrolfejl

3.6. **Beskrivelse af kommandoer**

Påbudte kommandoer for fartskriverkort er beskrevet i dette kapitel.

Supplerende relevante enkeltheder om de anvendte kryptografiske operationer er givet i tillæg 11 (fælles sikkerhedsmekanismer).

Alle kommandoer beskrives uafhængigt af den anvendte protokol (T=0 eller T=1). APDU bytene CLA, INS, P1, P2, Lc og Le bliver altid angivet. Hvis Lc eller Le ikke er nødvendig for den beskrevne kommando, er den tilhørende længde, værdi og beskrivelse tomme.

TCS_315 Anmodes der om begge længdebytes (Lc og Le), skal den beskrevne kommando deles i to dele, hvis kortlæseren bruger protokol T=0: Kortlæseren sender kommandoen som beskrevet ved hjælp af P3=Lc + data og sender derefter en GET RESPONSE (se punkt 3.6.6) kommando med P3=Le.

TCS_316 Anmodes der om begge længdebytes, og Le=0 (sikker meddelelsesoverførsel):

— når der bruges protokol T=1, skal kortet svare på Le=0 ved at sende alle tilgængelige uddata.

— når protokol T=0 anvendes, skal kortlæseren sende den første kommando med P3=Lc + data, kortet skal (på det implicitte Le=0) svare med statusbytes '61La', hvor La er antal svarbytes til rådighed. Kortlæseren skal derefter generere en GET RESPONSE kommando med P3 = La for at læse data.

3.6.1. ***Select File***

Denne kommando overholder ISO/IEC 7816-4, men har begrænset anvendelse i forhold til den i normen definerede kommando.

SELECT FILE kommandoen anvendes:

— til at vælge en applikationsdedikeret fil (skal vælges med navn)

— til at vælge en elementærfil svarende til det forelagte filnavn

3.6.1.1. *Valg ved navn (AID)*

Med denne kommando kan der vælges en applikationsdedikeret fil på kortet.

TCS_317 Denne kommando kan udføres fra et vilkårligt sted i filstrukturen (efter svar på nulstilling (ATR) eller på et vilkårligt tidspunkt).

TCS_318 Når der vælges en applikation, bliver det aktuelle sikkerhedsmiljø nulstillet. Når der er valgt applikation, er der ikke længere valgt en aktuel offentlig nøgle, og nøglen til den tidligere session er ikke længere til rådighed for sikre meddelelser. Adgangsbetingelsen AUT mistes ligeledes.

TCS_319 Kommandomeddelelse

Byte	Længde	Værdi	Beskrivelse
CLA	1	'00h'	
INS	1	'A4h'	
P1	1	'04h'	Valg ved navn (AID)
P2	1	'0Ch'	Intet svar forventet
Lc	1	'NNh'	Antal bytes sendt til kortet (længde af AID): '06h' for fartskriveapplikationen
#6-#(5+NN)	NN	'XX..XXh'	AID: 'FF 54 41 43 48 4F' for fartskriverapplikationen

Der kræves intet svar på kommandoen SELECT FILE (Le findes ikke i T=1, eller der anmodes ikke om svar i T=0).

TCS_320 Svarmeddelelse (der er ikke anmodet om svar)

Byte	Længde	Værdi	Beskrivelse
SW	2	'XXXXh'	Statusord (SW1, SW2)

— Giver kommandoen resultat, tilbagemelder kortet '9000'.

— Hvis den applikation, som svarer til applikationsnavnet, ikke findes, tilbagemeldes status '6A82'.

— Hvis byten Le er til stede i T=1, tilbagemeldes status '6700'.

— Hvis der i T=0 anmodes om et svar efter SELECT FILE kommandoen, tilbagemeldes status '6900'.

— Hvis den valgte applikation anses for beskadiget (der er fundet integritetsfejl i filattributterne), tilbagemeldes status '6400' eller '6581'.

3.6.1.2. *Valg af en elementærfil ved hjælp af filnavnet*

TCS_321 Kommandomeddelelse

Byte	Længde	Værdi	Beskrivelse
CLA	1	'00h'	
INS	1	'A4h'	
P1	1	'02h'	Valg af en elementærfil under den aktuelle dedikerede fil
P2	1	'0Ch'	Intet svar forventet
Lc	1	'02h'	Antal bytes sendt til kortet
#6-#7	2	'XXXXh'	Filnavn

Der kræves intet svar på kommandoen SELECT FILE (Le findes ikke i T=1, eller der anmodes ikke om svar i T=0).

TCS_322 Svarmeddelelse (der er ikke anmodet om svar)

Byte	Længde	Værdi	Beskrivelse
SW	2	'XXXXh'	Statusord (SW1, SW2)

— Giver kommandoen resultat, tilbagemelder kortet '9000'.

— Hvis filen svarende til det pågældende filnavn ikke findes, tilbagemeldes status '6A82'.

— Hvis byten Le er til stede i T=1, tilbagemeldes status '6700'.

— Hvis der i T=0 anmodes om et svar efter SELECT FILE kommandoen, tilbagemeldes status '6900'.

— Hvis den valgte fil anses for beskadiget, (der er fundet integritetsfejl i filattributterne), tilbagemeldes status '6400' eller '6581'.

3.6.2. ***Read Binary***

Denne kommando overholder ISO/IEC 7816-4, men har begrænset anvendelse i forhold til den i normen definerede kommando.

Kommandoen READ BINARY anvendes til at læse data fra en transparent fil.

Kortets svar består i at tilbagemelde de læste data, om ønsket indkapslet i en sikker meddelelsesstruktur.

TCS_323 Kommandoen kan kun udføres, forudsat at sikkerhedsstatus opfylder de sikkerhedsegenskaber, som er defineret for elementærfilen med henblik på READ-funktionen.

3.6.2.1. *Kommando uden sikker meddelelsesoverførsel*

Denne kommando giver kortlæseren mulighed for uden sikker meddelelsesoverførsel at læse data fra den aktuelt valgte elementærfil.

TCS_324 Med denne kommando må der ikke kunne læses data fra en fil mærket som »krypteret«.

TCS_325 Kommandomeddelelse

Byte	Længde	Værdi	Beskrivelse
CLA	1	'00h'	Der er ikke anmodet om sikker meddelelsesoverførsel
INS	1	'B0h'	
P1	1	'XXh'	Forskydning i bytes fra filens begyndelse: Mest betydende byte
P2	1	'XXh'	Forskydning i bytes fra filens begyndelse: Mindst betydende byte
Le	1	'XXh'	Forventet længde af data. Antal bytes som skal læses

Bemærkning: bit 8 af P1 skal være sat til 0.

TCS_326 Svarmeddelelse

Byte	Længde	Værdi	Beskrivelse
#1-#X	X	'XX..XXh'	Data læst
SW	2	'XXXXh'	Statusord (SW1, SW2)

— Giver kommandoen resultat, tilbagemelder kortet '9000'.

— Vælges ingen elementærfil, tilbagemeldes status '6986'.

— Er adgangsbetingelserne for den valgte fil ikke opfyldt, afbrydes kommandoen med '6982'.

— Er forskydningen ikke forenelig med elementærfilens størrelse (forskydning > størrelse af EF), tilbagemeldes status '6B00'.

— Er størrelsen af de data, der skal læses, ikke forenelig med elementærfilens størrelse (forskydning + Le > størrelsen af EF), tilbagemeldes status '6700' eller '6Cxx', hvor 'xx' er den eksakte længde.

— Konstateres der en integritetsfejl i filatttributterne, skal kortet anse filen for uoprettelig beskadiget, og den tilbagemeldte behandlingsstatur er '6400' eller '6581'.

— Konstateres der en integritetsfejl i de lagrede data, skal kortet returnere de ønskede data, og der tilbagemeldes status '6281'.

3.6.2.2. *Kommando med sikker meddelelsesoverførsel*

Denne kommando giver IDF mulighed for at læse data fra den aktuelt valgte elementærfil med sikkert meddelelsessystem, med det formål at efterprøve identiteten af de modtagne data og beskytte fortroligheden af data i tilfælde hvor elementærfilen er mærket »krypteret«.

TCS_327 Kommandomeddelelse

Byte	Længde	Værdi	Beskrivelse
CLA	1	'0Ch'	Der er anmodet om sikker meddelelsesoverførsel
INS	1	'B0h'	INS
P1	1	'XXh'	P1 (forskydning i bytes fra filens begyndelse): Mest betydende byte
P2	1	'XXh'	P2 (forskydning i bytes fra filens begyndelse): Mindst betydende byte
Lc	1	'09h'	Længde af inddata til sikker meddelelse
#6	1	'97h'	T_{LE}: Etiket for angivelse af forventet længde.
#7	1	'01h'	L_{LE}: Forventet længde
#8	1	'NNh'	Angivelse af forventet længde (oprindelig Le): Antal bytes som skal læses

Byte	Længde	Værdi	Beskrivelse
#9	1	'8Eh'	T_{CC}: Etiket for kryptografisk kontrolsum
#10	1	'04h'	L_{CC}: Længde af efterfølgende kryptografiske kontrolsum
#11-#14	4	'XX..XXh'	Kryptografisk kontrolsum (4 mest betydende bytes)
Le	1	'00h'	Som foreskrevet i ISO/IEC 7816-4

TCS_328 Svarmeddelelse hvis elementærfilen ikke er mærket som »krypteret« og hvis indgangsformatet for sikker meddelelsesoverførsel er korrekt:

Byte	Længde	Værdi	Beskrivelse
#1	1	'81h'	T_{PV}: Etiket for data med ordinær værdi
#2	L	'NNh' eller '81 NNh'	L_{PV}: Længde af tilbagemeldte data (= original Le) L er 2 bytes hvis L_{PV}>127 bytes
#(2+L)-#(1+L+NN)	NN	'XX..XXh'	Ordinær dataværdi
#(2+L+NN)	1	'8Eh'	T_{CC}: Etiket for kryptografisk kontrolsum
#(3+L+NN)	1	'04h'	L_{CC}: Længde af efterfølgende kryptografiske kontrolsum
#(4+L+NN)-#(7+L+NN)	4	'XX..XXh'	Kryptografisk kontrolsum (4 mest betydende bytes)
SW	2	'XXXXh'	Statusord (SW1, SW2)

TCS_329 Svarmeddelelse hvis elementærfilen er mærket som »krypteret« og hvis inddataformatet for sikker meddelelsesoverførsel er korrekt:

Byte	Længde	Værdi	Beskrivelse
#1	1	'87h'	$T_{PI\ CG}$: Etiket for krypterede data (kryptogram)
#2	L	'MMh' eller '81 MMh'	$L_{PI\ CG}$: Længde af tilbagemeldte krypterede data (afviger pga. udfyldning fra kommandoens oprindelig længde Le) L er 2 bytes hvis $L_{PI\ CG}$ > 127 bytes
#(2+L)-#(1+L+MM)	MM	'01XX..XXh'	Krypterede data: Udfyldningsindikator og kryptogram
#(2+L+MM)	1	'8Eh'	T_{CC}: Etiket for kryptografisk kontrolsum
#(3+L+MM)	1	'04h'	L_{CC}: Længde af efterfølgende kryptografiske kontrolsum
#(4+L+MM)-#(7+L+MM)	4	'XX..XXh'	Kryptografisk kontrolsum (4 mest betydende bytes)
SW	2	'XXXXh'	Statusord (SW1, SW2)

De tilbagemeldte krypterede data indeholder en første byte, som angiver den anvendte udfyldningmåde. Til fartskriverapplikationen antager udfyldningsindikatoren altid værdien '01h', som angiver, at den anvendte udfyldningsmåde er den, der foreskrives i ISO/IEC 7816-4 (én byte med værdien '80h' efterfulgt af nogle nul-bytes: ISO/IEC 9797 metode 1).

De »ordinære« behandlingsstatusser, som beskrives for kommandoen READ BINARY uden sikker dataoverførsel (se punkt 3.6.2.1), kan tilbagemeldes med de svarmeddelelsesstrukturer, som er beskrevet ovenfor.

Derudover kan der optræde visse fejl særligt vedrørende sikker meddelelsesoverførsel. I så fald tilbagemeldes behandlingsstatus simpelthen, uden at nogen struktur for sikker dataoverførsel er inddraget:

TCS_330 Svarmeddelelse hvis det indlæste format for sikker meddelelsesoverførsel er ukorrekt

Byte	Længde	Værdi	Beskrivelse
SW	2	'XXXXh'	Statusord (SW1, SW2)

— Foreligger der ingen nøgle for den aktuelle session, tilbagemeldes behandlingsstatus '6A88'. Dette sker, hvis sessionsnøglen enten ikke er genereret i forvejen eller er blevet ugyldig (i så fald skal kortlæseren på ny udføre den gensidige ægthedsbekræftelse, så der fastsættes en ny sessionsnøgle).

— Hvis der mangler nogle forventede dataobjekter (som ovenfor specificeret) i formatet for sikker meddelelsesoverførsel, tilbagemeldes behandlingsstatus '6987': Denne fejl opstår, hvis der mangler en forventet etiket eller hvis kommandoen ikke er korrekt opbygget.

— Hvis nogle dataobjekter er ukorrekte, tilbagemeldes status '6988': Denne fejl optræder, når alle de nødvendige etiketter er tilstede, men visse af længderne ikke svarer til de forventede.

— Lykkes verifikationen af den kryptografiske kontrolsum ikke, tilbagemeldes behandlingsstatus '6688'.

3.6.3. ***Update Binary***

Denne kommando overholder ISO/IEC 7816-4, men har begrænset anvendelse i forhold til den i normen definerede kommando.

Med kommandomeddelelsen UPDATE BINARY igangsættes opdatering (sletning + skrivning) af de bits, der i forvejen ligger i en binær elementærfil, med de bits, der er indeholdt i kommandoen APDU.

TCS_331 Kommandoen kan kun udføres, hvis sikkerhedsstatus opfylder de sikkerhedsegenskaber, som er defineret for elementærfilen med henblik på UPDATE-funktionen. Indgår PRO SM i adgangskontrollen til UPDATE-funktionen, skal der tilføjes sikker meddelelsesoverførsel i kommandoen).

3.6.3.1. *Kommando uden sikker meddelelsesoverførsel*

Denne kommando giver kortlæseren mulighed for at skrive data til den aktuelt valgte elementærfil, uden at kortet kontrollerer ægtheden af de modtagne data. Denne ordinære funktionsmåde tillades kun, hvis den tilknyttede fil ikke er mærket som »krypteret«.

TCS_332 Kommandomeddelelse

Byte	Længde	Værdi	Beskrivelse
CLA	1	'00h'	Der er ikke anmodet om sikker meddelelsesoverførsel
INS	1	'D6h'	
P1	1	'XXh'	Forskydning i bytes fra filens begyndelse: Mest betydende byte
P2	1	'XXh'	Forskydning i bytes fra filens begyndelse: Mindst betydende byte
Lc	1	'NNh'	Længde af data, som skal opdateres. Antal bytes som skal skrives
#6-#(5+NN)	NN	'XX..XXh'	Data som skal skrives

Bemærkning: bit 8 af P1 skal være sat til 0.

TCS_333 Svarmeddelelse

Byte	Længde	Værdi	Beskrivelse
SW	2	'XXXXh'	Statusord (SW1, SW2)

— Giver kommandoen resultat, tilbagemelder kortet '9000'.

— Vælges ingen elementærfil, tilbagemeldes behandlingsstatus '6986'.

— Er adgangsbetingelserne for den valgte fil ikke opfyldt, afbrydes kommandoen med '6982'.

— Er forskydningen ikke forenelig med elementærfilens størrelse (forskydning > størrelse af EF), tilbagemeldes status '6B00'.

— Er størrelsen af de data, der skal skrives, ikke forenelig med elementærfilens størrelse (forskydning + Le > størrelsen af EF), tilbagemeldes status '6700'.

— Konstateres der en integritetsfejl i filattributterne, skal kortet anse filen for uoprettelig beskadiget, og der tilbagemeldes status '6400' eller '6500'.

— Hvis der ikke kan skrives, tilbagemeldes behandlingsstatus '6581'.

3.6.3.2. *Kommando med sikker meddelelsesoverførsel*

Denne kommando giver kortlæseren mulighed for at skrive data til den aktuelt valgte elementærfil, idet kortet kontroller ægtheden af de modtagne data. Da der ikke kræves fortrolighed, er data ikke krypteret.

TCS_334 Kommandomeddelelse

Byte	Længde	Værdi	Beskrivelse
CLA	1	'0Ch'	Sikker overførsel Anmodet
INS	1	'D6h'	INS
P1	1	'XXh'	Forskydning i bytes fra filens begyndelse: Mest betydende byte
P2	1	'XXh'	Forskydning i bytes fra filens begyndelse: Mindst betydende byte
Lc	1	'XXh'	Længde af det sikrede datafelt
#6	1	'81h'	T_{PV}: Etiket for data med ordinær værdi
#7	L	'NNh' eller '81 NNh'	L_{PV}: Længde af overførte data L er 2 bytes hvis L_{PV} > 127 bytes
#(7+L)-#(6+L+NN)	NN	'XX..XXh'	Værdi af ordinære data (data som skal skrives)
#(7+L+NN)	1	'8Eh'	T_{CC}: Etiket for kryptografisk kontrolsum
#(8+L+NN)	1	'04h'	L_{CC}: Længde af efterfølgende kryptografiske kontrolsum
#(9+L+NN)-#(12+L+NN)	4	'XX..XXh'	Kryptografisk kontrolsum (4 mest betydende bytes)
Le	1	'00h'	Som foreskrevet i ISO/IEC 7816-4

TCS_335 Svarmeddelelse hvis inddata har det korrekte format til sikker meddelelsesoverførsel

Byte	Længde	Værdi	Beskrivelse
#1	1	'99h'	T_{SW}: Etiket for statusord (skal beskyttes af CC)
#2	1	'02h'	L_{SW}: Længde af tilbagemeldte statusord
#3-#4	2	'XXXXh'	Statusord (SW1, SW2)
#5	1	'8Eh'	T_{CC}: Etiket for kryptografisk kontrolsum
#6	1	'04h'	L_{CC}: Længde af efterfølgende kryptografiske kontrolsum
#7-#10	4	'XX..XXh'	Kryptografisk kontrolsum (4 mest betydende bytes)
SW	2	'XXXXh'	Statusord (SW1, SW2)

De »ordinære« behandlingsstatusser, som beskrives for kommandoen UPDATE BINARY uden sikker meddelelsesoverførsel (se punkt 3.6.3.1), kan tilbagemeldes med den svarmeddelelsesstruktur, som er beskrevet ovenfor.

Derudover kan der optræde visse fejl, som særligt vedrører sikker meddelelsesoverførsel. I så fald tilbagemeldes behandlingsstatus simpelthen, uden at nogen struktur for sikker meddelelsesoverførsel er inddraget:

TCS_336 Svarmeddelelse ved fejl i sikker meddelelsesoverførsel

Byte	Længde	Værdi	Beskrivelse
SW	2	'XXXXh'	Statusord (SW1, SW2)

— Foreligger der ingen nøgle for den aktuelle session, tilbagemeldes behandlingsstatus '6A88'.

— Hvis der mangler nogle forventede dataobjekter (som ovenfor specificeret) i formatet for sikker meddelelsesoverførsel, tilbagemeldes behandlingsstatus '6987': Denne fejl opstår, hvis der mangler en forventet etiket, eller hvis kommandoen ikke er korrekt opbygget.

— Hvis nogle dataobjekter er ukorrekte, tilbagemeldes '6988': Denne fejl optræder, når alle de nødvendige etiketter er tilstede, men visse af længderne er forskellige fra de forventede.

— Lykkes verifikationen af den kryptografiske kontrolsum ikke, tilbagemeldes behandlingsstatus '6688'.

3.6.4. ***Get Challenge***

Denne kommando overholder ISO/IEC 7816-4, men har begrænset anvendelse i forhold til den i normen definerede kommando.

Med GET CHALLENGE kommandoen beder man kortet afgive en challenge for at bruge den i en sikkerhedsrelateret procedure, hvori der sendes et kryptogram eller nogle kryptograferede data til kortet.

TCS_337 Den challenge, som afgives af kortet, er kun gyldig for den næste kommando, som anvender en challenge, som sendes til kortet.

TCS_338 Kommandomeddelelse

Byte	Længde	Værdi	Beskrivelse
CLA	1	'00h'	CLA
INS	1	'84h'	INS
P1	1	'00h'	P1
P2	1	'00h'	P2
Le	1	'08h'	Le (forventet længde af challenge).

TCS_339 Svarmeddelelse

Byte	Længde	Værdi	Beskrivelse
#1-#8	8	'XX..XXh'	Challenge
SW	2	'XXXXh'	Statusord (SW1, SW2)

— Giver kommandoen resultat, tilbagemelder kortet '9000'.

— Hvis længden Le er forskellig fra '08h', er behandlingsstatus '6700'.

— Hvis parametrene P1-P2 er ukorrekte, er behandlingsstatus '6A86'.

3.6.5. ***Verify***

Denne kommando overholder ISO/IEC 7816-4, men har begrænset anvendelse i forhold til den i normen definerede kommando.

VERIFY kommandoen får kortet til at sammenholde de CHV- (PIN) data, som sendes med kommandoen, med kortindehaverens reference-CHV, som er gemt på kortet.

Bemærkning: Det PIN, der er indlæst af brugeren, skal af kortlæseren være udfyldt mod højre med 'FFh'-bytes til en længde af 8 bytes.

TCS_340 Hvis kommandoen giver resultat, åbnes rettigheder svarende til korrekt CHV, og tælleren for resterende CHV-forsøg tilbagestilles.

TCS_341 Manglende overensstemmelse mellem oplysningerne registreres på kortet for at begrænse antal yderligere forsøg på benyttelse af reference-CHV.

TCS_342 Kommandomeddelelse

Byte	Længde	Værdi	Beskrivelse
CLA	1	'00h'	CLA
INS	1	'20h'	INS
P1	1	'00h'	P1
P2	1	'00h'	P2 (det verificerede CHV kendes implicit)
Lc	1	'08h'	Længden af den overførte CHV-kode
#6-#13	8	'XX..XXh'	CHV

TCS_343 Svarmeddelelse

Byte	Længde	Værdi	Beskrivelse
SW	2	'XXXXh'	Statusord (SW1, SW2)

— Giver kommandoen resultat, tilbagemelder kortet '9000'.

— Hvis reference-CHV'et ikke findes, tilbagemeldes status '6A88'.

— Hvis CHV'er er blokeret (tælleren for restererende forsøg for det pågældende CHV har værdien nul),tilbagemeldes behandlingsstatus '6983'. Når først CHV'et er i denne status, kan det pågældende CHV ikke længere fremvises med held.

— Stemmer oplysningerne ikke sammen, bliver tælleren for resterende forsøg formindsket, og der tilbagemeldes status '63CX' (X > 0 og X er lig værdien af tælleren for resterende CHV-forsøg). Hvis X = 'F', har tælleren for CHV-forsøg større værdi end 'F').

— Hvis reference-CHV anses for beskadiget, tilbagemeldes status '6400' eller '6581'.

3.6.6. ***Get Response***

Denne kommando er i overensstemmelse med ISO/IEC 7816-4.

Denne kommando (som kun er nødvendig og tilgængelig for protokollen T=0) benyttes til at overføre behandlede data fra kortet til kortlæseren (i tilfælde hvor både Lc og Le er indgået i en kommando).

Kommandoen GET RESPONSE skal udstedes straks efter den kommando, som behandler data, ellers mistes data. Efter udførelse af kommandoen GET RESPONSE, er de tidligere behandlede data ikke længere tilgængelige (medmindre fejlen '61xx' eller '6Cxx' optræder, se nedenfor).

TCS_344 Kommandomeddelelse

Byte	Længde	Værdi	Beskrivelse
CLA	1	'00h'	
INS	1	'C0h'	
P1	1	'00h'	
P2	1	'00h'	
Le	1	'XXh'	Antal bytes forventet

TCS_345 Svarmeddelelse

Byte	Længde	Værdi	Beskrivelse
#1-#X	X	'XX..XXh'	Data
SW	2	'XXXXh'	Statusord (SW1, SW2)

— Giver kommandoen resultat, tilbagemelder kortet '9000'.

— Hvis ingen data er behandlet af kortet, tilbagemeldes status '6900' eller '6F00'.

— Hvis længden (Le) overstiger antal bytes til rådighed eller hvis Le er nul, tilbagemeldes status '6Cxx', hvor 'xx' er det nøjagtige antal bytes til rådighed. I dette tilfælde er de behandlede data stadig til rådighed for en efterfølgende GET RESPONSE kommando.

— Hvis Le ikke er nul og er mindre end antal bytes til rådighed, bliver de ønskede data sendt på normal måde af kortet, og der tilbagemeldes status '61xx', hvor 'xx' er antal bytes, som stadig er til rådighed ved en efterfølgende GET RESPONSE kommando.

— Hvis kommandoen ikke understøttes (protokol T=1), tilbagemelder kortet '6D00'.

3.6.7. ***PSO: Verify Certificate***

Denne kommando overholder ISO/IEC 7816-8 men har begrænset anvendelse i forhold til den i normen definerede kommando.

VERIFY CERTIFICATE kommandoen anvendes af kortet til at hente en offentlig nøgle udefra og kontrollere dens gyldighed.

TCS_346 Når en VERIFY CERTIFICATE kommando giver resultat, bliver den offentlige nøgle gemt til fremtidig anvendelse i sikkerhedsmiljøet. Denne nøgle skal udtrykkelig være angivet til brug i sikkerhedsrelaterede kommandoer (INTERNAL AUTHENTICATE, EXTERNAL AUTHENTICATE eller VERIFY CERTIFICATE) af MSE-kommandoen (se punkt 3.6.10) med anvendelse af nøgleidentifikatoren.

TCS_347 I alle tilfælde anvender kommandoen VERIFY CERTIFICATE den offentlige nøgle, som tidligere er valgt af MSE-kommandoen til at åbne certifikatet. Denne offentlige nøgle skal tilhøre en medlemsstat eller EU.

TCS_348 Kommandomeddelelse

Byte	Længde	Værdi	Beskrivelse
CLA	1	'00h'	CLA
INS	1	'2Ah'	Udfør sikkerhedsoperation
P1	1	'00h'	P1
P2	1	'AEh'	P2: Ikke BER-TLV kodede data (sammenkædning af dataelementer)
Lc	1	'CEh'	Lc: Certifikatets længde, 194 bytes
#6-#199	194	'XX..XXh'	Certifikat: Sammenkædning af dataelementer (som beskrevet i tillæg 11)

TCS_349 Svarmeddelelse

Byte	Længde	Værdi	Beskrivelse
SW	2	'XXXXh'	Statusord (SW1, SW2)

— Giver kommandoen resultat, tilbagemelder kortet '9000'.

— Lykkes verifikationen af den kryptografiske kontrolsum ikke, tilbagemeldes behandlingsstatus '6688'. Verifikation og udpakning af certifikatet beskrives i tillæg 11.

— Hvis der ikke findes nogen offentlig nøgle i sikkerhedsmiljøet, tilbagemeldes '6A88'.

— Hvis den valgte offentlige nøgle (som benyttes til udpakning af certifikatet) anses for beskadiget, tilbagemeldes status '6400' eller '6581'.

— Hvis den valgte offentlige nøgle (som anvendes til at udpakke certifikatet) har en anden CHA.LSB (`CertificateHolderAuthorisation.equipmentType`) end '00' (dvs. ikke tilhører en EU-medlemsstat), tilbagemeldes status '6985'.

3.6.8. ***Internal Authenticate***

Denne kommando er i overensstemmelse med ISO/IEC 7816-4.

Med kommandoen INTERNAL AUTHENTICATE kan kortlæseren bekræfte kortets ægthed.

Ægthedsbekræftelsen er beskrevet i tillæg 11. Den indeholder følgende sætninger:

TCS_350 Kommandoen INTERNAL AUTHENTICATE anvender kortets private nøgle (som er valgt implicit) til signering af ægthedsdata, som indeholder K1 (første element i session nøgleoverensstemmelse) og RND1, og anvender den offentlige nøgle, der aktuelt er valgt (ved den seneste MSE-kommando), til at kryptere underskriften og udforme ægthedsbekræftelsestoken (nærmere detaljer i tillæg 11).

TCS_351 Kommandomeddelelse

Byte	Længde	Værdi	Beskrivelse
CLA	1	'00h'	CLA
INS	1	'88h'	INS
P1	1	'00h'	P1
P2	1	'00h'	P2
Lc	1	'10h'	Længde af data sendt til kortet
#6-#13	8	'XX..XXh'	Challenge anvendt til bekræftelse af kortets identitet
#14-#21	8	'XX..XXh'	VU.CHR (se tillæg 11)
Le	1	'80h'	Forventet længde af data fra kortet

TCS_352 Svarmeddelelse

Byte	Længde	Værdi	Beskrivelse
#1-#128	128	'XX..XXh'	Token for identifikation af kort (se tillæg 11)
SW	2	'XXXXh'	Statusord (SW1, SW2)

— Giver kommandoen resultat, tilbagemelder kortet '9000'.

— Findes ingen offentlig nøgle i sikkerhedsmiljøet, tilbagemeldes status '6A88'.

— Findes der ikke ingen privat nøgle i sikkerhedsmiljøet, tilbagemeldes status '6A88'.

— Hvis VU.CHR ikke svarer til navnet for den aktuelle offentlige nøgle, tilbagemeldes status '6A88'.

— Hvis den valgte private nøgle anses for beskadiget, tilbagemeldes status '6400' eller '6581'.

TCS_353 Hvis INTERNAL AUTHENTICATE kommandoen giver resultat, slettes den eventuelle nøgle for den aktuelle session og er ikke længere til rådighed. For at man kan få adgang til en ny sessionsnøgle, skal kommandoen EXTERNAL AUTHENTICATE gennemføres med resultat.

3.6.9. ***External Authenticate***

Denne kommando er i overensstemmelse med ISO/IEC 7816-4.

Med kommandoen EXTERNAL AUTHENTICATE kan kortet bekræfte identiteten af kortlæseren.

Identitetsbekræftelsen er beskrevet i tillæg 11. Den indeholder følgende sætninger:

TCS_354 En GET CHALLENGE kommando skal gå umiddelbart forud for EXTERNAL AUTHENTICATE kommandoen. Kortet afgiver en challenge (RND3).

TCS_355 Til verifikation af kryptogrammet anvendes RND3 (challenge afgivet af kortet), kortets private nøgle (valgt implicit) og den offentlige nøgle, som i forvejen er valgt med MSE-kommandoen.

TCS_356 Kortet verificerer kryptogrammet, og hvis det er korrekt, åbnes adgangsbetingelsen AUT.

TCS_357 Indgangskryptogrammet indeholder det andet element K2 til sessionsnøgleoverensstemmelse.

TCS_358 Kommandomeddelelse

Byte	Længde	Værdi	Beskrivelse
CLA	1	'00h'	CLA
INS	1	'82h'	INS
P1	1	'00h'	P1
P2	1	'00h'	P2 (den offentlige nøgle, som skal anvendes, kendes implicit og er i forvejen fastlagt ved MSE-kommandoen)
Lc	1	'80h'	Lc (Længde af data sendt til kortet)
#6-#133	128	'XX..XXh'	Kryptogram (se tillæg 11)

TCS_359 Svarmeddelelse

Byte	Længde	Værdi	Beskrivelse
SW	2	'XXXXh'	Statusord (SW1, SW2)

— Giver kommandoen resultat, tilbagemelder kortet '9000'.

— Findes der ingen offentlig nøgle i sikkerhedsmiljøet, tilbagemeldes '6A88'.

— Hvis CHA for den aktuelt fastsatte offentlige nøgle ikke er en sammenføjning af fartskriverapplikationens navn (AID) og en type køretøjsenhed, tilbagemeldes status '6F00' (se tillæg 11).

— Findes der ikke ingen privat nøgle i sikkerhedsmiljøet, tilbagemeldes status '6A88'.

— Lykkes verifikationen af den kryptografiske kontrolsum ikke, tilbagemeldes behandlingsstatus '6688'.

— Hvis denne kommando ikke følger umiddelbart efter en GET CHALLENGE kommando, tilbagemeldes status '6985'.

— Hvis den valgte private nøgle anses for beskadiget, tilbagemeldes status '6400' eller '6581'.

TCS_360 Hvis EXTERNAL AUTHENTICATE kommandoen ikke giver resultat, og hvis første del af sessionsnøglen er tilgængelig fra en vellykket nylig udført INTERNAL AUTHENTICATE, bliver sessionsnøglen til fremtidige kommandoer fastsat med sikker meddelelsesoverførsel.

TCS_361 Er sessionsnøglens første del ikke til rådighed fra en tidligere INTERNAL AUTHENTICATE kommando, bliver sessionsnøglens anden del, som sendes af kortlæseenheden, ikke gemt på kortet. Derved sikres, at den gensidige ægthedsbekræftelse finder sted i den rækkefølge, som foreskrives i tillæg 11.

3.6.10. ***Manage Security Environment***

Med denne kommando fastsættes en offentlig nøgle til brug for ægthedsbekræftelse.

Denne kommando er i overensstemmelse med ISO/IEC 7816-8. Brugen af denne kommando er begrænset med hensyn til den tilknyttede standard.

TCS_362 Den nøgle, der henvises til i MSE-datafeltet, er gyldig for enhver dedikeret fartskriverfil.

TCS_363 Den nøgle, der henvises til i MSE-datafeltet, er den aktuelle offentlige nøgle indtil næste korrekte MSE-kommando.

TCS_364 Hvis den nøgle, der henvises til, ikke (allerede) er tilstede på kortet, sker der ingen ændring i sikkerhedsmiljøet.

TCS_365 Kommandomeddelelse

Byte	Længde	Værdi	Beskrivelse
CLA	1	'00h'	CLA
INS	1	'22h'	INS
P1	1	'C1h'	P1: Den nøgle, der henvises til, er gyldig for alle kryptografiske operationer
P2	1	'B6h'	P2 (data, som der er henvist til vedrørende digital underskrift)
Lc	1	'0Ah'	Lc: Længde af efterfølgende datafelt
#6	1	'83h'	Etiket bestemt til henvisning til en offentlig nøgle i asymmetriske tilfælde
#7	1	'08h'	Længde af nøglehenvisning (nøgleidentifikator)
#8-#15	08h	'XX..XXh'	Nøgleidentifikator som foreskrevet i tillæg 11

TCS_366 Svarmeddelelse

Byte	Længde	Værdi	Beskrivelse
SW	2	'XXXXh'	Statusord (SW1, SW2)

— Giver kommandoen resultat, tilbagemelder kortet '9000'.

— Hvis den nøgle, der henvises til, ikke er tilstede på kortet, tilbagemeldes behandlingsstatus '6A88'.

— Hvis visse forventede dataobjekter ikke findes i sikkert meddelelsesformat, tilbagemeldes status '6987'. Dette kan være tilfældet, hvis etiketten '83h' mangler.

— Hvis nogle dataobjekter er ukorrekte, tilbagemeldes behandlingsstatus '6988'. Dette kan ske, hvis længden af nøgleidentifikatoren ikke er '08h'.

— Anses den valgte nøgle for beskadiget, tilbagemeldes status '6400' eller '6581'.

3.6.11. ***PSO: Hash***

Denne kommando anvendes til at overføre værdien af en hashberegning på visse data til kortet. Kommandoen bruges til verifikation af digitale underskrifter. Hash-værdien lagres i EEPROM til den efterfølgende kommando om verifikation af digital underskrift.

Denne kommando er i overensstemmelse med ISO/IEC 7816-8. Brugen af denne kommando er begrænset med hensyn til den tilknyttede standard.

TCS_367 Kommandomeddelelse

Byte	Længde	Værdi	Beskrivelse
CLA	1	'00h'	CLA
INS	1	'2Ah'	Udfør sikkerhedsoperation
P1	1	'90h'	Tilbagemeld hashkode
P2	1	'A0h'	Etiket: Datafeltet indeholder dataobjekter, som er relevante for hashing
Lc	1	'16h'	Længde Lc af det efterfølgende datafelt
#6	1	'90h'	Etiket til hashkode
#7	1	'14h'	Længde af hashkode
#8-#27	20	'XX..XXh'	Hashkode

TCS_368 Svarmeddelelse

Byte	Længde	Værdi	Beskrivelse
SW	2	'XXXXh'	Statusord (SW1, SW2)

— Giver kommandoen resultat, tilbagemelder kortet '9000'.

— Hvis nogle af de forventede dataobjekter (som ovenfor angivet) mangler, tilbagemeldes status '6987'. Dette kan ske, hvis en af etiketterne '90h' mangler.

— Hvis nogle dataobjekter er ukorrekte, tilbagemeldes behandlingsstatus '6988'. Denne fejl opstår, hvis den nødvendige etiket er tilstede, men dens længde er forskellig fra '14h'.

3.6.12. ***Perform Hash of File***

Denne kommando er ikke i overensstemmelse med ISO/IEC 7816-8. Klassebyten (CLA) i denne kommando angiver således, at der er en ophavsretligt beskyttet anvendelse af PERFORM SECURITY OPERATION/HASH.

TCS_369 Kommandoen PERFORM HASH OF FILE anvendes til hashing af dataområdet i den aktuelt valgte transparente elementærfil (EF).

TCS_370 Resultatet af hashoperationen gemmes på kortet. Derefter kan det benyttes til at sætte en digital underskrift på filen ved hjælp af kommandoen PSO: COMPUTE DIGITAL SIGNATURE. Dette resultat vil være til rådighed for kommandoen COMPUTE DIGITAL SIGNATURE indtil næste PERFORM HASH OF FILE kommando er gennemført med resultat.

TCS_371 Kommandomeddelelse

Byte	Længde	Værdi	Beskrivelse
CLA	1	'80h'	CLA
INS	1	'2Ah'	Udfør sikkerhedsoperation
P1	1	'90h'	Etiket: Hash
P2	1	'00h'	P2: Hash data i den aktuelt valgte transparente fil

TCS_372 Svarmeddelelse

Byte	Længde	Værdi	Beskrivelse
SW	2	'XXXXh'	Statusord (SW1, SW2)

— Giver kommandoen resultat, tilbagemelder kortet '9000'.

— Er ingen applikation valgt, tilbagemeldes behandlingsstatus '6986'.

— Anses den valgte elementærfil for beskadiget, tilbagemeldes status '6400' eller '6581'.

— Er den valgte fil ikke en transparent fil, tilbagemeldes status '6986'.

3.6.13. ***PSO: Compute Digital Signature***

Denne kommando anvendes til at beregne den digitale underskrift af en tidligere beregnet hashkode (se PERFORM HASH OF FILE, punkt 3.6.12).

Denne kommando er i overensstemmelse med ISO/IEC 7816-8. Brugen af denne kommando er begrænset med hensyn til den tilknyttede standard.

TCS_373 Kortets private nøgle anvendes til at beregne den digitale underskrift og kendes implicit af kortet.

TCS_374 Kortet udfører en digital underskrift med en udfyldningsmetode, som er i overensstemmelse med PKCS1 (se tillæg 11 for nærmere detaljer).

TCS_375 Kommandomeddelelse

Byte	Længde	Værdi	Beskrivelse
CLA	1	'00h'	CLA
INS	1	'2Ah'	Udfør sikkerhedsoperation
P1	1	'9Eh'	Digital underskrift, som skal tilbagemeldes
P2	1	'9Ah'	Etiket: Datafeltet indeholder data, som skal underskrives. Da der ikke indgår noget datafelt, formodes data allerede at være tilstede i kortet (hash af filen)
Le	1	'80h'	Længde af den forventede underskrift

TCS_376 Svarmeddelelse

Byte	Længde	Værdi	Beskrivelse
#1-#128	128	'XX..XXh'	Underskrift af den tidligere beregnede hash
SW	2	'XXXXh'	Statusord (SW1, SW2)

— Giver kommandoen resultat, tilbagemelder kortet '9000'.

— Hvis den implicit valgte private nøgle anses for beskadiget, tilbagemeldes status '6400' eller '6581'.

3.6.14. ***PSO: Verify Digital Signature***

Denne kommando anvendes til at verificere den digitale underskrift, som tilføres som inddata, i overensstemmelse med PKCS1 for en meddelelse, for hvilken hash kendes af kortet. Underskriftsalgoritmen kendes implicit af kortet.

Denne kommando er i overensstemmelse med ISO/IEC 7816-8. Brugen af denne kommando er begrænset med hensyn til den tilknyttede standard.

TCS_377 Kommandoen VERIFY DIGITAL SIGNATURE anvender altid samme offentlige nøgle, som er valgt af den forudgående MANAGE SECURITY ENVIRONMENT kommando, og den forudgående hashkode, som er indlæst med en PSO: HASH kommando.

TCS_378 Kommandomeddelelse

Byte	Længde	Værdi	Beskrivelse
CLA	1	'00h'	CLA
INS	1	'2Ah'	Udfør sikkerhedsoperation
P1	1	'00h'	
P2	1	'A8h'	Etiket: Datafeltet indeholder dataobjekter relevante for verifikation
Lc	1	'83h'	Længde Lc af det efterfølgende datafelt
#28	1	'9Eh'	Etiket for digital underskrift
#29-#30	2	'8180h'	Længde af digital underskrift (128 bytes, kodet i overensstemmelse med ISO/IEC 7816-6)
#31-#158	128	'XX..XXh'	Indhold af digital underskrift

TCS_379 Svarmeddelelse

Byte	Længde	Værdi	Beskrivelse
SW	2	'XXXXh'	Statusord (SW1, SW2)

— Giver kommandoen resultat, tilbagemelder kortet '9000'.

— Lykkes verifikationen af underskriften ikke, tilbagemeldes behandlingsstatus '6688'. Verifikationsprocessen er beskrevet i tillæg 11.

— Hvis der ikke er valgt nogen offentlig nøgle, tilbagemeldes status '6A88'.

— Hvis nogle af de forventede dataobjekter (som angivet ovenfor) mangler, tilbagemeldes status '6987'. Dette kan forekomme, hvis en af de ønskede etiketter mangler.

— Hvis der til behandling af kommandoen ikke er nogen hashkode til rådighed (som resultat af en forudgående PSO: HASH kommando), tilbagemeldes status '6985'.

— Hvis nogle dataobjekter er ukorrekte, tilbagemeldes behandlingsstatus '6988'. Dette kan forekomme, hvis længden af en af de ønskede etiketter er forkert.

— Hvis den valgte offentlige nøgle anses for beskadiget, tilbagemeldes status '6400' eller '6581'.

4. FARTSKRIVERKORTENES STRUKTUR

Dette afsnit angiver fartskriverkortenes filstruktur til lagring af tilgængelige data.

Det specificerer ikke producentafhængige interne strukturer i kortet som f.eks. startetiketter på filer eller lagring og behandling af dataelementer, som udelukkende behøves til intern brug, som f.eks. `EuropeanPublicKey, CardPrivateKey, TDesSessionKey eller WorkshopCardPin`.

Den effektive lagerplads på fartskriverkort skal være mindst 11 kbytes. Der kan anvendes større lagerplads. I så fald er kortets struktur den samme, men visse af elementerne i strukturen indeholder flere poster. Dette afsnit angiver mindste- og størsteværdier for antallet af sådanne poster.

4.1. **Førerkortets struktur**

TCS_400 Efter at førerkortet er personaliseret, skal det have følgende permanente filstruktur og filadgangsbetingelser:

Fil	Fil-ID	Adgangsbetingelser		
		Læse	Opdatere	Krypteret
MF	3F00			
├─EF ICC	0002	ALW	NEV	Nej
├─EF IC	0005	ALW	NEV	Nej
└─DF Tachograph	0500			
├─EF Application_Identification	0501	ALW	NEV	Nej
├─EF Card_Certificate	C100	ALW	NEV	Nej
├─EF CA_Certificate	C108	ALW	NEV	Nej
├─EF Identifikation	0520	ALW	NEV	Nej
├─EF Card download	050E	ALW	ALW	Nej
├─EF Driving_Licence_Info	0521	ALW	NEV	Nej
├─EF Events_Data	0502	ALW	PRO SM / AUT	Nej
├─EF Faults_Data	0503	ALW	PRO SM / AUT	Nej
├─EF Driver_Activity_Data	0504	ALW	PRO SM / AUT	Nej
├─EF Vehicles_Used	0505	ALW	PRO SM / AUT	Nej
├─EF Places	0506	ALW	PRO SM / AUT	Nej
├─EF Current_Usage	0507	ALW	PRO SM / AUT	Nej
├─EF Control_Activity_Data	0508	ALW	PRO SM / AUT	Nej
└─EF Specific_Conditions	0522	ALW	PRO SM / AUT	Nej

TCS_401 Alle elementærfilers strukturer skal være transparente.

TCS_402 Læsning med sikker meddelelsesoverførsel skal være mulig for alle filer under den dedikerede fartskriverfil (DF Tachograph).

TCS_403 Førerkortet skal have følgende datastruktur:

Fil / Dataelement	Antalposter	Størrelse (bytes) Min	Maks	Standardværdier
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*	
╠└Last card download		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 Følgende værdier, der er anvendt som størrelsesangivelser i ovenstående tabel, er mindste og største antal poster i førerkortets datastruktur:

		Min	Maks
n_1	NoOfEventsPerType	6	12
n_2	NoOfFaultsPerType	12	24
n_3	NoOfCardVehicleRecords	84	200
n_4	NoOfCardPlaceRecords	84	112
n_6	CardActivityLengthRange	5 544 bytes (28 døgn * 93 aktivitetsskift)	13 776 Bytes (28 døgn * 240 aktivitetsskift)

4.2. **Værkstedskortets struktur**

TCS_405 Efter at værkstedskortet er personaliseret, skal det have følgende permanente filstruktur og filadgangsbetingelser:

		Adgangsbetingelser		
Fil	Fil-ID	Læse	Opdatere	Krypteret
MF	3F00			
├─EF ICC	0002	ALW	NEV	Nej
├─EF IC	0005	ALW	NEV	Nej
└─Dedikeret fartskriverfil (DF Tachograph)	0500			
├─EF Application_Identification	0501	ALW	NEV	Nej
├─EF Card_Certificate	C100	ALW	NEV	Nej
├─EF CA_Certificate	C108	ALW	NEV	Nej
├─Identifikation af elementærfil	0520	ALW	NEV	Nej
├─EF Card_Download	0509	ALW	ALW	Nej
├─Kalibrering af elementærfil (EF)	050A	ALW	PRO SM / AUT	Nej
├─EF Sensor_Installation_Data	050B	ALW	NEV	Ja
├─EF Events_Data	0502	ALW	PRO SM / AUT	Nej
├─EF Faults_Data	0503	ALW	PRO SM / AUT	Nej
├─EF Driver_Activity_Data	0504	ALW	PRO SM / AUT	Nej
├─EF Vehicles_Used	0505	ALW	PRO SM / AUT	Nej
├─EF Places	0506	ALW	PRO SM / AUT	Nej
├─EF Current_Usage	0507	ALW	PRO SM / AUT	Nej
├─EF Control_Activity_Data	0508	ALW	PRO SM / AUT	Nej
└─EF Specific_Conditions	0522	ALW	PRO SM / AUT	Nej

TCS_406 Alle elementærfilers strukturer skal være transparente.

TCS_407 Læsning med sikker meddelelsesoverførsel skal være mulig for alle filer under den dedikerede fartskriverfil (DF Tachograph).

TCS_408 Værkstedskortet skal have følgende datastruktur:

Fil / Dataelement	Antal poster	Størrelse (Bytes) Min	Maks	Standardværdi
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}
╚═Dedikeret fartskriverfil (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}
╠═Identifikation af elementærfil (EF)		*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}
═Elementærfilposition		*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 Følgende værdier, der er anvendt som størrelsesangivelse i ovenstående tabel, er det mindste og største antal poster i værkstedskortets datastruktur:

		Min	Max
n_1	NoOfEventsPerType	3	3
n_2	NoOfFaultsPerType	6	6
n_3	NoOfCardVehicleRecords	4	8
n_4	NoOfCardPlaceRecords	6	8
n_5	NoOfCalibrationRecords	88	255
n_6	CardActivityLengthRange	198 bytes (1 døgn * 93 aktivitetsskift)	492 bytes (1 døgn * 240 aktivitetsskift)

4.3. **Kontrolkortets struktur**

TCS_410 Efter at kontrolkortet er personaliseret, skal det have følgende permanente filstruktur og filadgangsbetingelser:

		Adgangsbetingelser		
Fil	Fil-ID	Læse	Opdatere	Krypteret
MF	3F00			
├─EF ICC	0002	ALW	NEV	Nej
├─EF IC	0005	ALW	NEV	Nej
└─Dedikeret fartskriverfil (DF Tachograph)	0500			
├─EF Application_Identification	0501	ALW	NEV	Nej
├─EF Card_Certificate	C100	ALW	NEV	Nej
├─EF CA_Certificate	C108	ALW	NEV	Nej
├─EF Identification	0520	AUT	NEV	Nej
└─EF Controller_Activity_Data	050C	ALW	PRO SM / AUT	Nej

TCS_411 Alle elementærfilers strukturer skal være transparente.

TCS_412 Læsning med sikker meddelelsesoverførsel skal være mulig for alle filer under fartskriverens dedikerede fil.

TCS_413 Kontrolkortet skal have følgende datastruktur:

Fil / Dataelement	Antal poster	Størrelse (Bytes) Min	Maks	Standardværdi
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}
╠═Dedikeret fartskriverfil (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}
┃ ╠═Identifikation af elementærfil (EF)		*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 Følgende værdier, der er anvendt som størrelsesangivelser i ovenstående tabel, er det mindste og største antal poster i kontrolkortets datastruktur:

		Min	Maks
n_7	NoOfControlActivityRecords	230	520

4.4. **Virksomhedskortets struktur**

TCS_415 Efter at virksomhedskortet er personaliseret, skal det have følgende permanente filstruktur og filadgangsbetingelser:

		Adgangsbetingelser		
Fil	Fil-ID	Læse	Opdatere	Krypteret
MF	3F00			
├─EF ICC	0002	ALW	NEV	Nej
├─EF IC	0005	ALW	NEV	Nej
└─Dedikeret fartskriverfil (DF Tachograph)	0500			
├─EF Application_Identification	0501	ALW	NEV	Nej
├─EF Card_Certificate	C100	ALW	NEV	Nej
├─EF CA_Certificate	C108	ALW	NEV	Nej
├─EF Identification	0520	AUT	NEV	Nej
└─EF Company_Activity_Data	050D	ALW	PRO SM / AUT	Nej

TCS_416 Alle elementærfilers strukturer skal være transparente.

TCS_417 Læsning med sikker meddelelsesoverførsel skal være mulig for alle filer under den dedikerede fartskriverfil (DF Tachograph).

TCS_418 Virksomhedskortet skal have følgende datastruktur:

Fil / Dataelement	Antal poster	Størrelse (bytes) Min	Maks	Standardværdi
MF		*11147*	*24487*	
╠═Elementærfil, chipkort (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}
╠═Dedikeret fartskriverfil (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}
╠╠═Identifikation af elementærfil (EF)		*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}
╠╠├─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 Følgende værdier, der er anvendt som størrelsesangivelser i ovenstående tabel, er det mindste og største antal poster i virksomhedskortets datastruktur:

		Min	Maks
n_8	NoOfCompanyActivityRecords	230	520

Tillæg 3

PIKTOGRAMMER

PIC_001 Kontrolapparatet kan anvende følgende piktogrammer og kombinationer af piktogrammer:

1. BASISPIKTOGRAMMER

	Personer	**Handlinger**	**Funktionsmåder**
	Virksomhed		Virksomhedsmåde
	Tilsynsførende	Kontrol	Kontrolmåde
	Fører	Kørsel	Driftsmåde
	Værksted/prøvestation	Eftersyn/kalibrering	Kalibreringsmåde
	Fabrikant		

	Aktiviteter	**Varighed**
	Til rådighed	Aktuel rådighedsperiode
	Kørsel	Kontinuerlig køretid
	Hvile	Aktuel hvileperiode
	Arbejde	Aktuel arbejdsperiode
	Pause	Akkumuleret pausetid
?	Ukendt	

	Apparat	**Funktioner**
1	Førerkortplads	
2	Kortplads f. medchauffør	
	Kort	
	Ur	
	Skærm	Visning på skærm
	Overførsel til eksternt lager	Dataoverførsel
	Strømforsyning	
	Printer/udskrift	Udskrivning
	Føler	
	Dækstørrelse	
	Køretøj/køretøjsenhed	

	Særlige omstændigheder
OUT	Uden for gyldighedsområde
	Overfart med færge/tog

	Forskelligt
!	Hændelser
	Fejl
	Den daglige arbejdstids begyndelse
	Den daglige arbejdstids afslutning
	Sted
M	Manuel indlæsning af føreraktiviteter
	Sikkerhed
	Hastighed
	Tid
Σ	Total/sum

	Angivelse
24h	Dagligt
|	Ugentligt
||	Hver anden uge
+	Fra eller til

2. KOMBINATIONER AF PIKTOGRAMMER

	Forskelligt
	Kontrolsted
	Sted hvor den daglige arbejdstid begynder
	Sted hvor den daglige arbejdstid slutter
	Fra tidspunkt
	Til tidspunkt
	Fra køretøj
OUT+	Uden for gyldighedsområde (start)
+OUT	Uden for gyldighedsområde (slut)

	Kort
	Førerkort
	Virksomhedskort
	Kontrolkort
	Værkstedskort
– – –	Intet kort

	Kørsel
	Førerholdkørsel
|	Køretid for én uge
||	Køretid for to uger

	Udskrift
24h	Daglig udskrift af føreraktivitet fra kort
24h	Daglig udskrift af føreraktivitet fra køretøjsenhed
! ×	Udskrift af hændelser og fejl fra kort
! ×	Udskrift af hændelser og fejl fra køretøjsenhed
	Udskrift af tekniske data
>>	Udskrift af overskridelse af tilladt hastighed

	Hændelser
!	Isætning af ugyldigt kort
!|	Kortkonflikt
!	Tidsoverlapning
!	Kørsel uden behørigt kort
!	Isætning af kort under kørslen
!	Seneste kortsession ikke korrekt afsluttet
>>	Overskridelse af tilladt hastighed
! ÷	Svigt af strømforsyningen
!	Fejl ved køredata
!	Sikkerhedsbrud
!	Justering af klokkeslæt (foretaget af værksted)
>	Kontrol af overskridelse af tilladt hastighed

Fejl

	Kortfejl (førerkortplads)
	Kortfejl (medchaufførs kortplads)
	Displayfejl
	Dataoverførselsfejl
	Printerfejl
	Følerfejl
	Intern fejl i køretøjsenhed

Manuel indlæsning

	Stadig samme daglige arbejdstid ?
	Slut på foregående arbejdsperiode ?
	Bekræft eller indlæs sted hvor daglig arbejdsperiode slutter
	Indlæs starttidspunkt
	Indlæs sted hvor daglig arbejdsperiode begynder

Bemærkning: Andre kombinationer af piktogrammer, som danner en udskrivningsgruppe eller datanavne for poster, er givet i tillæg 4.

Tillæg 4

UDSKRIFTER

1. GENERELT

Hver udskrift er opbygget ved kædning af forskellige datagrupper, om muligt identificeret med en gruppeidentifikator.

En datagruppe indeholder en eller flere poster, eventuelt identificeret ved en postidentifikator.

PRT_001 Når en gruppeidentifikator står umiddelbart foran en postidentifikator, bliver postidentifikatoren ikke udskrevet.

PRT_002 Når et dataelement er ukendt eller ikke må udskrives af grunde vedrørende dataadgang, udskrives mellemrum i stedet.

PRT_003 Hvis indholdet af en hel linje er ukendt eller ikke behøver udskrives, udelades hele linjen.

PRT_004 Numeriske datafelter udskrives højrejusteret, med mellemrum som skilletegn for tusinder og millioner, og uden foranstillede nuller.

PRT_005 Strengdatafelter udskrives venstrejusteret og udfyldt med mellemrum til dataelementets længde eller om nødvendigt afkortet til dataelementets længde (navn og adresse).

2. SPECIFIKATION AF DATAGRUPPER

I dette kapitel er anvendt følgende notationsregler for format:

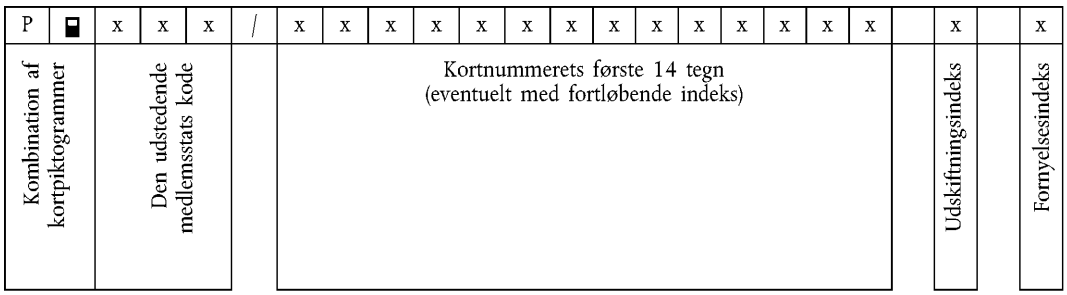
— tegn med **fede typer** angiver almindelig tekst, som skal udskrives (udskrives med normale tegn),

— normale typer angiver variable (piktogrammer eller data) som ved udskrivning skal erstattes med deres værdi,

— variabelnavne er omgivet af understregningstegn for at angive den længde, som dataelementer for den pågældende variabel kan have,

— datoer angives i formatet »dd/mm/yyyy« (dag, måned, år). Der kan også anvendes formatet »dd.mm.yyyy«,

— betegnelsen »kortidentifikation« angiver sammensætningen af: Kortets type gennem en kombination af kortpiktogrammer, den kortudstedende medlemsstats kode, en normal skråstreg og kortets nummer med udskiftningsindekset og fornyelsesindekset adskilt af et mellemrum:



PRT_006 Udskrifter skal anvende følgende datablokke og/eller dataposter i overensstemmelse med følgende betydninger og formater:

Datagruppe- eller postnummer Betydning	Dataformat
1 **Dato og tidspunkt for udskrivning af dokumentet**	dd/mm/yyyy hh:mm **(UTC)**

2 **Udskriftens art**

Datagruppeidentifikator

Piktogramkombination i udskrift (se tillæg 3) Hastighedsbegrænserens indstilling (kun ved udskrivning af overskridelser af tilladt hastighed)

```
----------T ------------
Picto xxx km/h
```

3 **Identifikation af kortindehaver**

Datagruppeidentifikator. P = piktogram for personer

Kortindehaverens efternavn

Kortindehaverens eventuelle fornavn(e)

Identifikation af kort

Eventuel udløbsdato for kortet

Er kortet ikke et personligt kort og ikke påført kortindehaverens efternavn, skal i stedet udskrives virksomhedens, værkstedets eller kontrolorganets navn.

```
----------P-------------
P Last_Name _____________
  First_Name _____________
Card_Identification _______
  dd/mm/yyyy
```

4 **Identifikation af køretøjet**

Datagruppeidentifikator

VIN

Registrerende medlemsstat og køretøjets indregistreringsnummer

```
------------A -----------
A VIN ____________________
  Nat/VRN ________________
```

5 **Identifikation af køretøjsenhed**

Datagruppeidentifikator

Køretøjsfabrikantens navn

Reservedelsnummer for køretøjsenhed

```
------------B-----------
B VU_Manufacturer _________
  VU_Part_Number __________
```

6 **Seneste kalibrering af kontrolapparatet**

Datagruppeidentifikator

Værkstedets navn

Identifikation af værkstedskort

Dato for kalibreringen

```
------------T-----------
T Last_Name _____________
Card_Identification _______
T  dd/mm/yyyy
```

7 **Seneste kontrol (ved en tilsynsførende)**

Datagruppeidentifikator

Idenfikation af tilsynsførendes kort

Kontroldato, -klokkeslæt og -art

Kontrollens art: Indtil fire piktogrammer. Kontrollens art kan være følgende eller en kombination deraf:

: Dataoverførsel, kort, : Dataoverførsel, køretøjsenhed, : Udprintning, : Visning på skærm

```
------------C-----------
Card_Identification _______
C  dd/mm/yyyy hh:mm pppp
```

8 **Føreraktiviteter, gemt på kortet, i kronologisk rækkefølge**

Datagruppeidentifikator

Forespørgselsdato (kalenderdag omfattet af udskriften) + tæller for daglig tilstedeværelse

```
------------D-----------
        dd/mm/yyyy xxx
```

8.1 *Periode hvor kortet ikke var isat*

8.1a Postidentifikator (periodens start)

8.1b *Ukendt periode*. Start- og sluttid, varighed

8.1c *Aktivitet indlæst manuelt*

Aktivitetspiktogram, start- og sluttid (inkl.), varighed, hvileperioder à mindst én time er markeret med en stjerne.

```
   --------------------
?  hh:mm hh:mm hhhmm
A  hh:mm hh:mm hhhmm          *
```

8.2 *Indsættelse af kort I kortplads S*

Postidentifikator; S = Kortpladspiktogram
Registrerende medlemsstat og køretøjets indregistreringsnummer
Køretøjets kilometerstand ved isætning af kortet

```
----------S----------
Nat/VRN _______________
x xxx xxx km
```

8.3 *Aktivitet (mens kortet var isat)*

Aktivitetspiktogram, start- og sluttid (inkl.), varighed, førerholdstatus (førerholdspiktogram hvis FØRERHOLD, blanke hvis ÉN FØRER) samt hvileperioder på mindst én time er markeret med en stjerne.

```
A hh:mm hh:mm hhhmm ⊙⊙      *
```

8.3a *Særlig omstændighed.* Indlæsningstidpunkt, piktogram (eller piktogramkombination) for særlige omstændigheder.

```
hh:mm ----- pppp -----
```

8.4 *Udtagning af kort*

Køretøjets kilometerstand og tilbagelagt distance siden sidste isætning ved kendt kilometerstand.

```
x xxx xxx km; x xxx km
```

9 **Føreraktiviteter, lagret i køretøjsenheden for hver kortplads i kronologisk rækkefølge**

Datagruppeidentifikator
Forespørgselsdato (kalenderdag, som udskriften omhandler)
Køretøjets kilometerstand ved kl. 00:00 og 24:00

```
-----------⊙-----------
        dd/mm/yyyy
x xxx xxx - x xxx xxx km
```

10 **Aktiviteter, som er registreret i kortplads S**

Datagruppeidentifikator

```
---------- S ----------
```

10.1 *Periode, hvor der ikke har været isat et kort i kortplads S*

Postidentifikator
Intet kort isat
Køretøjets kilometerstand ved periodens begyndelse

```
--------------------
⊙ ---
x xxx xxx km
```

10.2 *Isætning af kort*

Postidentifikator for isætning af kort
Førers navn
Førers fornavn
Identifikation af førerkort
Førerkortets udløbsdato
Registrerende medlemsstat og indregisteringsnummer for det foregående køretøj, som er anvendt
Dato og klokkeslæt for udtagning af kortet af det foregående køretøj
Tom linje
Køretøjets kilometerstand ved isætning af kortet, manuel indlæsning af flag for føreraktivetet (M for ja, blank for nej).

```
--------------------
⊙ 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, start- og sluttid (inkl.), varighed, førerstatus (førerholdspiktogram hvis FØRERHOLD, blanke hvis ÉN FØRER), hvileperioder på mindst én time er markeret med en stjerne.

```
A hh:mm hh:mm hhhmm ⊙⊙      *
```

10.3a *Særlig omstændighed.* Indlæsningstidpunkt, piktogram (eller piktogramkombination) for særlige omstændigheder.

```
hh:mm ----- pppp -----
```

10.4 *Udtagning af kort, eller slutning på »intet kort« periode*

Køretøjets kilometerstand ved udtagning af kortet eller ved slutningen af »intet kort« perioden, og tilbagelagt distance siden isætning eller siden »intet kort« periodens begyndelse.

```
x xxx xxx km; x xxx km
```

11 **Døgnsammenfatning**

Datagruppeidentifikator

```
----------Σ---------
```

11.1 **Køretøjsenhedens oversigt over perioder uden kort i førerens kortplads**

Datagruppeidentifikator

```
10■---
```

11.2 **Køretøjsenhedens oversigt over perioder uden kort i medchaufførens kortplads**

Datagruppeidentifikator

```
20■---
```

11.3 **Køretøjsenhedens døgnoversigt for hver fører**

Postidentifikator
Førers efternavn
Førers fornavn(e)
Identifikation af førerkort

```
  --------------------
0 Last_Name ________________
  First_Name ________________
Card_Identification _______
```

11.4 *Indlæsning af sted, hvor daglig arbejdstid begynder og/eller slutter*

pi = piktogram for sted begynder/slutter, tidspunkt, stat, region,
Kilometerstand

```
pihh:mm  Cou  Reg
  x xxx  xxx  km
```

11.5 *Totalværdier for aktivitet (fra et kort)*

Total varighed af kørsel, tilbagelangt distance
Total varighed af arbejde og rådighed
Total varighed af hvile og ukendt
Total varighed af førerholdsaktiviteter

```
  0 hhhmm x xxx km
  ⚒ hhhmm ◘ hhhmm
  ⊢ hhhmm ? hhhmm
00 hhhmm
```

11.6 *Totalværdier for aktivitet (perioder uden kort i førerens kortplads)*

Total varighed af kørsel, tilbagelangt distance
Total varighed af arbejde og rådighed
Total varighed af hvile

```
  0 hhhmm x xxx km
  ⚒ hhhmm ◘ hhhmm
  ⊢ hhhmm
```

11.7 *Totalværdier for aktivitet (perioder uden kort i medchaufførens kortplads)*

Total varighed af arbejde og rådighed
Total varighed af hvile

```
  ⚒ hhhmm ◘ hhhmm
  ⊢ hhhmm
```

11.8 *Totalværdier for aktivitet (pr. chauffør, begge kortpladser medregnet)*

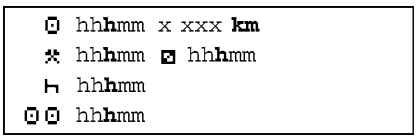
Total varighed af kørsel, tilbagelangt distance

Total varighed af arbejde og rådighed

Total varighed af hvile

Total varighed af førerholdsaktiviteter

Når der kræves daglig udskrift for det aktuelle døgn, beregnes daglig sammenfatning med de data, der foreligger på udprintningstidspunktet.



12 **Hændelser og/eller fejl, som er gemt på et kort**

12.1 Datagruppeidentifikator for seneste 5 »hændelser og fejl« fra et kort

12.2 Datagruppeidentifikator for alle registrerede »hændelser« på et kort

12.3 Datagruppeidentifikator for alle registrerede »fejl« på et kort

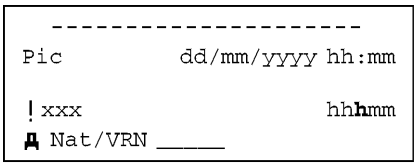
12.4 *Post vedrørende hændelser og/eller fejl*

Postidentifikator

Piktogram for hændelser/fejl, postens formål, startdato og -klokkeslæt

Eventuel supplerende fejl-/hændelseskode, varighed

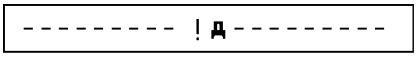
Registrerende medlemsstat og registreringsnummer for det køretøj, hvor hændelsen eller fejlen optrådte.



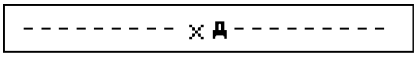
13 **Hændelser og/eller fejl, som er gemt eller er igangværende på en køretøjsenhed**

13.1 Datagruppeidentifikator for seneste 5 »hændelser og fejl« fra køretøjsenheden

13.2 Datagruppeidentifikator for alle registrerede eller igangværende »hændelser« på en køretøjsenhed



13.3 Datagruppeidentifikator for alle registrerede eller igangværende »fejl« på en køretøjsenhed



13.4 *Post vedrørende hændelser og/eller fejl*

Postidentifikator

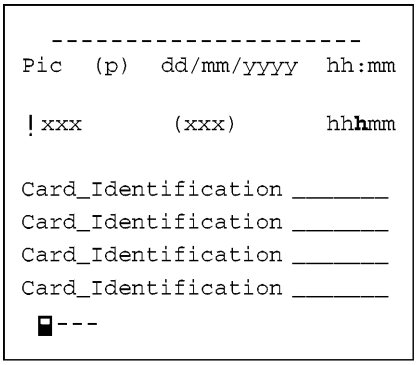
Piktogram for hændelser/fejl, postens formål, startdato og -klokkeslæt

Eventuel supplerende fejl-/hændelseskode, antal tilsvarende hændelser det pågældende døgn, varighed

Identifikation af de kort, der er indsat ved begyndelsen eller enden på hændelsen eller fejlen (indtil 4 linjer uden to gentagelser af de samme kortnumre)

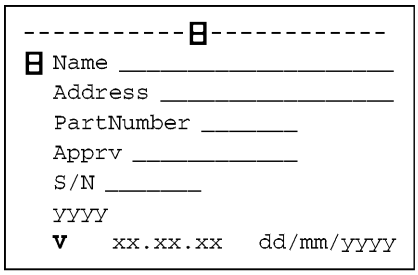
Tilfælde hvor intet kort var isat

Postens formål (p) er en numerisk kode, som forklarer, hvorfor hændelsen eller fejlen blev registreret, kodet i henhold til dataelementets `EventFaultRecordPurpose`.



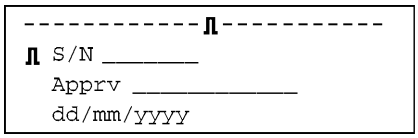
14 **Identifikation af køretøjsenhed**

Datagruppeidentifikator
Navn på køretøjsenhedens fabrikant
Adresse på køretøjsenhedens fabrikant
Reservedelsnummer for køretøjsenhed
Godkendelsesnummer på køretøjsenhed
Serienummer på køretøjsenhed
Fabrikationsår på køretøjsenheden
Version og installationsdato for køretøjsenhedens programmel



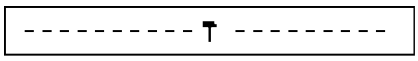
15 **Identifikation af føler**

Datagruppeidentifikator
Serienummer på føler
Godkendelsesnummer på føler
Dato for første montering af føleren



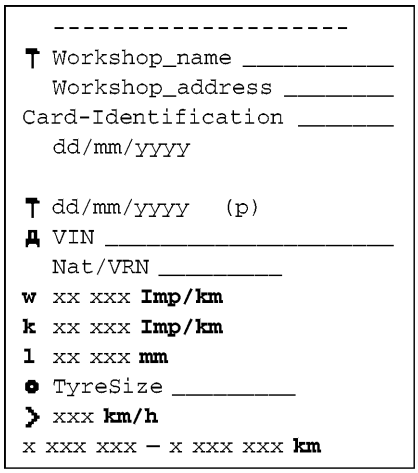
16 **Kalibreringsdata**

Datagruppeidentifikator



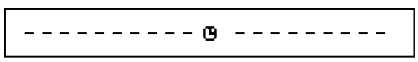
16.1 *Kalibreringspost*

Postidentifikator
Værksted, som har udført kalibreringen
Værkstedets adresse
Identifikation af værkstedskort
Værkstedskortets udløbsdato
Tom linje
Kalibreringsdato + kalibreringens formål
VIN
Registrerende medlemsstat og køretøjets indregistreringsnummer
Køretøjets vejdrejetal
Kontrolapparatets konstant
Køretøjets effektive hjulperiferi
Størrelse på de monterede dæk
Indstilling af hastighedsbegrænser
Gammel og ny kilometerstand
Kalibreringens formål (p) er en numerisk kode, som forklarer, hvorfor disse kalibreringsparametre blev registreret, kodet i henhold til dataelementet `Calibration-Purpose`.



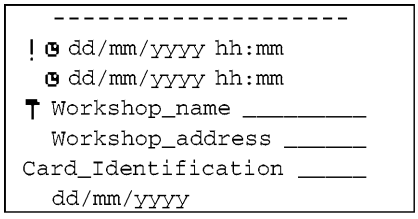
17 **Tidsjustering**

Datagruppeidentifikator



17.1 *Tidsjusteringspost*

Postidentifikator
Gammel dato og gammelt klokkeslæt
Ny dato og nyt klokkeslæt
Værksted, som har udført tidsjusteringen
Værkstedets adresse
Identifikation af værkstedskort
Værkstedskortets udløbsdato



18 **Den seneste hændelse og fejl, som er registreret i køretøjsenheden**

Datagruppeidentifikator
Dato og klokkeslæt for seneste hændelse
Dato og klokkeslæt for seneste fejl

```
---------- !✕🖷----------
!  jj/mm/yyyy  hh:mm
✕  jj/mm/yyyy  hh:mm
```

19 **Information vedrørende overskridelse af tilladt hastighed**

Datagruppeidentifikator
Dato og klokkeslæt for seneste KONTROL MED OVERSKRIDELSE AF TILLADT HASTIGHED
Dato og klokkeslæt for første overskridelse af tilladt hastighed og antal hændelser med overskridelse af tilladt hastighed siden da

```
-----------›› ----------
›▯ dd/mm/yyyy  hh:mm
›› dd/mm/yyyy  hh:mm (nnn)
```

20 **Post vedrørende overskridelser af tilladt hastighed**

20.1 Datagruppeidentifikator »første overskridelse af tilladt hastighed efter seneste kalibrering«

```
-------- ››T --------
```

20.2 Datagruppeidentifikator for »de 5 alvorligste inden for de sidste 365 dage«

```
------- ››(365)-------
```

20.3 Datagruppeidentifikator for »den alvorligste for hver af de 10 seneste dage, den er forekommet«

```
------- ››(10) -------
```

20.4 Postidentifikator
Dato, klokkeslæt og varighed
Maksimum- og gennemsnitshastighed, antal tilsvarende hændelser det pågældende døgn
Førers efternavn
Førers fornavn(e)
Identifikation af førerkort

```
   ------------------
›› dd/mm/yyyy hh:mm hhhmm
   xxx km/h xxx km/h (xxx)
▯  Last_Name _____________
   First_Name _____________
Card_Identification _______
```

20.5 Hvis der inden for en datagruppe ikke er nogen post vedrørende overskridelse af tilladt hastighed

```
›› - - -
```

21 **Håndskrevne oplysninger**

Datagruppeidentifikator
21.1 Kontrolsted
21.2 Den tilsynsførendes underskrift
21.3 Fra tidspunkt
21.4 Til tidspunkt
21.5 Førers' underskrift:
»Håndskrevne oplysninger«: Indsæt så mange blanke linjer over et håndskrevet punkt, at de ønskede oplysninger faktisk kan skrives eller der kan påføres en underskrift.

```
------------------------
▯● .....
▯  .....
◷+ .....
+◷ .....
▯  .....
```

3. SPECIFIKATION AF UDSKRIFTER

I dette kapitel er anvendt følgende notationsregler for format:

N	Udskriv datagruppe- eller postantal N
N	Udskriv datagruppe- eller postantal N, gentaget så mange gange som nødvendigt
X/Y	Udskriv datagruppe eller post X og/eller Y efter behov, gentaget som mange gange som nødvendigt.

3.1. **Daglig udskrift af føreraktivitet fra kort**

PRT_007 Daglig udskrift af føreraktivitet fra kort skal overholde følgende format:

1	Dato og tidspunkt for udskrivning af dokumentet
2	Udskriftens art
3	Identifikation af den tilsynsførende (hvis der er isat et kontrolkort i køretøjsenheden)
3	Identifikation af føreren (fra det kort, der er omfattet af udskriften)
4	Identifikation af køretøj (det køretøj, hvorfra udskriften tages)
5	Identifikation af køretøjsenhed (den køretøjsenhed, hvorfra udskriften tages)
6	Seneste kalibrering af denne køretøjsenhed
7	Seneste kontrol, som den kontrollerede fører har været genstand for
8	Skilletegn for føreraktiviteter
8.1a / 8.1b / 8.1c / 8.2 / 8.3 / 8.3a / 8.4	Føreraktiviteter i kronologisk orden
11	Skilletegn for døgnoversigt
11.4	Indlæste steder i kronologisk rækkefølge
11.5	Aktivitet, totalværdier
12.1	Hændelser eller fejl fra skilletegn for kort
12.4	Poster med hændelser/fejl (seneste 5 hændelser eller fejl, som er gemt på kortet)
13.1	Hændelser eller fejl fra skilletegn for køretøjsenhed
13.4	Poster med hændelser/fejl (seneste 5 hændelser eller fejl, som er gemt eller igangværende på køretøjsenheden)
21.1	Kontrolsted
21.2	Den tilsynsførendes underskrift
21.5	Førers underskrift

3.2. **Daglig udskrift af føreraktivitet fra køretøjsenhed**

PRT_008 Daglig udskrift af føreraktivitet fra køretøjsenhed skal overholde følgende format:

1	Dato og tidspunkt for udskrivning af dokumentet
2	Udskriftens art
3	Identifikation af kortindehaver (for alle kort isat i køretøjsenhed)
4	Identifikation af køretøj (det køretøj, hvorfra udskriften tages)
5	Identifikation af køretøjsenhed (den køretøjsenhed, hvorfra udskriften tages)
6	Seneste kalibrering af denne køretøjsenhed
7	Seneste kontrol på dette kontrolapparat
9	Skilletegn for føreraktiviteter
10	Skilletegn for førerkortplads (kortplads 1)
10.1 / 10.2 / 10.3 /10.3a / 10.4	Aktiviteter i kronologisk rækkefølge (førerkortplads)
10	Skilletegn for førerkortplads (kortplads 2)
10.1 / 10.2 / 10.3 /10.3a / 10.4	Aktiviteter i kronologisk rækkefølge (medchaufførens kortplads)
11	Skilletegn for døgnsammenfatning
11.1	Oversigt over perioder uden kort i førerens kortplads
11.4	Indlæste steder i kronologisk rækkefølge
11.6	Aktivitet, totalværdier

11.2	Oversigt over perioder uden kort i medchaufførens kortplads
11.4	Indlæste steder i kronologisk rækkefølge
11.7	Aktivitet, totalværdier
11.3	Oversigt over føreraktiviteter, begge kortpladser medregnet
11.4	Steder indlæst af denne fører i kronologisk rækkefølge
11.7	Aktiviteter total for denne fører
13.1	Skilletegn for fejl
13.4	Poster med hændelser/fejl (seneste 5 hændelser eller fejl, som er gemt eller igangværende på køretøjsenheden)
21.1	Kontrolsted
21.2	Den tilsynsførendes underskrift
21.3	Fra tidspunkt (plads til rådighed for en fører uden kort til angivelse af de relevante perioder)
21.4	Til tidspunkt
21.5	Førers underskrift

3.3. **Udskrift af hændelser og fejl fra kort**

PRT_009 Udskrift af hændelser og fejl fra kort skal overholde følgende format:

1	Dato og tidspunkt for udskrivning af dokumentet
2	Udskriftens art
3	Identifikation af den tilsynsførende (hvis et kontrolkort er isat i køretøjsenheden)
3	Identifikation af føreren (fra det kort, der er omfattet af udskriften)
4	Identifikation af køretøj (det køretøj, hvorfra udskriften tages)
12.2	Skilletegn for hændelser
12.4	Hændelsesposter (alle hændelser gemt på kortet)
12.3	Skilletegn for fejl
12.4	Poster vedrørende fejl (alle fejl gemt på kortet)
21.1	Kontrolsted
21.2	Den tilsynsførendes underskrift
21.5	Førers underskrift

3.4. **Udskrift af hændelser og fejl fra køretøjsenhed**

PRT_010 Udskrift af hændelser og fejl fra køretøjsenhed skal overholde følgende format:

1	Dato og tidspunkt for udskrivning af dokumentet
2	Udskriftens art
3	Identifikation af kortindehaver (for alle kort isat i køretøjsenhed)
4	Identifikation af køretøj (det køretøj, hvorfra udskriften tages)
13.2	Skilletegn for hændelser
13.4	Hændelsesposter (alle hændelser, som er gemt eller igangværende på køretøjsenheden)
13.3	Skilletegn for fejl
13.4	Poster vedrørende fejl (alle fejl, som er gemt eller igangværende på køretøjsenheden)
21.1	Kontrolsted
21.2	Den tilsynsførendes underskrift
21.5	Førers underskrift

3.5. **Udskrift af tekniske data**

PRT_011 Udskrift af tekniske data skal overholde følgende format:

1	Dato og tidspunkt for udskrivning af dokumentet
2	Udskriftens art
3	Identifikation af kortindehaver (for alle kort isat i køretøjsenhed)
4	Identifikation af køretøj (det køretøj, hvorfra udskriften tages)
14	Identifikation af køretøjsenhed
15	Identifikation af føler
16	Skilletegn for kalibreringsdata
16.1	Kalibreringsposter (alle foreliggende poster i kronologisk rækkefølge)
17	Skilletegn for tidsjustering
17.1	Poster vedrørende tidsjustering (alle poster, som er til rådighed fra tidsjustering og fra kalibreringsdataposter)
18	Den seneste hændelse og fejl, som er registreret i køretøjsenheden

3.6. **Udskrift af overskridelser af tilladt hastighed**

PRT_012 Udskrift af overskridelser af tilladt hastighed skal overholde følgende format:

1	Dato og tidspunkt for udskrivning af dokumentet
2	Udskriftens art
3	Identifikation af kortindehaver (for alle kort isat i køretøjsenhed)
4	Identifikation af køretøj (det køretøj, hvorfra udskriften tages)
19	Information vedrørende overskridelse af tilladt hastighed
20.1	Identifikator for data vedrørende overskridelser af tilladt hastighed
20.4 / 20.5	Første overskridelse af tilladt hastighed efter seneste kalibrering
20.2	Identifikator for data vedrørende overskridelser af tilladt hastighed
20.4 / 20.5	De 5 alvorligste hændelser med overskridelse af tilladt hastighed inden for de sidste 365 dage
20.3	Identifikator for data vedrørende overskridelser af tilladt hastighed
20.4 / 20.5	Den alvorligste hændelse vedrørende overskridelse af tilladt hastighed for hver af de 10 seneste dage, den er forekommet
21.1	Kontrolsted
21.2	Den tilsynsførendes underskrift
21.5	Førers underskrift

Tillæg 5

SKÆRMBILLEDE

I dette tillæg er anvendt følgende notationsregler for format:

— tegn med **fede typer** angiver almindelig tekst, som vises (vises på skærmen med normale typer),

— normale typer angiver variable (piktogrammer eller data) som på skærmen skal erstattes med deres værdi:

dd mm yyyy: dag, måned, år,

hh: timer,

mm: minutter,

D: varighedspiktogram,

EF: kombination af piktogrammer for begivenheder eller fejl,

O: piktogram for funktionsmåde.

DIS_001 Kontrolapparatet skal på skærmen vise data i følgende formater:

Data	Format
Standardskærmbillede	
Lokal tid	hh:mm
Funktionsmåde	O
Oplysninger vedrørende fører	1 D**h**h**h**mm ▮▮**h**h**h**mm
Oplysninger vedrørende medchauffør	2 D**h**h**h**mm
Omstændigheden »uden for område« åbnet	OUT
Visning af advarsel	
Overskridelse af sammenhængende køretid	1 O **h**h**h**mm ▮▮**h**h**h**mm
Hændelse eller fejl	EF
Andre skærmbilleder	
UTC-dato Klokkeslæt	**UTC** dd/mm/yyyy or **UTC** dd/mm/yyyy hh:mm
Førers sammenhængende køretid og akkumulerede pausetid	1 O **h**h**h**mm ▮▮**h**h**h**mm
Medchaufførs sammenhængende køretid og akkumulerede pausetid	2 O **h**h**h**mm ▮▮**h**h**h**mm
Førers akkumulerede køretid for den foregående og den aktuelle uge	1 O ‖ **h**h**h**mm
Medchaufførs akkumulerede køretid for den foregående og den aktuelle uge	2 O ‖ **h**h**h**mm

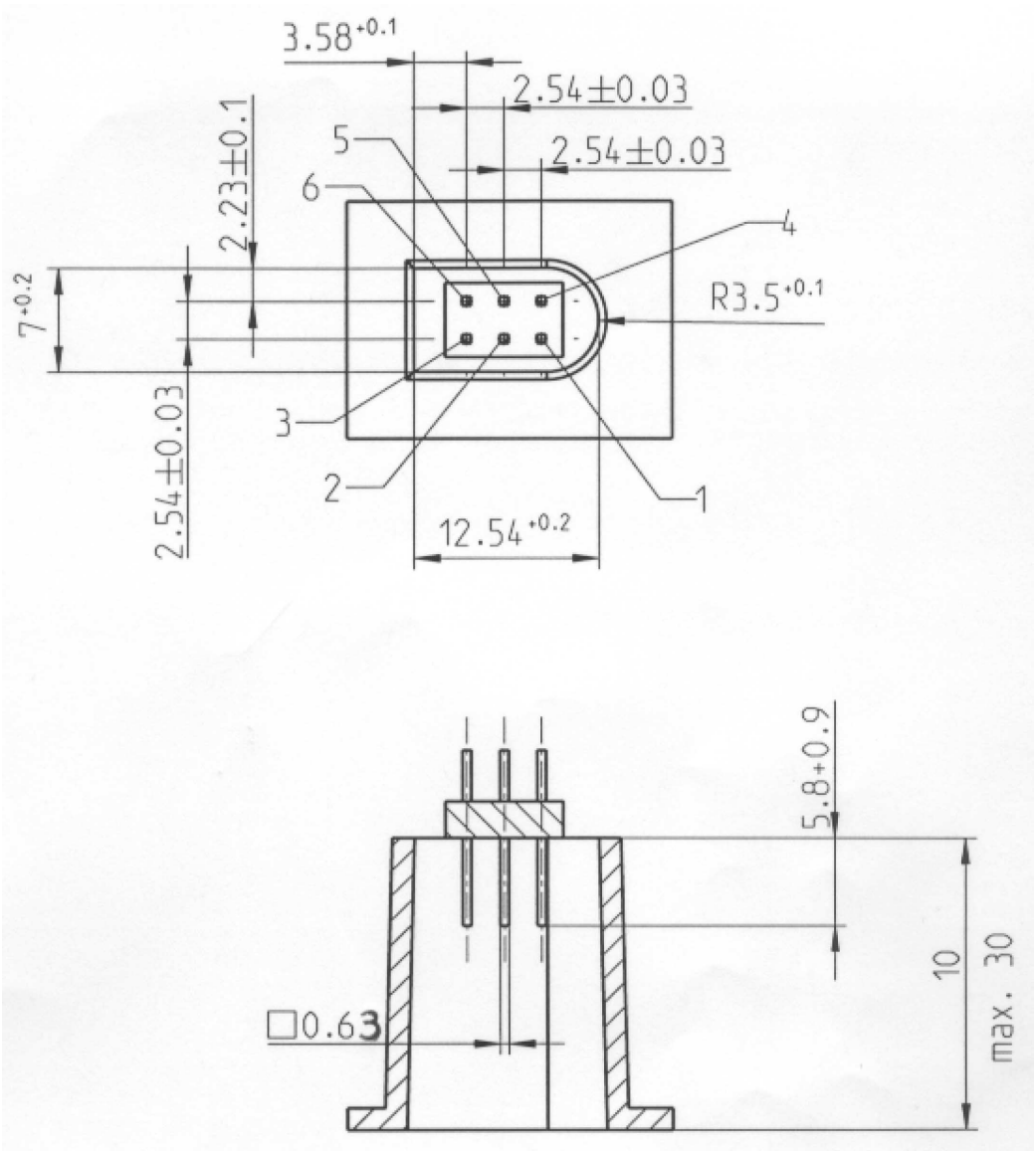
Tillæg 6

EKSTERNE GRÆNSEFLADER

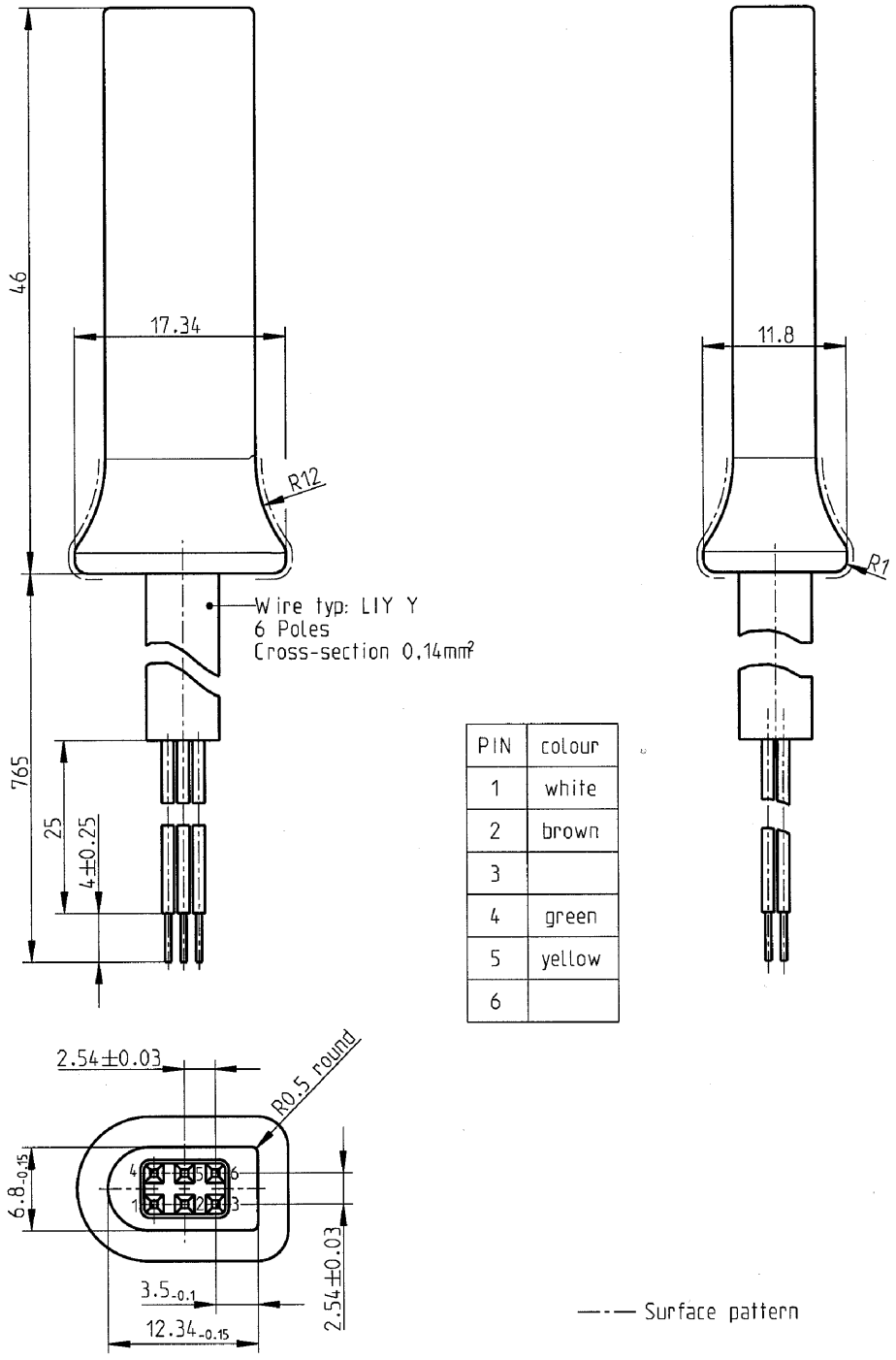
1. HARDWARE

1.1. **Tilslutningsstik**

INT_001 Stikket til dataoverførsel/kalibrering skal være 6-benet, skal være tilgængeligt fra frontpanelet, uden at nogen del af kontrolapparatet behøver adskilles, og skal være i overensstemmelse med følgende tegning (alle mål i mm):



Følgende diagram viser et typisk 6-benet stik:



PIN	colour
1	white
2	brown
3	
4	green
5	yellow
6	

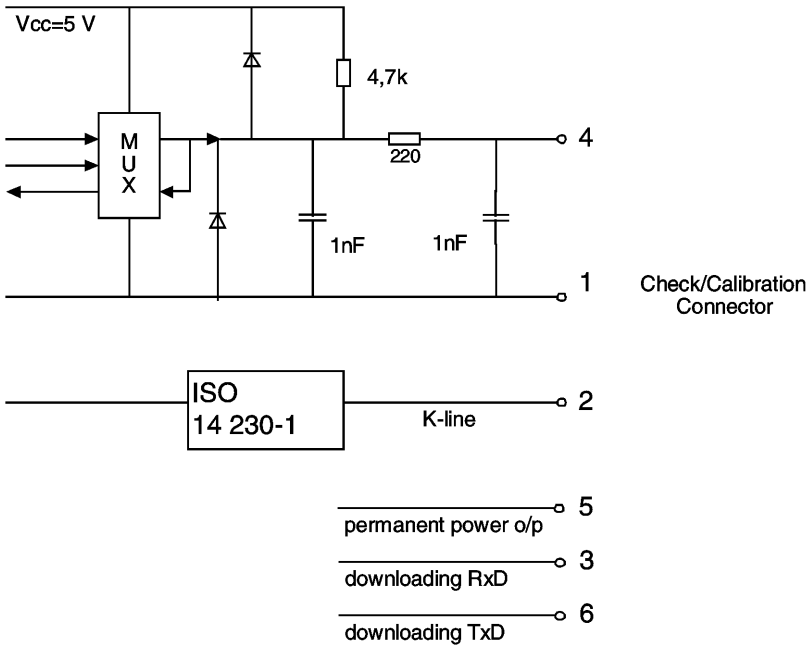
1.2. **Kontakternes tildeling**

INT_002 Kontakterne skal være tildelt i overensstemmelse med følgende tabel:

Klemme	Beskrivelse	Bemærkning
1	Batteri minus	Tilsluttet køretøjets negative batteripol
2	Datakommunikation	K-linie (ISO 14230-1)
3	RxD — Dataoverførsel	Dataindgang til kontrolapparat
4	Indgangs-/udgangssignal	Kalibrering
5	Permanent effektudgang	Det foreskrevne spændingsområde er som køretøjets strømforsyning minus 3 V for at tage hensyn til spændingstabet over beskyttelseskredsen Udgangseffekt 40 mA
6	TxD — Dataoverførsel	Dataoverførsel fra kontrolapparatet

1.3. **Blokdiagram**

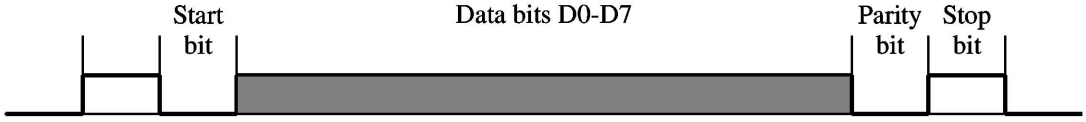
INT_003 Blokdiagrammet skal være i overensstemmelse med følgende:



2. GRÆNSEFLADE FOR DATAOVERFØRSEL

INT_004 Grænsefladen for dataoverførsel skal opfylde specifikationerne RS232.

INT_005 Grænsefladen for dataoverførsel skal have én startbit, 8 mindst betydende databits først, én lige paritetsbit og 1 stopbit.



Organisation af data bytes

Startbit: én bit med logisk niveau 0;

Databits: overføres med mindst betydende bit først;

Paritetsbit: lige paritet

Stopbit: én bit med logisk niveau 1;

Ved overførsel af numeriske data bestående af flere end én byte overføres den mest betydende byte først, og den mindst betydende byte sidst.

INT_006 Transmissionshastigheden skal kunne indstilles mellem 9 600 bps og 115 200 bps. Transmission skal kunne ske med den højst mulige transmissionshastighed, idet den indledende hastighed efter start af kommunikationen er stillet på 9 600 bps.

3. GRÆNSEFLADE FOR KALIBRERING

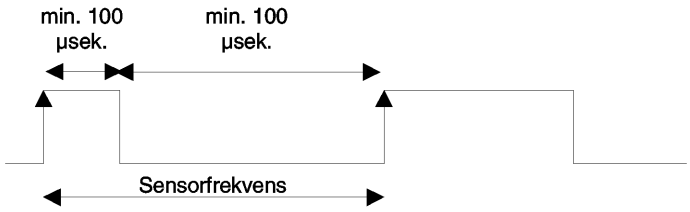
INT_007 Datakommunikationen skal opfylde ISO 14230-1 Road vehicles — Diagnostic systems — Keyword protocol 2000 — Part 1: Physical layer, First edition: 1999.

INT_008 Indgangs- og udgangssignalet skal opfylde følgende elektriske forskrift:

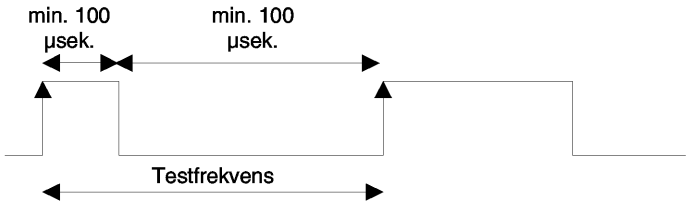
Parameter	Minimum	Typisk	Maksimum	Bemærkning
U_{lav} (ind)			1,0 V	I = 750 µA
$U_{høj}$ (ind)	4 V			I = 200 µA
Frekvens			4 kHz	
U_{lav} (ud)			1,0 V	I = 1 mA
$U_{høj}$ (ud)	4 V			I = 1 mA

INT_009 Indgangs- og udgangssignalet skal opfylde følgende tidsdiagrammer:

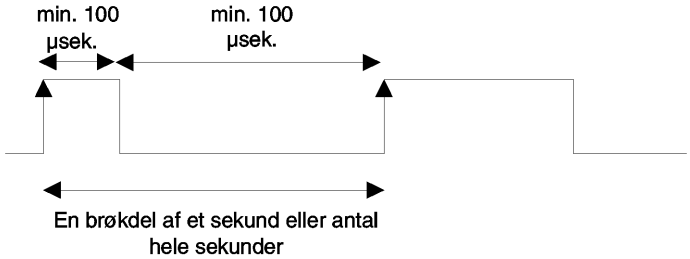
Signal fra sensor (udgang)



Testsignal (indgang)



UTC klokkesignal



Tillæg 7

PROTOKOLLER FOR DATAOVERFØRSEL

1. INDLEDNING

Dette tillæg beskriver de procedurer, der skal følges ved forskellige typer dataoverførsel til et eksternt lagermedium (ESM), foruden de protokoller, der skal gennemføres for at sikre korrekt overførsel af data og fuld kompatibilitet af det overførte dataformat, således at enhver tilsynsførende har adgang til disse data og mulighed for at kontrollere deres ægthed og integritet, før han analyserer dem.

1.1. **Område**

Der kan overføres data til et eksternt lagermedium:

— fra en køretøjsenhed med en intelligent dedikeret enhed (IDE) tilsluttet køretøjsenheden,

— fra et fartskriverkort med en IDE-enhed med kortlæser (IFD),

— fra et fartskriverkort via en køretøjsenhed ved hjælp af en IDE-enhed tilsluttet køretøjsenheden.

For at man skal kunne fastslå ægthed og integritet af overførte data, som er gemt på et eksternt lagermedium, bliver der ved dataoverførsel vedhæftet en underskrift i overensstemmelse med tillæg 11 (fælles sikkerhedsmekanismer). Kildeenhedens (køretøjsenhed eller kort) identifikation og sikkerhedsattester (fra medlemsstaten og for udstyret) bliver ligeledes overført. Den, der kontrollerer data, skal uafhængigt være indehaver af en betroet europæisk offentlig nøgle.

DDP_001 Data overført i én overførselssession skal på det eksterne lagermedium gemmes i én fil.

1.2. **Akronymer og notation**

I dette tillæg anvendes følgende akronymer:

AID	Applikationsnavn
ATR	Svar på nulstilling
CS	Kontrolsumbyte
DF	Dedikeret fil
DS	Diagnosesession
EF	Elementærfil
ESM	Eksternt lagermedium
FID	Filidentifikator (filnavn)
FMT	Formatbyte (første byte i meddelelsens hoved)
ICC	Chipkort
IDE	Intelligent dedikeret udstyr: Det udstyr, som anvendes til at overføre data til det eksterne lagermedium (f.eks. PC)
IFD	Kortlæser (Interface device)
KWP	Nøgleordsprotokol 2000
LEN	Længdebyte (sidste byte i meddelelsens hoved)
PPS	Valg af protokolparametre
PSO	Udfør sikkerhedsoperation
SID	Tjenesteidentifikator
SRC	Kildebyte
TGT	Adressebyte
TLV	Længde af mærkat
TREP	Parameter for svar på overførsel
TRTP	Parameter for anmodning om overførsel
VU	Køretøjsenhed

2. DATAOVERFØRSEL FRA KØRETØJSENHED

2.1. **Fremgangsmåde ved dataoverførsel**

For at overføre data fra køretøjsenheden skal operatøren foretage følgende:

— indsætte sit fartskriverkort i en kortplads i køretøjsenheden ([1]);

— tilslutte IDE-enheden til køretøjsenhedens datastik;

— etablere forbindelse mellem IDE-enhed og køretøjsenhed;

— på IDE-enheden, vælge data som skal overføres, og sende anmodningen til køretøjsenheden;

— afslutte dataoverførselssessionen.

2.2. **Protokol for dataoverførsel**

Protokollen har master/slave struktur, således at IDE-enheden fungerer som master og køretøjsenheden som slave.

Meddelelsesstruktur, -typer og -strøm er hovedsagelig baseret på Keyword protocol 2000 (KWP) (ISO 14230-2 Road vehicles — Diagnostic systems — Keyword protocol 2000 — Part 2: Data link layer).

Applikationslaget bygger hovedsagelig på det aktuelle udkast til ISO 14229-1 (Road vehicles — Diagnostic systems — Part 1: Diagnostic services, version 6 af 22. februar 2001).

2.2.1. ***Meddelelsesstruktur***

DDP_002 Alle meddelelser, som udveksles mellem IDE-enhed og køretøjsenhed, er formateret med tredelt struktur:

— et hoved bestående af en formatbyte (FMT), en destinationsbyte (TGT), en kildebyte (SRC) og eventuelt en længdebyte (LEN),

— et datafelt bestående af en tjenesteidentifikatorbyte (SID) og et varierende antal databytes, som kan omfatte en ikke obligatorisk diagnosesessionsbyte (DS) eller en frivillig overførselsparameterbyte (TRTP eller TREP).

— en kontrolsum bestående af en kontrolsumbyte (CS).

Hoved				Datafelt					Kontrolsum
FMT	TGT	SRC	LEN	SID	LID	DATA	. . .	. . .	CS
4 bytes				Maks. 255 bytes					1 byte

TGT- og SRC-byten repræsenterer den fysiske adresse på modtageren og afsenderen af meddelelsen. De har værdierne F0 Hex for IDE-enheden og EE Hex for køretøjsenheden.

LEN-byten er længden af datafeltdelen.

Kontrolsumbyten er 8 bit sumserie modulo 256 for alle meddelelsens bytes bortset fra selve kontrolsummen.

FMT-, SID-, DS-, TRTP- og TREP-bytes er defineret senere i dette dokument.

([1]) Det indsatte kort vil udløse de nødvendige adgangsrettigheder til overførselsfunktionen og til data.

DDP_003 Hvis de data, som meddelelsen skal medføre, er længere end pladsen i datafeltdelen, bliver meddelelsen reelt sendt som flere delmeddelelser. Hver sådan delmeddelelse har et hoved, samme SID og TREP og en 2-byte delmeddelelsestæller, som angiver delmeddelelsens nummer i den samlede meddelelse. For at der skal kunne foretages fejlkontrol og afbrydelse, kvitterer IDE-enheden for hver delmeddelelse. IDE-enheden kan acceptere delmeddelelsen, anmode om at den genoverføres, anmode køretøjsenheden om at begynde igen eller afbryde dataoverførslen.

DDP_004 Hvis den sidste delmeddelelse indeholder nøjagtig 255 bytes i datafeltet, skal der vedhæftes en afsluttende delmeddelelse, hvor datafeltet er tomt (bortset fra SID, TREP og delmeddelelsestælleren) som angivelse af meddelelsens slutning.

Eksempel:

Hoved	SID	TREP	Meddelelse	CS
4 bytes	Længere end 255 bytes			

Vil blive overført som:

Hoved	SID	TREP	00	01	Delmeddelelse 1	CS
4 bytes	255 bytes					

Hoved	SID	TREP	00	02	Delmeddelelse 2	CS
4 bytes	255 bytes					

. . .

Hoved	SID	TREP	xx	yy	Delmeddelelse n	CS
4 bytes	Mindre end 255 bytes					

eller som:

Hoved	SID	TREP	00	01	Delmeddelelse 1	CS
4 bytes	255 bytes					

Hoved	SID	TREP	00	02	Delmeddelelse 2	CS
4 bytes	255 bytes					

. . .

Hoved	SID	TREP	xx	yy	Delmeddelelse n	CS
4 bytes	255 bytes					

Hoved	SID	TREP	xx	yy+1	CS
4 bytes	4 bytes				

2.2.2. ***Meddelelsestyper***

Kommunikationsprotokollen for overførsel af data mellem køretøjsenheden og IDE-enheden kræver udveksling af 8 forskellige typer meddelelser.

Disse meddelelser er sammenfattet i følgende tabel.

Meddelelsesstruktur	Maks. 4 byte Hoved				Maks. 255 byte Data			1 byte Kontrolsum
IDE -> <- VU	FMT	TGT	SRC	LEN	SID	DS_ / TRTP	DATA	CS
Anmodning om at begynde kommunikation	81	EE	F0		81			E0
Positivt svar på anmodningen begynd kommunikation	80	F0	EE	03	C1		8F,EA	9B
Anmodning om at begynde diagnose-session	80	EE	F0	02	10	81		F1
Positivt svar på anmodningen begynd diagnose	80	F0	EE	02	50	81		31
Link-kontrol tjeneste								
Kontrollér transmissionshastighed (trin 1)								
9 600 Bd	80	EE	F0	04	87		01,01,01	EC
19 200 Bd	80	EE	F0	04	87		01,01,02	ED
38 400 Bd	80	EE	F0	04	87		01,01,03	EE
57 600 Bd	80	EE	F0	04	87		01,01,04	EF
115 200 Bd	80	EE	F0	04	87		01,01,05	F0
Positivt svar på kontrollér transmissionshastighed	80	F0	EE	02	C7		01	28
Transmissionshastighed (2. trin)	80	EE	F0	03	87		02,03	ED
Anmodning om at uploade	80	EE	F0	0A	35		00,00,00,00, 00,FF,FF, FF,FF	99
Positivt svar på anmodning om at uploade	80	F0	EE	03	75		00,FF	D5
Anmodning om dataoverførsel								
Oversigt	80	EE	F0	02	36	01		97
Aktiviteter	80	EE	F0	06	36	02	Dato	CS
Hændelser og fejl	80	EE	F0	02	36	03		99
Detaljeret hastighed	80	EE	F0	02	36	04		9A
Tekniske data	80	EE	F0	02	36	05		9B
Dataoverførsel af kort	80	EE	F0	02	36	06		9C
Positivt svar på anmodning om dataoverførsel	80	F0	EE	Len	35	TREP	Data	CS
Anmodning om at forlade dataoverførsel	80	EE	F0	01	37			96
Positivt svar på forlad dataoverførsel	80	F0	EE	01	77			D6
Anmodning om at standse kommunikation	80	EE	F0	01	82			E1
Positivt svar på stands kommunikation	80	F0	EE	01	C2			21
Kvittér for delmeddelelse	80	EE	F0	Len	83		Data	CS
Negative svar								
Generel afvisning	80	F0	EE	03	7F	Sid Req	10	CS
Tjeneste understøttes ikke	80	F0	EE	03	7F	Sid Req	11	CS
Delfunktion understøttes ikke	80	F0	EE	03	7F	Sid Req	12	CS
Ukorrekt meddelelseslængde	80	F0	EE	03	7F	Sid Req	13	CS
Betingelser ikke korrekte eller fejl i anmodnings-sekvens	80	F0	EE	03	7F	Sid Req	22	CS
Anmodning uden for gyldighedsområde	80	F0	EE	03	7F	Sid Req	31	CS
Upload ikke accepteret	80	F0	EE	03	7F	Sid Req	50	CS
Svar uafgjort	80	F0	EE	03	7F	Sid Req	78	CS
Data foreligger ikke	80	F0	EE	03	7F	Sid Req	FA	CS

Bemærkninger:

— Sid Req = Sid for den tilsvarende anmodning, Lid Req = Lid for den tilsvarende anmodning.
— TREP = TRTP for den tilsvarende anmodning.
— Mørke celler angiver at intet er overført.
— Betegnelsen upload (set fra IDE-enheden) anvendes for kompatibilitet med nøgleordsprotokollen (ISO 14229). Betydningen er den samme som af dataoverførsel (set fra køretøjsenheden).
— Eventuelle 2-byte delmeddelelsestællere er ikke vist i denne tabel.

2.2.2.1. *Anmodning om at begynde kommunikation (SID 81)*

DDP_005 Denne meddelelse afgives af IDE-enheden for at etablere en kommunikationsforbindelse med køretøjsenheden. Den indledende kommunikation udføres altid ved 9 600 baud (indtil transmissionshastigheden til sidst ændres ved hjælp af de pågældende link-kontroltjenester).

2.2.2.2. *Positivt svar på begynd kommunikation (SID C1)*

DDP_006 Denne meddelelse afgives af IDE-enheden som positivt svar på anmodning om at begynde kommunikation. Den indeholder de to nøglebytes '8F' 'EA' som angiver, at enheden understøtter protokollen, og hovedet indeholder oplysninger om destination, kilde og længde.

2.2.2.3. *Anmodning om at begynde diagnose-session (SID 10)*

DDP_007 Anmodning om at begynde diagnose-session afgives af IDE-enheden for at anmode om en ny diagnosesession med køretøjsenheden. Delfunktionen 'default session' (81 Hex) angiver, at der skal åbnes en standarddiagnosesession.

2.2.2.4. *Positivt svar på begynd diagnose (SID 50)*

DDP_008 Meddelelsen om positivt svar på begynd diagnose afgives af køretøjsenheden som positivt svar på anmodning om diagnosesession.

2.2.2.5. *Link kontrol tjeneste (SID 87)*

DDP_052 Link kontrol tjenesten anvendes af IDE-enheden til at indlede en ændring i transmissionshastigheden. Dette sker i to trin. I første trin foreslår IDE-enheden en ændring i transmissionshastigheden. Ved modtagelse af et positivt svar fra køretøjsenheden afgiver IDE-enheden en bekræftelse på den ændrede transmissionshastighed til køretøjsenheden (andet trin). IDE-enheden skifter derefter til den nye transmissionshastighed. Efter modtagelse af bekræftelsen skifter køretøjsenheden til den nye transmissionshastighed.

2.2.2.6. *Positivt svar på link kontrol (SID C7)*

DDP_053 Positivt svar på link kontrol angives af køretøjsenheden som svar på en anmodning til link kontrol tjenesten (første trin). Bemærk at der ikke svares på bekræftelsen af anmodningen (trin to).

2.2.2.7. *Anmodning om at uploade (SID 35)*

DDP_009 Meddelelsen anmodning om at uploade afgives af IDE-enheden for over for køretøjsenheden at anmode om en dataoverførsel. For at opfylde kravene i ISO14229 indgår der data om adresse, størrelse og format af de ønskede data. Da disse ikke kendes af IDE-enheden før overførslen, sættes lageradressen til 0, formatet til ukrypteret og lagerstørrelsen til maksimum.

2.2.2.8. *Positivt svar på anmodning om at uploade (SID 75)*

DDP_010 Positivt svar på anmodning om at uploade sendes af køretøjsenheden for at fortælle IDE-enheden, at køretøjsenheden er klar til at overføre data. For at opfylde kravene i ISO14229 indeholder den positive svarmeddelelse data, som fortæller IDE-enheden, at yderligere meddelelser med positivt svar på dataoverførsel vil indeholde maksimalt 00FF hex byte.

2.2.2.9. *Anmodning om dataoverførsel (SID 36)*

DDP_011 Anmodning om dataoverførsel sendes af IDE-enheden for over for køretøjsenheden at specificere den type data, som skal overføres. Overførslens type angives af en parameter for anmodning om dataoverførsel (TRTP) på én byte.

Der er seks typer dataoverførsel:

— Oversigt (TRTP 01).

— Aktiviteter på en nærmere angivet dato (TRTP 02),

— Hændelser og fejl (TRTP 03),

— Detaljeret hastighed (TRTP 04),

— Tekniske data (TRTP 05),

— Overførsel af data fra kort (TRTP 06).

DDP_054 IDE-enheden skal obligatorisk anmode om oversigt over dataoverførsel (TRTP 01) under en dataoverførselssession, da det kun på denne måde kan sikres, at køretøjsenhedens certifikater registreres i den overførte fil (så der er mulighed for verificering af en digital underskrift).

I andet tilfælde (TRTP 02) er det i meddelelsen overfør data angivet, hvilken kalenderdag (`TimeReal` format) der skal overføres.

2.2.2.10. *Positivt svar på overfør data (SID 76)*

DDP_012 Positivt svar på overfør data afgives af køretøjsenheden som svar på anmodningen om dataoverførsel. Meddelelsen indeholder de anmodede data med en parameter for svar på overførsel (TREP) svarende til anmodningens TRTP.

DDP_055 I første tilfælde (TREP F01) vil køretøjsenheden sende data, som hjælper IDE-operatøren til at vælge de data, som han yderligere vil overføre. Denne meddelelse indeholder følgende oplysninger:

— Sikkerhedscertifikater,

— Køretøjsidentifikation,

— Køretøjsenhedens aktuelle dato og klokkeslæt,

— Mindste og største dato, som kan overføres (data fra køretøjsenhed),

— Angivelse af kort, som er isat i køretøjsenheden,

— Tidligere dataoverførsler til en virksomhed

— Virksomhedslåse,

— Tidligere kontroller

2.2.2.11. *Anmodning om at forlade overførsel (SID 37)*

DDP_013 Anmodningen forlad dataoverførsel afgives af IDE-enheden for at fortælle køretøjsenheden, at dataoverførselssessionen er slut.

2.2.2.12. *Positivt svar på forlad overførsel (SID 77)*

DDP_014 Positivt svar på forlad dataoverførsel afgives af køretøjsenheden for at kvittere for anmodningen om dataoverførsel.

2.2.2.13. *Anmodningen stands kommunikation (SID 82)*

DDP_015 Anmodning om at standse kommunikation afgives af IDE-enheden for at afbryde kommunikationsforbindelsen til køretøjsenheden.

2.2.2.14. *Positivt svar på stands kommunikation (SID C2)*

DDP_016 Positivt svar på stands kommunikation afgives af køretøjsenheden for at kvittere for anmodningen om at standse kommunikation.

2.2.2.15. *Kvittér for delmeddelelse (SID 83)*

DDP_017 Delmeddelelsen kvittering afgives af IDE-enheden for at bekræfte de enkelte dele af en meddelelse, der overføres som flere delmeddelelser. Datafeltet indeholder den SID, som er modtaget fra køretøjsenheden, og en 2-byte kode som følger:

— MsgC + 1 Kvitterer for korrekt modtagelse af delmeddelelse nummer MsgC.
Anmodning fra IDE-enheden til køretøjsenheden om at sende næste delmeddelelse

— MsgC angiver, at der er en fejl ved modtagelse af delmeddelelse nummer MsgC.
Anmodning fra IDE-enheden til køretøjsenheden om at genfremsende delmeddelelsen.

— FFFF anmoder om afslutning af meddelelsen.
Dette kan af IDE-enheden anvendes til at afslutte overførslen af meddelelsen fra køretøjsenheden uanset grund.

For den afsluttende delmeddelelse i en meddelelse (LEN byte < 255) kan der kvitteres med enhver af disse koder, eller kvittering kan undlades.

Svar fra køretøjsenheden består af flere delmeddelelser og kan være:

— Positivt svar på anmodning om dataoverførsel (SID 76).

2.2.2.16. *Negativt svar (SID 7F)*

DDP_018 Som svar på ovennævnte anmodninger sender køretøjsenheden negativt svar, når køretøjsenheden ikke kan imødekomme anmodningen. Meddelelsens datafelter indeholder svarets SID (7F), anmodningens SID og en kode, som angiver begrundelsen for det negative svar. Følgende koder er til rådighed:

— 10 generel afvisning
Operationen kan ikke gennemføres af grunde, som ikke er omfattet af nedenstående.

— 11 tjeneste ikke understøttet
Anmodningens SID er ikke blevet forstået.

— 12 delfunktion understøttes ikke
Anmodningens DS eller TRTP forstås ikke, eller der er ikke flere delmeddelelser at overføre.

— 13 ukorrekt meddelelseslængde
Længden af den modtagne meddelelse er forkert.

— 22 ukorrekte betingelser eller fejl i anmodningssekvens
Den anmodede tjeneste er ikke aktiv eller sekvensen af anmodningsmeddelelsen ukorrekt.

— 31 Anmodningen uden for det fastlagte område
Posten med anmodningens parametre (datafelt) ugyldig.

— 50 upload ikke accepteret
Anmodningen kan ikke efterkommes (køretøjsenhed ikke i korrekt driftsmåde, eller intern fejl i køretøjsenhed).

— 78 svar uafgjort
Den anmodede operation kan ikke gennemføres i tide, og køretøjsenheden er ikke klar til at modtage endnu en anmodning.

— FA-data foreligger ikke
Dataobjektet for en anmodning om dataoverførsel findes ikke i køretøjsenheden (f.eks. hvis der ikke er isat noget kort) . . .).

2.2.3. ***Meddelelsesstrøm***

En typisk meddelelsesstrøm ved en normal dataoverførselsprocedure er følgende:

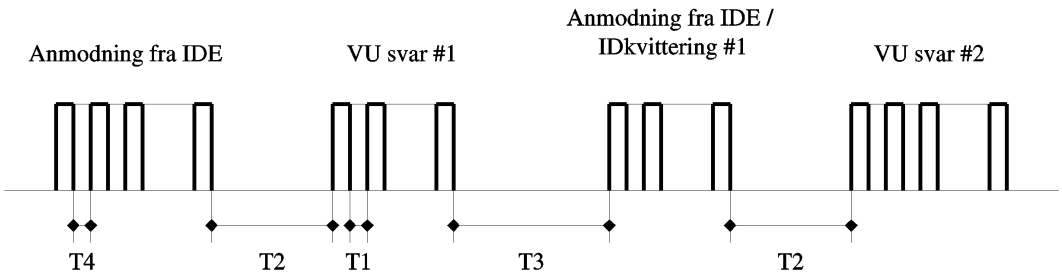
IDE-enhed		Køretøjsenhed
Anmodning om at begynde kommunikation	⇨	
	⇦	Positivt svar
Anmodning om at begynde diagnosetjeneste	⇨	
	⇦	Positivt svar
Anmodning om at uploade	⇨	
	⇦	Positivt svar
Anmodning om oversigt over dataoverførsel	⇨	
	⇦	Positivt svar
Anmodning om dataoverførsel #2	⇨	
	⇦	Positivt svar #1
Kvittér for delmeddelelse #1	⇨	
	⇦	Positivt svar #2
Kvittér for delmeddelelse #2	⇨	
	⇦	Positivt svar #m
Kvittér for delmeddelelse #m	⇨	
	⇦	Positivt svar (Datafelt < 255 Bytes)
Kvittér for delmeddelelse (ikke obligatorisk)	⇨	
. . .		
Anmodning om dataoverførsel #n	⇨	
	⇦	Positivt svar
Anmodning om at forlade dataoverførsel	⇨	
	⇦	Positivt svar
Anmodning om at standse kommunikation	⇨	
	⇦	Positivt svar

2.2.4. ***Synkronisering***

DDP_019 Under normal drift er tidsparametrene i følgende figur relevante:

Figur 1

Meddelelsesstrøm, synkronisering



Hvor:

P1 = Tidsrum, som adskiller bytes for svar fra køretøjsenhed

P2 = Tid fra slutning af IDE-enhedens anmodning til start på køretøjsenhedens svar, eller fra slutning af IDE-enhedens kvittering til start på køretøjsenhedens næste svar.

P3 = Tid fra slutning af køretøjsenhedens svar til start på ny anmodning fra IDE-enheden, eller fra slutningen af køretøjsenhedens svar til start på IDE-enhedens kvittering, eller fra slutningen af IDE-enhedens anmodning til start på ny anmodning fra IDE-enheden hvis køretøjsenheden ikke svarer.

P4 = Tidsrum der adskiller bytes i anmodning fra IDE-enheden.

P5 = Forlænget T3 ved overførsel fra kort.

Tilladte værdier af tidsparametrene er angivet i følgende tabel (det udvidede KWP-tidsparametersæt, som anvendes ved fysisk adressering for at gøre kommunikationen hurtigere).

Synkroniseringsparameter	Nedre grænseværdi (ms)	Øvre grænseværdi (ms)
P1	0	20
P2	20	1 000 (*)
P3	10	5 000
P4	5	20
P5	10	20 minutter

(*) hvis køretøjsenheden afgiver et negativt svar indeholdende en kode med betydningen »anmodning korrekt modtaget, svar uafgjort« udvides denne værdi til samme øvre grænseværdi for P3.

2.2.5. ***Fejlhåndtering***

Indtræffer der en fejl under meddelelsesudvekslingen, ændres meddelelsesstrømmene alt efter hvilket udstyr der har fundet fejlen, og den meddelelse, som har udløst fejlen.

I fig. 2 og fig. 3 vises fejlhåndteringsprocedurer for hhv. køretøjsenhed og IDE-enhed.

2.2.5.1. *Start kommunikation fase*

DDP_020 Hvis IDE-enheden finder en fejl i start kommunikation fasen, enten i synkroniseringen eller i bitstrømmen, venter den i et tidsrum af P3min, før den igen afgiver anmodningen.

DDP_021 Hvis køretøjsenheden finder en fejl i den afgivne sekvens fra IDE-enheden, skal den intet svar sende og vente på endnu en anmodning om start på kommunikation inden for et tidsrum af P3max.

2.2.5.2. *Kommunikationsfase*

Der kan defineres to forskellige fejlhåndteringsområder:

1. Køretøjsenheden konstaterer en fejl i dataoverførslen for IDE-enheden

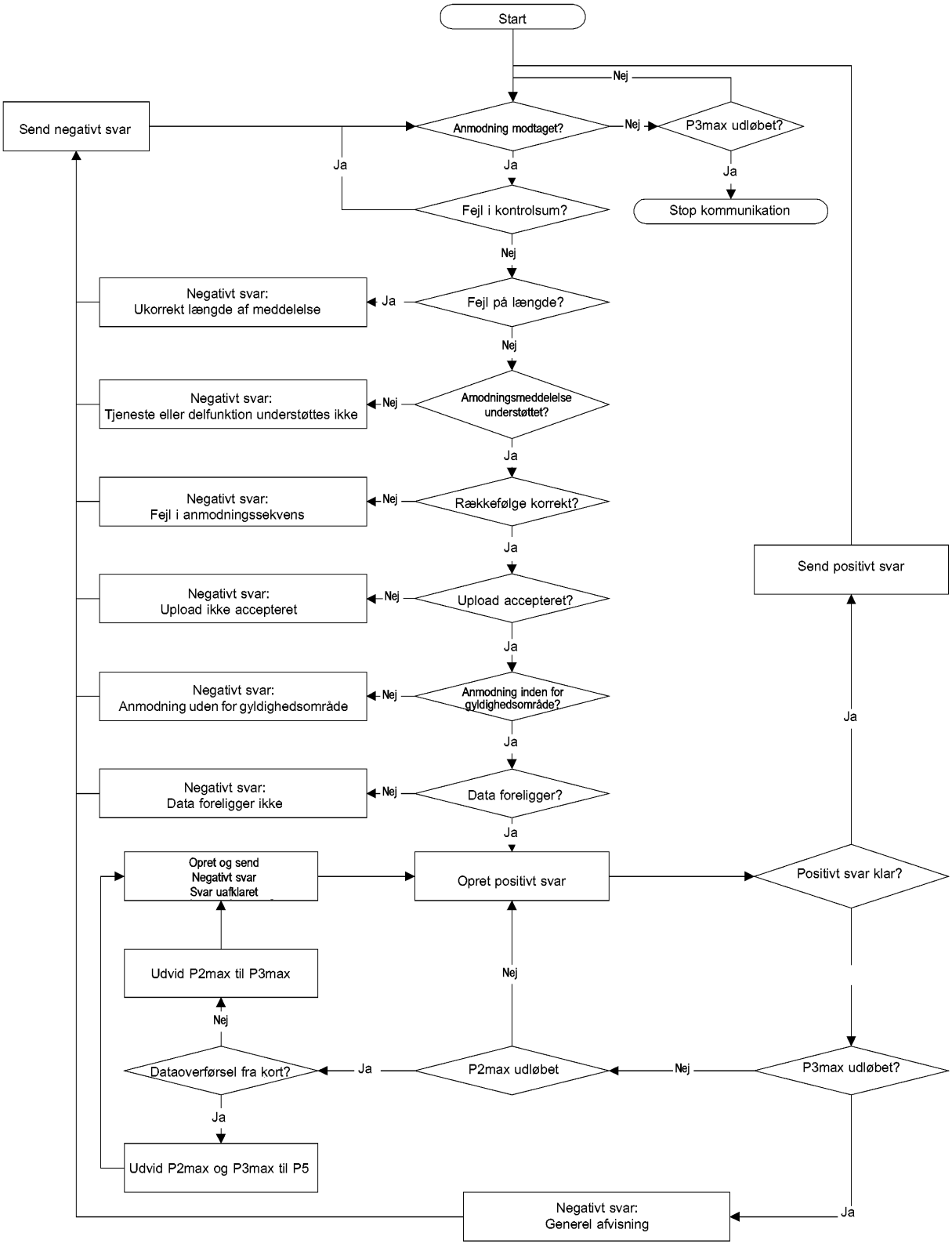
DDP_022 For hver modtaget meddelelse skal køretøjsenheden finde eventuelle synkroniseringsfejl, fejl ved byteformat, (f.eks. fejl ved start- og stopbit) og rammefejl (forkert antal bytes modtaget, forkert kontrolsumbyte).

DDP_023 Hvis køretøjsenheden finder en af ovennævnte fejl, afgiver den intet svar og ignorerer den modtagne meddelelse.

DDP_024 Køretøjsenheden kan finde andre fejl i den modtagne meddelelses format eller indhold (f.eks. at meddelelsen ikke understøttes), uanset om meddelelsen opfylder forskrifterne for længde og kontrolsum; i så fald skal køretøjsenheden svare IDE-enheden med en negativ svarmeddelelse med angivelse af fejlens art.

Figur 2

Håndtering af fejl ved køretøjsenhed



2. IDE-enheden registrerer en dataoverførselsfejl ved køretøjsenheden

DDP_025 For hver modtagen meddelelse skal IDE-enheden finde eventuelle synkroniseringsfejl, fejl ved byteformat, (f.eks. fejl ved start- og stopbit) og rammefejl (forkert antal bytes modtaget, forkert kontrolsumbyte).

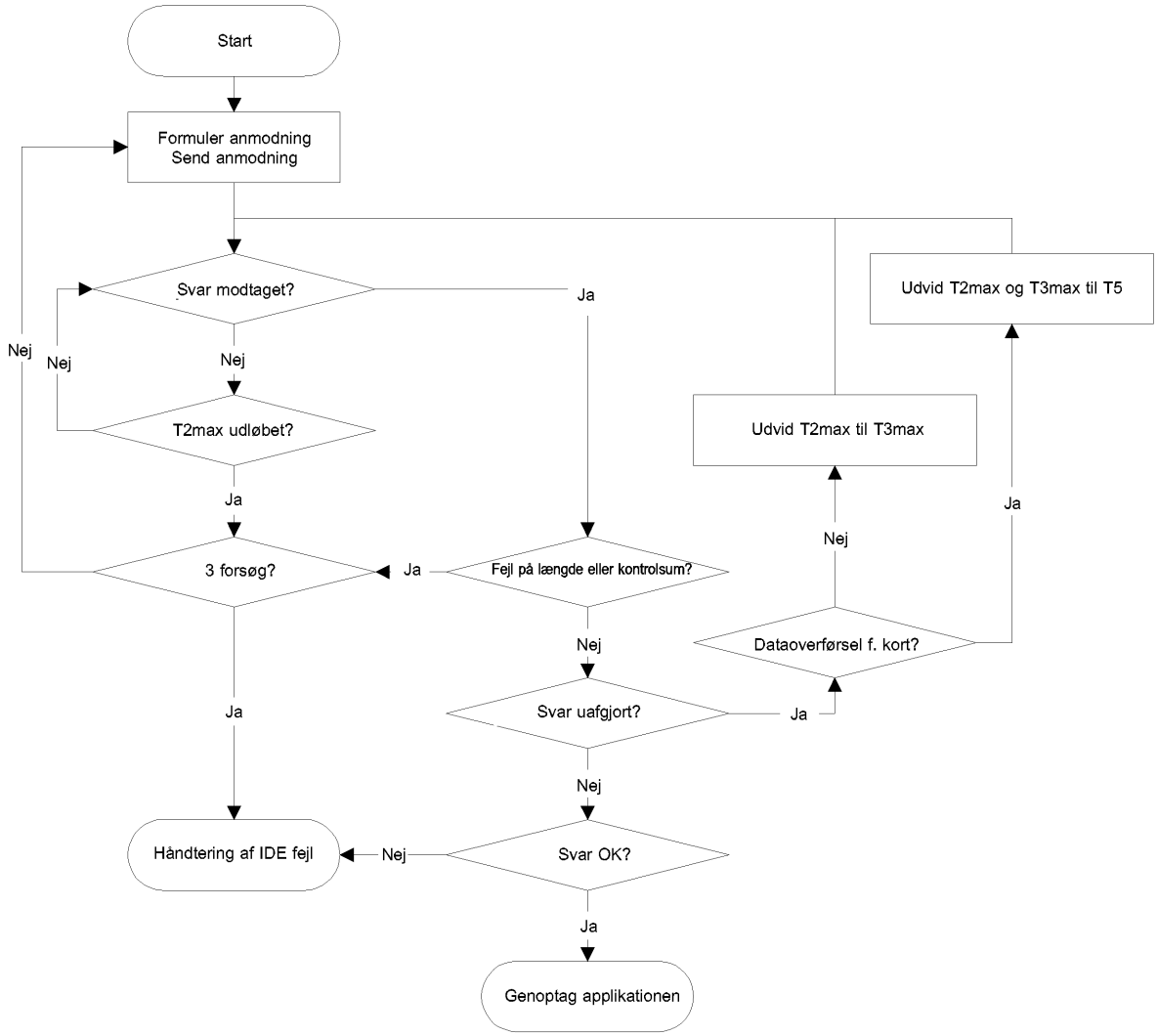
DDP_026 IDE-enheden skal finde sekvensfejl, f.eks. ukorrekt forøgelse af tællerne for delmeddelelser i successivt modtagne meddelelser.

DDP_027 Hvis IDE-enheden konstaterer en fejl eller der ikke kom svar fra køretøjsenheden inden for et tidsrum af P2max, vil anmodningen blive sendt igen, til den er sendt i alt højst tre gange. Hvad angår denne fejlfinding vil en kvittering for delmeddelelse blive betragtet som en anmodning til køretøjsenheden.

DDP_028 IDE-enheden skal vente mindst P3min, før den begynder hver dataoverførsel; venteperioden måles fra seneste beregnede forekomst af en stopbit, efter at fejlen blev konstateret.

Figur 3

Håndtering af fejl ved IDE-enheden



2.2.6. ***Svarmeddelelsens indhold***

Dette afsnit angiver indholdet af datafelterne i de forskellige positive svarmeddelelser.

Dataelementerne er defineret i tillæg 1 (Dataordliste).

2.2.6.1. *Positivt svar på oversigt over data til overførsel*

DDP_029 Datafeltet i meddelelsen »Positivt svar på oversigt over data til overførsel« skal bære følgende data i følgende rækkefølge under SID 76 Hex, TREP 01 Hex og med passende opdeling i delmeddelelser og behørig tælling:

Dataelement	Længde (bytes)	Kommentar
MemberStateCertificate	194	Sikkerhedsattester for køretøjsenhed
VUCertificate	194	
VehicleIdentificationNumber	17	Identifikation af køretøjet
VehicleRegistrationIdentification		
vehicleRegistrationNation	1	
vehicleRegistrationNumber	14	
CurrentDateTime	4	Aktuel dato og klokkeslæt på køretøjsenhed
VuDownloadablePeriod		Downloadable period
minDownloadableTime	4	
maxDownloadableTime	4	
CardSlotsStatus	1	Type kort, som er indsat i køretøjsenheden
VuDownloadActivityData		Foregående dataoverførsel for køretøjsenhed
downloadingTime	4	
fullCardNumber	18	
companyOrWorkshopName	36	
VuCompanyLocksData		Alle virksomhedslåse, som er gemt. Hvis afsnittet er tomt, sendes kun noOfLocks = 0
noOfLocks	1	
...	(98)	
VuVirksomhedLåsPost: lockInTime	4	
VuVirksomhedLåsPost: lockOutTime	4	
VuVirksomhedLåsPost: companyName	36	
VuVirksomhedLåsPost: companyAddress	36	
VuVirksomhedLåsPost: companyCardNumber	18	
...		
VuControlActivityData		Alle kontrolposter, som er gemt i køretøjsenheden. Hvis afsnittet er tomt, sendes kun noOfControls = 0
noOfControls	1	
...	(31)	
VuKontrolAktivitetPost: controlType	1	
VuKontrolAktivitetPost: controlTime	4	
VuKontrolAktivitetPost: controlCardNumber	18	
VuKontrolAktivitetPost: downloadPeriodBeginTime	4	
VuKontrolAktivitetPost: downloadPeriodEndTime	4	
...		
Underskrift	128	RSA-underskrift af alle data (bortset fra certifikater) begyndende fra VehicleIdentificationNumber ned til sidste byte i sidste VuControlActivityRecord

2.2.6.2. *Positivt svar på overførsel af dataaktiviteter*

DDP_030 Datafeltet i meddelelsen »Positivt svar på anmodning om overførsel af dataaktivitet« skal indeholde følgende data i følgende rækkefølge under SID 76 Hex og TREP 02 Hex med passende opdeling i delmeddelelser og behørig tælling:

Dataelement	Længde (Bytes)	Kommentar
TimeReal	4	Dato for dataoverførsel
OdometerValueMidnight	3	Kilometerstand ved slutningen af overførselsdøgnet
VuCardIWData noOfVuCardIWRecords	2	Data vedrørende isætnings- og udtagningscykluser for kort. — Hvis der ikke foreligger nogen data i dette afsnit, sendes kun noOfVuCardIWRecords = 0 — Når en VuCardIWRecord strækker sig hen over 00:00 (kortet isat det foregående døgn) eller hen over 24:00 (kortet udtaget det følgende døgn) skal den fremstå fuldt synlig i begge de pågældende døg
...	(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 noOfActivityChanges	2	Kortlæserstatus kl. 00:00 og aktivitetsskift registreret det døgn, for hvilket dataoverførsel har fundet sted
...		
ActivityChangeInfo	2	
...		
VuPlaceDailyWorkPeriodData noOfPlaceRecords	1	Stedrelaterede data for det døgn, for hvilket dataoverførsel har fundet sted. Hvis afsnittet er tomt, sendes kun noOfPlaceRecords = 0
...	(28)	
Post: fullCardNumber	18	
placeRecord		
entryTime	4	
entryTypeDailyWorkPeriod	1	
dailyWorkPeriodCountry	1	
dailyWorkPeriodRegion	1	
vehicleOdometerValue	3	
...		
VuSpecificConditionData noOfSpecificConditionRecords	2	Data vedrørende særlige omstændigheder registreret for det døgn, for hvilket data er overført. Er afsnittet tomt, sendes kun noOfSpecificConditionRecords = 0
...	(5)	
SpecificConditionRecord		
EntryTime	4	
specificConditionType	1	
...		
Underskrift	128	RSA-underskrift af alle data (bortset fra certifikater) begyndende fra TimeReal ned til sidste byte i sidste post vedrørende særlige omstændigheder

2.2.6.3. *Positivt svar på overførsel af datahændelser og -fejl*

DDP_031 Datafeltet i meddelelsen »Positivt svar på anmodning om overførsel af datahændelser og -fejl« skal indeholde følgende data i følgende rækkefølge under SID 76 Hex og TREP 03 Hex, med passende opdeling i delmeddelelser og behørig tælling:

Dataelement	Længde (bytes)	Kommentar
VuFaultData		Alle fejl, som er gemt eller i gang i køretøjsenheden. Er afsnittet tomt, sendes kun 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		Alle hændelser (bortset fra overskridelse af tilladt hastighed), som er gemt eller i gang i køretøjsenheden. Er afsnittet tomt, sendes kun 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 vedrørende seneste kontrol med overskridelse af tilladt hastighed (hvis ingen data foreligger, anvendes standardværdi)
LastOverspeedControlTime	4	
FirstOverspeedSince	4	
NumberOfOverspeedSince	1	
VuOverSpeedingEventData		Alle hændelser med overskridelse af tilladt hastighed, som er gemt i køretøjsenheden. Er afsnittet tomt, sendes kun 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		Alle hændelser med overskridelser af tilladt hastighed, som er gemt i køretøjsenheden (uden for rammerne af en fuld kalibrering). Er afsnittet tomt, sendes kun noOfVuTimeAdjRecords = 0
NoOfVuTimeAdjRecords	1	
...	(98)	
JusteringPost: OldTimeValue	4	
JusteringPost: NewTimeValue	4	
JusteringPost: WorkshopName	36	
JusteringPost: WorkshopAddress	36	
JusteringPost: WorkshopCardNumber	18	
...		
Underskrift	128	RSA-underskrift af alle data, begyndende fra noOfVuFaults ned til sidste byte i sidste tidsjusteringspost

2.2.6.4. *Positivt svar om overførsel af detaljerede hastighedsdata*

DDP_032 Datafeltet i meddelelsen »Positivt svar på anmodning om overførsel af detaljeret hastighed« skal indeholde følgende data i følgende rækkefølge under SID 76 Hex og TREP 04 Hex, med passende opdeling i delmeddelelser og behørig tælling:

Dataelement	Længde (bytes)	Kommentar
VuDetailedSpeedData		Alle detaljerede hastighedsdata, som er gemt i køretøjsenheden (én hastighedsblok i minuttet i den tid, køretøjet har været i bevægelse) 60 hastighedsværdier i minuttet (én i sekundet)
NoOfSpeedBlocks	2	
...		
VuDeatailedSpeedBlock		
SpeedBlockBeginDate	4	
speedsPerSecond	60	
...		
Underskrift	128	RSA-underskrift af alle data, begyndende fra noOfSpeedBlocks ned til sidste byte i sidste hastighedsdatagruppe

2.2.6.5. *Positivt svar på overførsel af tekniske data*

DDP_033 Datafeltet i meddelelsen »Positivt svar på anmodning om overførsel af tekniske data« skal indeholde følgende data i følgende rækkefølge under SID 76 Hex og TREP 05 Hex med passende opdeling i delmeddelelser og behørig tælling:

Dataelement	Længde (bytes)	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		Alle kalibreringsposter, som er gemt i køretøjsenheden.
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	
...		
Underskrift	128	RSA-underskrift af alle data, begyndende fra vuManufacturerName ned til sidste byte i sidste VuCalibrationRecord

2.3. **Lagring af fil på eksternt lagermedium**

DDP_034 Når en dataoverførselssession har omfattet overførsel af data fra en køretøjsenhed, skal IDE-enheden i én fysisk fil gemme alle data, som er modtaget fra køretøjsenheden under overførselssessionen i meddelelser om positiv respons på dataoverførsel. Data som gemmes, omfatter ikke meddelelsers hoved, delmeddelelsestællere, tomme delmeddelelser og kontrolsummer, men indbefatter SID og TREP (af første delmeddelelse kun hvis der er flere delmeddelelser).

3. PROTOKOL FOR OVERFØRSEL AF FARTSKRIVERKORT

3.1. **Anvendelsesområde**

Dette afsnit beskriver direkte overførsel af data fra et fartskriverkort til en IDE-enhed. IDE-enheden er ikke en del af det sikre miljø; derfor udføres der ikke ægthedskontrol mellem kortet og IDE-enheden.

3.2. **Definitioner**

Overførselssession: Hver gang der finder en overførsel af chipkortdata sted. Sessionen omfatter hele forløbet fra en kortlæser nulstiller chipkortet til deaktivering af chipkortet (udtagning af kort eller næste isætning).

Underskrevet datafil: En fil fra chipkortet. Filen overføres til kortlæseren som almindelig tekst. På chipkortet bliver filen hashet og underskrevet, og underskriften overføres til kortlæseren.

3.3. **Dataoverførsel af kort**

DDP_035 Overførsel af et fartskriverkort omfatter følgende trin:

— Overførsel af kortets fælles oplysninger i elementærfilerne `ICC` og `IC`. Disse oplysninger er ikke obligatoriske og sikres ikke med digital underskrift.

— Overførsel af elementærfilens `Card_Certificate` og `CA_Certificate`. Disse oplysninger sikres ikke med digital underskrift.

Det er obligatorisk at overføre disse filer ved hver overførselssession.

— Overførsel af applikationens øvrige elementærfiler (i den dedikerede fil `Tachograph`) undtagen elementærfilen `Card_Download`. Disse oplysninger sikres med digital underskrift.

— Ved hver overførselssession er det obligatorisk som minimum at overføre elementærfilerne `Application_Identification` og `ID`.

— Ved overførsel af et førerkort er det desuden obligatorisk at overføre følgende elementærfiler:

— `Events_Data`,

— `Faults_Data`,

— `Driver_Activity_Data`,

— `Vehicles_Used`,

— `Places`,

— `Control_Activity_Data`,

— `Specific_Conditions`.

— Ved dataoverførsel fra førerkort opdateres `LastCardDownload` datoen i elementærfilen `Card_Download`

— Ved overførsel fra værkstedskort skal kalibreringstælleren i elementærfilen `Card_Download` nulstilles.

3.3.1. ***Initialiseringssekvens***

DDP_036 IDE-enheden skal indlede sekvensen som følger:

Kort	Retning	IDE-enhed/Kortlæser	Betydning/Bemærkninger
	⇦	Nulstilling af hardware	
ATR	⇨		

Om ønsket kan man ved hjælp af PPS skifte til en højere transmissionshastighed, når blot denne understøttes af chipkortet.

3.3.2. ***Sekvens for ikke underskrevne datafiler***

DDP_037 Følgende sekvens anvendes til overførsel af elementærfilerne `ICC`, `IC`, `Card_Certificate` og `CA_Certificate`:

Kort	Retning	IDE-enhed/Kortlæser	Betydning/Bemærkninger
	⇦	SELECT FILE	Vælg ved filnavn
OK	⇨		
	⇦	READ BINARY	Indeholder filen flere data end svarende til bufferstørrelsen af kortlæser eller kort, må kommandoen gentages, indtil hele filen er læst.
Fildata OK	⇨	Gem data på eksternt lagermedium	I overensstemmelse med 3.4 Format for lagring af data

Før valg af `Card_Certificate` elementærfilen skal fartskriverapplikationen være valgt (vælges ved applikationsnavn).

3.3.3. ***Sekvens for underskrevne datafiler***

DDP_038 Følgende sekvens anvendes til hver af de efterfølgende filer, som skal overføres med tilhørende underskrift:

Kort	Dir	IDE-enhed/Kortlæser	Betydning/Bemærkninger
	⇦	SELECT FILE	
OK	⇨		
	⇦	PERFORM HASH OF FILE	Beregner hash-værdien af den valgte fils dataindhold ved hjælp af den foreskrevne hash-algoritme i overensstemmelse med tillæg 11. Denne kommando er ikke en ISO-kommando
Beregn hashværdi af fil og gem hashværdi midlertidigt			
OK	⇨		
	⇦	READ BINARY	Indeholder filen flere data end svarende til bufferstørrelsen af kortlæser eller kort, må kommandoen gentages, indtil hele filen er læst.
Fildata OK	⇨	Gem de modtagne data på eksternt lagermedium	I overensstemmelse med 3.4 Format for lagring af data
	⇦	PSO: COMPUTE DIGITAL SIGNATURE	
Udfør sikkerhedsoperationen »Compute Digital Signature« 'med anvendelse af den midlertidigt gemte hash-værdi			
Underskrift OK	⇨	Tilføj data til de data, som i forvejen er gemt på det eksterne lagermedium	I overensstemmelse med 3.4 Format for lagring af data

3.3.4. ***Sekvens for nulstilling af kalibreringstæller.***

DDP_039 Til nulstilling af `NoOfCalibrationsSinceDownload` tælleren i elementærfilen `Card_Download` på et værkstedskort anvendes følgende sekvens:

Kort	Dir	IDE-enhed/Kortlæser	Betydning/Bemærkninger
	⇦	SELECT FILE EF `Card_Download`	Vælg ved filnavn
OK	⇨		
	⇦	UPDATE BINARY `NoOfCalibrationsSinceDownload` = '00 00'	
nulstiller antal overførsler fra kort			
OK	⇨		

3.4. **Format for lagring af data**

3.4.1. ***Indledning***

DDP_040 De overførte data skal gemmes i overensstemmelse med følgende betingelser:

— Data skal opbevares transparent. Dette indebærer, at byte-rækkefølgen såvel som bitrækkefølgen i den overførte byte skal forblive uændret ved overførslen.

— Alle filer, der overføres fra kortet i løbet af en overførselssession, gemmes i én fil på det eksterne lagermedium.

3.4.2. ***Filformat***

DDP_041 Filformatet er en sammenkædning af flere TLV-objekter.

DDP_042 Mærkaten for en elementærfil skal være filidentifikatoren med tilføjelsen »00«.

DDP_043 Mærkaten for en elementærfils underskrift skal være filidentifikatoren plus tilføjelsen »01«.

DDP_044 Længden er en to byte værdi. Værdien fastlægger antal bytes i værdifeltet. Værdien »FF FF« i længdefeltet er forbeholdt fremtidig brug.

DDP_045 Når en fil ikke overføres, må intet vedrørende filen gemmes (ingen mærkat og ingen nullængde).

DDP_046 En underskrift skal gemmes som næste TLV-objekt direkte efter det TLV-objekt, som indeholder filens data.

Definition	Betydning	Længde
FID (2 bytes) || »00«	Mærkat for elementærfil (FID)	3 bytes
FID (2 bytes) || »01«	Mærkat for underskrift af elementærfil (FID)	3 bytes
xx xx	Længde af værdifelt	2 bytes

Eksempel på data i en fil overført til eksternt lagermedium:

Mærkat	Længde	Værdi
`00 02 00`	`00 11`	Data i elementærfilen `ICC`
`C1 00 00`	`00 C2`	Data i elementærfilens `Card_Certificate`
		...
`05 05 00`	`0A 2E`	Data i elementærfilen `Vehicles_Used`
`05 05 01`	`00 80`	Underskrift af elementærfilen `Vehicles_Used`

4. OVERFØRSEL AF FARTSKRIVERKORT VIA KØRETØJSENHEDEN

DDP_047 Køretøjsenheden skal gøre det muligt at overføre indholdet af et førerkort, som indsættes i en tilsluttet IDE-enhed.

DDP_048 IDE-enheden sender en meddelelse med »Anmodning om overførsel af kortdata« til køretøjsenheden for at indlede denne arbejdsmåde (se 2.2.2.9).

DDP_049 Køretøjsenheden skal derefter overføre hele kortet fil for fil i overensstemmelse med protokollen for overførsel af kort som fastlagt i punkt 3, og skal fremsende alle data, som er modtaget fra kortet, til det eksterne lagermedium i det korrekte TLV-filformat (se 3.4.2) og indkapslet i en »Positivt svar på overførsel af data« meddelelse.

DDP_050 IDE-enheden skal hente data fra meddelelsen om »positivt svar på overførsel af data« (efter fjernelse af hoveder, SID, TREP, delmeddelelsestællere eller kontrolsummer) og gemme dem i én fysisk fil som beskrevet i punkt 2.3.

DDP_051 Køretøjsenheden skal derefter i givet fald ajourføre førerkortets `Control_Activity_Data` eller `Card_Download` fil.

Tillæg 8

KALIBRERINGSPROTOKOL

1. INDLEDNING

I dette tillæg beskrives, hvordan der udveksles data mellem en køretøjsenhed og en tester via K-linjen, som er en del af den i tillæg 6 beskrevne kalibreringsgrænseflade. Det beskriver desuden styringen af ind-/uddatalinjen på kalibreringsstikket.

Etablering af K-linje kommunikationer er beskrevet i punkt 4 »Kommunikationsservicer«.

I dette tillæg anvendes begrebet diagnose»sessioner« til fastlæggelse af omfanget af styring over K-linjen under forskellige betingelser. Den forudindstillede tilstand er »standardsessionen«, hvor alle data kan aflæses fra køretøjsenheden, men ingen data kan skrives til den.

Valg af diagnose-session er beskrevet i punkt 5 »Administrative servicer«.

CPR_001 I »ECUProgrammingSession« kan der indlæses data til køretøjsenheden. Ved indlæsning af kalibreringsdata (krav 097 og 098) skal køretøjsenheden desuden være i funktionsmåde CALIBRATION.

Dataoverførsel gennem K-linje er beskrevet i punkt 6 »Dataoverførselsservicer«. Format på de overførte data er beskrevet i punkt 8 »Formater på dataRecords«.

CPR_002 I »ECUAdjustmentSession« kan kalibrerings-I/O-signallinjens I/O-funktionsmåde vælges via K-linjegrænsefladen. Styring af I/O signallinjen er beskrevet i punkt 1.1.1 »Styring af testimpulser — funktionsenhed for ind-/uddatastyring«.

CPR_003 I hele dette dokument betegnes testerens adresse som 'tt'. Skønt visse adresser for testere kan være foretrukne, skal køretøjsenheden svare korrekt på enhver testeradresse. Køretøjsenhedens fysiske adresse er 0xEE.Termer

2. DEFINITIONER OG HENVISNINGER

Protokoller, meddelelser og fejlkoder bygger hovedsagelig på det aktuelle udkast til ISO 14229-1 (Road vehicles — Diagnostic systems — Part 1: Diagnostic services, version 6 af 22. februar 2001).

Der anvendes bytekodning og hexadecimale værdier til serviceidentifikatorer, serviceanmodninger og -svar samt standardparametre.

Begrebet »tester« anvendes for det udstyr, som benyttes til at indlæse programmerings- og kalibreringsdata i køretøjsenheden.

Begreberne »klient« og »server« henviser henholdsvis til testeren og køretøjsenheden.

Begrebet ECU står for »Electronic control unit« og henviser til køretøjsenheden.

Henvisninger:

ISO 14230-2: Road Vehicles — Diagnostic Systems — Keyword Protocol 2000 — Part 2: Data Link Layer. First edition: 1999. Diagnosesystemer til køretøjer

3. OVERSIGT OVER SERVICER

3.1. **Servicer, som er til rådighed**

I nedenstående tabel gives en oversigt over de servicer, som vil være til rådighed i kontrolapparatet og er fastlagt i dette dokument.

CPR_004 Tabellerne angiver servicer, som er til rådighed i en påbegyndt diagnose-session.

— Søjle 1 angiver de servicer, som er til rådighed

— Søjle 2 henviser til nummeret på det punkt i dette tillæg, hvor denne service er nærmere defineret.

— Søjle 3 tildeler værdier til serviceidentifikatorer for anmodningsmeddelelser.

— Søjle 4 angiver de servicer i en »StandardDiagnosticSession« (SS), som skal være implementeret i hver køretøjsenhed.

— Søjle 5 angiver de servicer i en »ECUAdjustmentSession« (ECUAS), som skal være implementeret, så der er mulighed for styring af I/O-signallinjen i kalibreringsstikket på køretøjsenhedens frontpanel.

— Søjle 6 angiver de servicer i en »ECUProgrammingSession« (ECUPS), som skal være implementeret, så der kan programmeres parametre i køretøjsenheden.

Tabel 1

Oversigtstabel over serviceidentifikatorer

			Diagnosesession		
Navn på diagnoseservice	Punkt nr.	Værdi af Sid anmodning	SD	ECUAS	ECUPS
StartCommunication	4.1	81	■	■	■
StopCommunication	4.2	82	■		
TesterPresent	4.3	3E	■	■	■
StartDiagnosticSession	5.1	10	■	■	■
SecurityAccess	5.2	27	■	■	■
ReadDataByIdentifier	6.1	22	■	■	■
WriteDataByIdentifier	6.2	2E			■
InputOutputControlByIdentifier	7.1	2F		■	

■ Dette symbol angiver, at servicen er obligatorisk i denne diagnose-session.
Hvis der ikke er noget symbol, er servicen ikke er tilladt i denne diagnose-session.

3.2. **Svarkoder**

Svarkoder er defineret for hver service.

4. KOMMUNIKATIONSSERVICER

Visse servicer er nødvendige til at etablere og opretholde kommunikation. De figurerer ikke i applikationslaget. De tilgængelige servicer beskrives i følgende tabel:

Tabel 2

Kommunikationsservicer

Servicens navn	Beskrivelse
StartCommunication	Klienten anmoder om påbegyndelse af en kommunikationssession med en server
StopCommunication	Klienten anmoder om at standse den aktuelle kommunikationssession
TesterPresent	Klienten angiver over for serveren, at den stadig er til stede

CPR_005 Servicen StartCommunication anvendes til at begynde en kommunikation. For enhver service gælder, at kommunikationen skal være initialiseret og kommunikationsparametrene skal være passende til den pågældende funktionsmåde.

4.1. **Servicen StartCommunication**

CPR_006 Ved modtagelse af en StartCommunication indikation skal køretøjsenheden kontrollere, om den ønskede dataforbindelse kan initialiseres under de aktuelle betingelser. De gældende betingelser for initialisering af en dataforbindelse er beskrevet i dokument ISO 14230-2.

CPR_007 Derefter skal køretøjsenheden udføres alle de operationer, som er nødvendige for at initialisere dataforbindelsen og sende et StartCommunication svar, hvor parametre for positivt svar er valgt.

CPR_008 Hvis en køretøjsenhed, som i forvejen er initialiseret (og har påbegyndt en diagnose-session uanset hvilken), modtager en ny StartCommunication anmodning (f.eks. pga. fejlafhjælpning i testeren), skal anmodningen accepteres, og køretøjsenheden skal reinitialiseres.

CPR_009 Hvis dataforbindelsen af en eller grund ikke kan initialiseres, skal køretøjsenheden fortsætte med at fungere som den gjorde umiddelbart før forsøget på at initialisere dataforbindelsen.

CPR_010 Meddelelsen med anmodningen StartCommunication skal være fysisk adresseret.

CPR_011 Initialisering af køretøjsenheden til servicer sker ved hurtig initialisering,

— forud for enhver aktivitet er en periode, hvor bussen er ledig,

— testeren sender derefter et initialiseringsmønster,

— alle oplysninger, som er nødvendige til oprettelse af dataforbindelsen, er indeholdt i svaret fra køretøjenheden.

CPR_012 Når initialisering har fundet sted,

— er alle kommunikationsparametre sat til de i tabel 4 fastlagte standardværdier i henhold til nøglebytes.

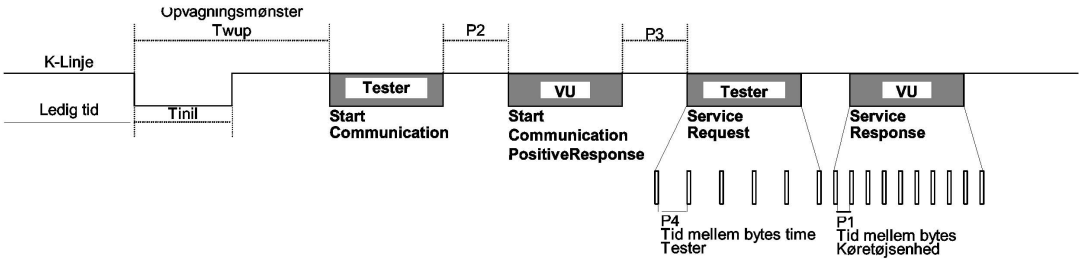
— afventer køretøjsenheden første anmodning fra testeren.

— er køretøjsenheden i sin standardfunktionsmåde for diagnose, dvs. StandardDiagnosticSession.

— er I/O-signallinjen for kalibrering i standardtilstanden, dvs. deaktiveret.

CPR_014 Datahastigheden på K-linjen skal være 10 400 Baud.

CPR_016 Hurtig initialisering igangsættes ved at testeren overfører et opvågningsmønster (Wup) på K-linjen. Efter den ledige periode på K-linjen begynder mønsteret med et kortvarigt Tinil. Testeren overfører første bit af StartCommunication servicen efter en periode med Twup, som efterfølger den første slutkant.



CPR_017 Synkroniseringsværdierne for hurtig initialisering og for meddelelser i almindelighed er givet i nedenstående tabel. Der er forskellige muligheder for den ledige tid:

— Første overførsel efter at der er tændt, Tidle = 300 ms.

— Efter afslutning af en StopCommunication Service, Tidle = P3 min.

— Efter afbrydelse af kommunikation ved tidsudkobling P3 maks, Tidle = 0.

Tabel 3

Synkroniseringsværdier for hurtig initialisering

Parameter		Minimumværdi	maksimumværdi
Tinil	25 ± 1 ms	24 ms	26 ms
Twup	50 ± 1 ms	49 ms	51 ms

Tabel 4

Synkroniseringsværdier for kommunikation

Synkronisering parameter	Parameterbeskrivelse	Nedre grænse (ms)	Øvre grænse(ms)
		min.	maks.
P1	Tid mellem bytes for svar fra køretøjsenhed	0	20
P2	Tid mellem anmodning fra tester og svar fra køretøjsenhed, eller mellem to svar fra køretøjsenhed	25	250
P3	Tid mellem slutning af svar fra køretøjsenhed og begyndelse på ny anmodning fra tester	55	5 000
P4	Tid mellem bytes for anmodning fra tester	5	20

CPR_018 Meddelelsesformatet for hurtig initialisering er givet i nedenstående tabeller.

Tabel 5

StartCommunication anmodning

Byte #	Parameternavn	Hex-værdi	Huskeværdi
#1	Formatbyte — fysisk adressering	81	FMT
#2	Adressebyte på destination	EE	TGT
#3	Adressebyte på kilde	tt	SRC
#4	Service-ID på StartCommunication anmodning	81	SCR
#5	Kontrolsum	00-FF	CS

Tabel 6

Positiv svarmeddelelse på StartCommunication

Byte #	Parameternavn	Hex-værdi	Huskeværdi
#1	Formatbyte — fysisk adressering	80	FMT
#2	Adressebyte på destination	tt	TGT
#3	Adressebyte på kilde	EE	SRC
#4	Ekstra længdebyte	03	LEN
#5	Service-ID for positivt svar på StartCommunication	C1	SCRPR
#6	Nøglebyte 1	EA	KB1
#7	Nøglebyte 2	8F	KB2
#8	Kontrolsum	00-FF	CS

CPR_019 Der findes intet negativt svar på en StartCommunication anmodning; er der ingen positiv svarmeddelelse at overføre, bliver køretøjsenheden ikke initialiseret, der overføres intet, og enheden fortsætter i normal funktionsmåde.

4.2. **StopCommunication service**

4.2.1. ***Beskrivelse af meddelelser***

Denne service er placeret i kommunikationslaget og anvendes til at afslutte en kommunikationssession.

CPR_020 Ved modtagelse af en StopCommunication indikation skal køretøjsenheden kontrollere, om kommunikationen kan afsluttes under de aktuelle betingelser. I bekræftende fald skal køretøjsenheden udføre alle de nødvendige operationer til at afslutte kommunikationen.

CPR_021 Hvis det kan lade sig gøre at afslutte kommunikationen, skal køretøjsenheden afgive et StopCommunication svar med parametre svarende til positivt svar, før kommunikationen afsluttes.

CPR_022 Hvis kommunikationen af en eller anden grund ikke kan afsluttes, skal køretøjsenheden afgive et StopCommunication svar med parameteren negativt svar.

CPR_023 Hvis køretøjsenheden registrerer tidsudkobling af P3max, skal kommunikationen afsluttes, uden at der afgives et svar.

4.2.2. ***Meddelelsesformat***

CPR_024 Meddelelsesformater for StopCommunication er givet i følgende tabeller:

Tabel 7

StopCommunication anmodning

Byte #	Parameternavn	Hex-værdi	Huskeværdi
#1	Formatbyte — fysisk adressering	80	FMT
#2	Adressebyte	EE	TGT
#3	Adressebyte på kilde	tt	SRC
#4	Ekstra længdebyte	01	LEN
#5	Service-ID på StopCommunication anmodning	82	SPR
#6	Kontrolsum	00-FF	CS

Tabel 8

Positiv svarmeddelelse på StopCommunication

Byte #	Parameternavn	Hex-værdi	Huskeværdi
#1	Formatbyte — fysisk adressering	80	FMT
#2	Adressebyte på destination	tt	TGT
#3	Adressebyte på kilde	EE	SRC
#4	Ekstra længdebyte	01	LEN
#5	Service-ID for positivt svar på StopCommunication	C2	SPRPR
#6	Kontrolsum	00-FF	CS

Tabel 9

Negativ svarmeddelelse på StopCommunication

Byte #	Parameternavn	Hex-værdi	Huskeværdi
#1	Formatbyte — fysisk adressering	80	FMT
#2	Adressebyte på destination	tt	TGT
#3	Adressebyte på kilde	EE	SRC
#4	Ekstra længdebyte	03	LEN
#5	Service-ID på negativt svar	7F	NR
#6	Service-ID på StopCommunication	82	SPR
#7	responseCode = generalReject	10	RC_GR
#8	Kontrolsum	00-FF	CS

4.2.3. ***Parameterdefinition***

Denne service kræver ingen parameterdefinition.

4.3. **TesterPresent service**

4.3.1. ***Meddelelsesbeskrivelse***

Servicen TesterPresent anvendes af testeren til at angive, at serveren stadig er til stede for at undgå at serveren automatisk returnerer til normal drift og eventuelt standser kommunikationen. Denne service, der udføres med regelmæssige mellemrum, holder diagnosesession/kommunikation aktive ved at tilbagestille P3 timeren hver gang der modtages en anmodning om denne service.

4.3.2. ***Meddelelsesformat***

CPR_079 Meddelelsesformater for TesterPresent instruktioner er angivet i følgende tabeller.

Tabel 10

TesterPresent forespørgsel

Byte #	Parameternavn	Hex-værdi	Mnemoteknisk
#1	Formatbyte — fysisk adressering	80	FMT
#2	Destinationsadressebyte	EE	TGT
#3	Kildeadressebyte	tt	SRC
#4	Byte for ekstra længde	02	LEN
#5	Identifikation af servicen TesterPresent forespørgsel	3E	TP
#6	Delfunktion = responseRequired = [ja	01	RESPREQ_Y
	Nej]	02	RESPREQ_NO
#7	Kontrolsum	00-FF	CS

CPR_080 Hvis parameteren responseRequired sættes til »ja«, skal serveren svare med følgende positive svarmeddelelse. Hvis den sættes til »nej«, kommer der intet svar fra serveren.

Tabel 11

Positiv svarmeddelelse på TesterPresent

Byte #	Parameternavn	Hex-værdi	Mnemoteknisk
#1	Formatbyte — fysisk adressering	80	FMT
#2	Destinationsadressebyte	tt	TGT
#3	Kildeadressebyte	EE	SRC
#4	Byte for ekstra længde	01	LEN
#5	Identifikation af servicen TesterPresent forespørgsel	7E	TPPR
#6	Kontrolsum	00-FF	CS

CPR_081 Servicen skal understøtte følgende negative svarkoder:

Table 12

Negativ svarmeddelelse på TesterPresent

Byte #	Parameternavn	Hex Value	Mnemonic
#1	Formatbyte — fysisk adressering	80	FMT
#2	Destinationsadressebyte	tt	TGT
#3	Kildeadressebyte	EE	SRC
#4	Byte for ekstra længde	03	LEN
#5	Identifikation af servicen negativt svar	7F	NR
#6	Identifikation af servicen TesterPresent forespørgsel	3E	TP
#7	responseCode = [SubFunctionNotSupported-InvalidFormat	12	RC_SFNS_IF
	incorrectMessageLength]	13	RC_IML
#8	Kontrolsum	00-FF	CS

5. ADMINISTRATIONSSERVICER

De tilgængelige servicer beskrives i følgende tabel:

Tabel 13

Administrationsservicer

Servicens navn	Beskrivelse
StartDiagnosticSession	Klienten anmoder om at påbegynde en diagnose-session med en VU
SecurityAccess	Klienten anmoder om adgang til funktioner, som er forbeholdt autoriserede brugere

5.1. **StartDiagnosticSession service**

5.1.1. ***Beskrivelse af meddelelser***

CPR_025 Servicen StartDiagnosticSession anvendes til at tillade forskellige diagnose-sessioner i serveren. En diagnose-session tillader et nærmere bestemt sæt servicer i henhold til tabel 17. En session kan for køretøjsfabrikanten åbne særlige servicer, som ikke indgår i dette dokument. Implementeringsreglerne skal være i overensstemmelse med følgende krav:

— Der skal altid være netop én aktiv diagnosesession i køretøjsenheden,

— Køretøjsenheden skal altid åbne StandardDiagnosticSession, når den startes op. Hvis der ikke påbegyndes nogen anden diagnosesession, skal StandardDiagnosticSession køre så længe køretøjsenheden er tændt.

— Har testeren anmodet om en diagnosesession som i forvejen kører, skal køretøjsenheden afgive en postiv svarmeddelelse,

— Når testeren anmoder om en ny diagnosesession, skal køretøjsenheden først sende en positiv svarmeddelelse på StartDiagnosticSession, før den nye session bliver aktiv i køretøjsenheden. Er køretøjsenheden ikke i stand til at starte den anmodede nye diagnosesession, skal den svare med en negativ svarmeddelelse på StartDiagnosticSession, og den aktuelle session skal fortsætte.

CPR_026 En diagnose-session må kun påbegyndes, hvis der er etableret kommunikation mellem klienten og køretøjsenheden.

CPR_027 Efter en vellykket StartDiagnosticSession med diagnosticSession parameteren sat til »StandardDiagnsticSession« i anmodningsmeddelelsen skal de i tabel 4 angivne synkroniseringsparametre være aktive, hvis en anden diagnose-session i forvejen var aktiv.

5.1.2. ***Meddelelsesformat***

CPR_028 Meddelelsesformaterne for StartDiagnosticSession er givet i følgende tabeller.

Tabel 14

StartDiagnosticSession anmodning

Byte #	Parameternavn	Hex-værdi	Huskeværdi
#1	Formatbyte — fysisk adressering	80	FMT
#2	Adressebyte på destination	EE	TGT
#3	Adressebyte på kilde	tt	SRC
#4	Ekstra længdebyte	02	LEN
#5	Service-ID på StartDiagnosticSession anmodning	10	STDS
#6	diagnosticSession = [én værdi fra tabel 17]	xx	DS_. . .
#7	Kontrolsum	00-FF	CS

Tabel 15

Positiv svarmeddelelse på StartDiagnosticSession

Byte #	Parameternavn	Hex-værdi	Huskeværdi
#1	Formatbyte — fysisk adressering	80	FMT
#2	Adressebyte på destination	tt	TGT
#3	Adressebyte på kilde	EE	SRC
#4	Ekstra længdebyte	02	LEN
#5	Service-ID for positivt svar på StartDiagnosticSession	50	STDSPR
#6	DiagnosticSession = [samme værdi som i byte #6 tabel 14]	xx	DS_. . .
#7	Kontrolsum	00-FF	CS

Tabel 16

Negativ svarmeddelelse på StartDiagnosticSession

Byte #	Parameternavn	Hex-værdi	Huskeværdi
#1	Formatbyte — fysisk adressering	80	FMT
#2	Adressebyte på destination	tt	TGT
#3	Adressebyte på kilde	EE	SRC
#4	Ekstra længdebyte	03	LEN
#5	Service-ID på negativt svar	7F	NR
#6	Service-ID på StartDiagnosticSession anmodning	10	STDS
#7	ResponseCode = [subFunctionNotSupported ([a])	12	RC_SFNS
	incorrectMessageLength ([b])	13	RC_IML
	conditionsNotCorrect ([c])]	22	RC_CNC
#8	Kontrolsum	00-FF	CS

([a]) Værdien indsat i byte #6 af anmodningsmeddelelsen understøttes ikke, dvs. findes ikke i tabel 17.
([b]) Meddelelsens længde er forkert.
([c]) Kriterierne for anmodningen StartDiagnosticSession er ikke opfyldt.

5.1.3. ***Parameterdefinition***

CPR_029 Parameteren diagnosticSession (DCS_) anvendes af StartDiagnosticSession servicen til at vælge en nærmere bestemt adfærd af serveren (serverne). Følgende diagnose-sessioner beskrives i dette dokument:

Tabel 17

Fastlæggelse af værdier for diagnosticSession

Hex	Beskrivelse	Huskeværdi
81	StandardDiagnosticSession Denne diagnose-session tillader alle servicer i tabel 1 kolonne 4 »SD«. Disse servicer giver mulighed for læsning af data fra en server (køretøjsenhed). Denne diagnose-session er aktiv efter vellykket initialisering mellem klient (tester) og server (køretøjsenhed). Denne diagnose-session kan overskrives af andre diagnose-sessioner, som foreskrives i dette afsnit.	SD
85	ECUProgrammingSession Denne diagnose-session giver mulighed for alle servicer i tabel 1 kolonne 6 »ECUPS«. Disse servicer understøtter programmering af hukommelsen på en server (køretøjsenhed). Denne diagnose-session kan overskrives af andre diagnose-sessioner, som beskrives i dette afsnit.	ECUPS
87	ECUAdjustmentSession Denne diagnose-session giver mulighed for alle servicer i tabel 1 kolonne 5 »ECUAS«. Disse servicer understøtter ind-/uddatastyring for en server (køretøjsenhed). Denne diagnose-session kan overskrives af andre diagnose-sessioner, som foreskrives i dette afsnit.	ECUAS

5.2. **SecurityAccess service**

Skrivning af kalibreringsdata eller adgang til kalibreringens ind-/uddatalinje er kun mulig, når køretøjsenheden er i CALIBRATION funktionsmåde. For at få adgang til CALIBRATION måde skal man isætte et gyldigt værkstedskort i køretøjsenheden og indlæse korrekt PIN-kode i køretøjsenheden.

SecurityAccess servicen kan anvendes til at indlæse PIN-koden og angive over for testeren, om køretøjsenheden er i funktionsmåde CALIBRATION eller ej.

Det kan godtages, at indlæsning af PIN-koden kan ske på anden måde.

5.2.1. ***Beskrivelse af meddelelser***

Sikkerhedsservicen består af en SecurityAccess »requestSeed« meddelelse, senere efterfulgt af en SecurityAccess »sendKey« meddelelse. SecurityAccess skal udføres efter StartDiagnosticSession.

CPR_033 Testeren skal anvende SecurityAccess »sendKey« meddelelsen til kontrol af, om køretøjsenheden er klar til at modtage en PIN-kode.

CPR_034 Er køretøjsenheden i forvejen i CALIBRATION måde, skal den besvare forespørgslen ved at sende et »basistal« på 0x0000 ved hjælp af servicen positivt svar på SecurityAccess.

CPR_035 Er køretøjsenheden klar til at modtage en PIN-kode med henblik på kontrol ved hjælp af et værkstedskort, skal den besvare forespørgslen ved at sende et »basistal« større end 0x0000 ved hjælp af servicen positivt svar på SecurityAccess.

CPR_036 Er køretøjsenheden ikke klar til at acceptere en PIN-kode fra testeren, enten fordi det isatte værkstedskort ikke er gyldigt, fordi der ikke er indsat et værkstedskort, eller fordi køretøjsenheden forventer PIN-koden indlæst på anden måde, skal den besvare forespørgslen med et negativt svar, hvor svarkoden er sat til conditionsNotCorrectOrRequestSequenceError.

CPR_037 Testeren skal derefter til sidst anvende servicen SecurityAccess »SendKey« meddelelse til at fremsende en PIN-kode til køretøjsenheden. For at give tid til ægthedskontrol skal køretøjsenheden anvende den negative svarkode requestCorrectlyReceived-ResponsePending for at forlænge tiden til at svare. Dog må den maksimale tid til at svare ikke være over 5 minutter. Så snart den ønskede service er udført, skal køretøjsenheden sende en positiv svarmeddelelse eller negativ svarmeddelse med en svarkode forskellig fra denne. Den negative svarkode requestCorrectlyReceived-ResponsePending kan af køretøjsenheden gentages, indtil den ønskede service er udført og den endelige svarmeddelelse sendt.

CPR_038 Køretøjsenheden skal kun besvare denne anmodning med servicen positivt svar på SecurityAccess, når den er i CALIBRATION funktionsmåde.

CPR_039 I følgende tilfælde skal køretøjsenheden besvare denne forespørgsel med et negativt svar med en svarkode sat til:

— subFunctionNot supported : Ugyldigt format af delfunktionens parameter (accessType),

— conditionsNotCorrectOrRequestSequenceError: Køretøjsenheden ikke klar til at acceptere en indtastet PIN-kode,

— invalidKey: PIN-kode ikke gyldig, og antal PIN-kodeforsøg ikke overskredet,

— exceededNumberOfAttempts: PIN-kode ikke gyldig, og antal PIN-kodeforsøg overskredet,

— generalReject: korrekt PIN-kode, men gensidig ægthedskontrol med værkstedskort ikke lykkedes.

5.2.2. ***Meddelelsesformat — SecurityAccess — requestSeed***

CPR_040 Meddelelsesformaterne for SecurityAccess »requestSeed« instruktionerne er angivet i nedenstående tabeller:

Tabel 18

SecurityAccessRequest — requestSeed meddelelse

Byte #	Parameternavn	Hex-værdi	Huskeværdi
#1	Formatbyte — fysisk adressering	80	FMT
#2	Adressebyte på destination	EE	TGT
#3	Adressebyte på kilde	tt	SRC
#4	Ekstra længdebyte	02	LEN
#5	Service-ID for SecurityAccess Request Service	27	SA
#6	accessType — requestSeed	7D	AT_RSD
#7	Kontrolsum	00-FF	CS

Tabel 19

Positiv svarmeddelelse på SecurityAccess — requestSeed

Byte #	Parameternavn	Hex-værdi	Huskeværdi
#1	Formatbyte — fysisk adressering	80	FMT
#2	Adressebyte på destination	tt	TGT
#3	Adressebyte på kilde	EE	SRC
#4	Ekstra længdebyte	04	LEN
#5	Service-ID for positivt svar på SecurityAccess	67	SAPR
#6	accessType — requestSeed	7D	AT_RSD
#7	Basistal højt	00-FF	SEEDH
#8	Basistal lavt	00-FF	SEEDL
#9	Kontrolsum	00-FF	CS

Tabel 20

Negativ svarmeddelelse på SecurityAccess — sendKey

Byte #	Parameternavn	Hex-værdi	Huskeværdi
#1	Formatbyte — fysisk adressering	80	FMT
#2	Adressebyte på destination	tt	TGT
#3	Adressebyte på kilde	EE	SRC
#4	Ekstra længdebyte	03	LEN
#5	Service-ID for negativeResponse	7F	NR
#6	Service-ID for SecurityAccessRequest	27	SA
#7	responseCode = [conditionsNotCorrectOrRequestSequenceError	22	RC_CNC
	incorrectMessageLength]	13	RC_IML
#8	Kontrolsum	00-FF	CS

5.2.3. ***Meddelelsesformat — SecurityAccess — sendKey***

CPR_041 Meddelelsesformaterne for SecurityAccess »sendKey« instruktioner er givet i nedenstående tabeller:

Tabel 21

SecurityAccess anmodning — sendKey meddelelse

Byte #	Parameternavn	Hex-værdi	Huskeværdi
#1	Formatbyte — fysisk adressering	80	FMT
#2	Adressebyte på destination	EE	TGT
#3	Adressebyte på kilde	tt	SRC
#4	Ekstra længdebyte	m+2	LEN
#5	Service-Id på SecurityAccess anmodning	27	SA
#6	accessType — sendKey	7E	AT_SK
#7 bis #m+6	Nøgle #1 (høj)	xx	NØGLE
	. . .	. . .	
	Nøgle #m (lav, m skal være mindst 4 og højst 8)	xx	
#m+7	Kontrolsum	00-FF	CS

Tabel 22

Positivt svar på SecurityAccess — sendKey

Byte #	Parameternavn	Hex-værdi	Huskeværdi
#1	Formatbyte — fysisk adressering	80	FMT
#2	Adressebyte på destination	tt	TGT
#3	Adressebyte på kilde	EE	SRC
#4	Ekstra længdebyte	02	LEN
#5	Service-ID for positivt svar på SecurityAccess	67	SAPR
#6	accessType — sendKey	7E	AT_SK
#7	Kontrolsum	00-FF	CS

Tabel 23

Negativ svarmeddelelse på SecurityAccess

Byte #	Parameternavn	Hex-værdi	Huskeværdi
#1	Formatbyte — fysisk adressering	80	FMT
#2	Adressebyte på destination	tt	TGT
#3	Adressebyte på kilde	EE	SRC
#4	Ekstra længdebyte	03	LEN
#5	Service-ID på NegativeResponse	7F	NR
#6	Service-Id på SecurityAccess anmodning	27	SA
#7	ResponseCode = [generalReject	10	RC_GR
	subFunctionNotSupported	12	RC_SFNS
	incorrectMessageLength	13	RC_IML
	conditionsNotCorrectOrRequestSequenceError	22	RC_CNC
	invalidKey	35	RC_IK
	exceededNumberOfAttempts	36	RC_ENA
	requestCorrectlyReceived-ResponsePending]	78	RC_RCR_RP
#8	Kontrolsum	00-FF	CS

6. DATAOVERFØRSELSSERVICER

De servicer, som er til rådighed, er beskrevet i følgende tabel:

Tabel 24

Dataoverførselsservicer

Servicens navn	Beskrivelse
ReadDataByIdentifier	Klienten anmoder om overførsel af den aktuelle værdi af en post med adgang gennem recordDataIdentifier.
WriteDataByIdentifier	Klienten anmoder om at skrive en post, hvortil der er adgang gennem recordDataIdentifier

6.1. **ReadDataByIdentifier service**

6.1.1. ***Beskrivelse af meddelelser***

CPR_050 Servicen ReadDataByIdentifier anvendes af klienten til at skrive recordValues (dataværdier) fra en server. Data identificeres af en recordDataIdentifier. Fabrikanten af køretøjsenheden har ansvaret for, at de for serveren gældende betingelser er opfyldt ved udførelse af denne service.

6.1.2. ***Meddelelsesformat***

CPR_051 Meddelelsesformaterne for ReadDataByIdentifier instruktioner er givet i følgende tabeller.

Tabel 25

ReadDataByIdentifier anmodning

Byte #	Parameternavn	Hex-værdi	Huskeværdi
#1	Formatbyte - fysisk adressering	80	FMT
#2	Adressebyte på destination	EE	TGT
#3	Adressebyte på kilde	tt	SRC
#4	Ekstra længdebyte	03	LEN
#5	Service-ID på ReadDataByIdentifier anmodning	22	RDBI
#6 bis #7	RecordDataIdentifier = [en værdi fra tabel 28]	xxxx	RDI_. . .
#8	Kontrolsum	00-FF	CS

Tabel 26

Positivt svar på ReadDataByIdentifier

Byte #	Parameternavn	Hex-værdi	Huskeværdi
#1	Formatbyte — fysisk adressering	80	FMT
#2	Adressebyte på destination	tt	TGT
#3	Adressebyte på kilde	EE	SRC
#4	Ekstra længdebyte	m+3	LEN
#5	Service-ID for positivt svar på ReadDataByIdentifier	62	RDBIPR
#6 and #7	recordDataIdentifier = [samme værdi som byte #6 og #7 tabel 25]	xxxx	RDI_. . .
#8 til #m+7	dataRecord[] = [data#1 : data#m]	xx : xx	DREC_DATA1 : DREC_DATAm
#m+8	Kontrolsum	00-FF	CS

Tabel 27

Negativ svarmeddelelse på ReadDataByIdentifier

Byte #	Parameternavn	Hex-værdi	Huskeværdi
#1	Formatbyte — fysisk adressering	80	FMT
#2	Adressebyte på destination	tt	TGT
#3	Adressebyte på kilde	EE	SRC
#4	Ekstra længdebyte	03	LEN
#5	Service-ID på NegativeResponse	7F	NR
#6	Service-ID på ReadDataByIdentifier anmodning	22	RDBI
#7	ResponseCode = [requestOutOfRange incorrectMessageLength conditionsNotCorrect]	31 13 22	RC_ROOR RC_IML RC_CNC
#8	Kontrolsum	00-FF	CS

6.1.3. ***Parameterdefinition***

CPR_052 Parameteren recordDataIdentifier (RDI_) i anmodningen ReadDataByIdentifier identificerer en datapost.

CPR_053 De værdier af recordDataIdentifier, som defineres af dette dokument, er vist i tabellen nedenfor.

Tabellen recordDataIdentifier består af tre søjler og mange linjer.

— Søjle 1 indeholder den »Hex-værdi« der er tilordnet den i søjle 3 angivne recordDataIdentifier.

— Søjle 2 (dataelement) fastlægger det dataelement i tillæg 1, som er knyttet til recordDataIdentifier (omkodning er undertiden nødvendig).

— Søjle 3 (beskrivelse) angiver navnet på den tilsvarende recordDataIdentifier.

— Søjle 4 (huskeværdi) angiver huskeværdien af denne recordDataIdentifier.

Tabel 28

Definition af recordDataIdentifier værdier

Hex	Dataelement	ecordDataIdentifier Name (se format i punkt 8.2)	Huskeværdi
F90B	CurrentDateTime	TimeDate	RDI_TD
F912	HighResOdometer	HighResolutionTotalVehicleDistance	RDI_HRTVD
F918	K-ConstantOfRecordingEquipment	Kfactor	RDI_KF
F91C	L-TyreCircumference	LfactorTyreCircumference	RDI_LF
F91D	W-VehicleCharacteristicConstant	WvehicleCharacteristicFactor	RDI_WVCF
F921	TyreSize	TyreSize	RDI_TS
F922	nextCalibrationDate	NextCalibrationDate	RDI_NCD
F92C	SpeedAuthorised	SpeedAuthorised	RDI_SA
F97D	vehicleRegistrationNation	RegisteringMemberState	RDI_RMS
F97E	VehicleRegistrationNumber	VehicleRegistrationNumber	RDI_VRN
F190	VehicleIdentificationNumber	VIN	RDI_VIN

CPR_054 Parameteren dataRecord (DREC_) anvendes af den positive svarmeddelelse på ReadDataByIdentifier til at hente den datapost, der er identificeret ved recordDataIdentifier, til klienten (testeren). Dataformater er fastlagt i punkt 8. Der kan fastlægges andre dataposter, som brugeren frivilligt kan benytte, herunder køretøjsenhedsspecifikke inddata, interne data og uddata, men disse er ikke defineret i dette dokument.

6.2. **WriteDataByIdentifier service**

6.2.1. ***Beskrivelse af meddelelser***

CPR_056 Servicen WriteDataByIdentifier anvendes af klienten til at skrive dataværdier til en server. Data identificeres af en recordDataIdentifier. Fabrikanten af køretøjsenheden har ansvaret for, at de for serveren gældende betingelser er opfyldt ved udførelse af denne service. For at opdatere parametrene i tabel 28 skal køretøjsenheden være i CALIBRATION funktionsmåde.

6.2.2. ***Meddelelsesformat***

CPR_057 Meddelelsesformaterne for WriteDataByIdentifier instruktioner er givet i nedenstående tabeller.

Tabel 29

WriteDataByIdentifier anmodning

Byte #	Parameternavn	Hex-værdi	Huskeværdi
#1	Formatbyte — fysisk adressering	80	FMT
#2	Adressebyte på destination	EE	TGT
#3	Adressebyte på kilde	tt	SRC
#4	Ekstra længdebyte	m+3	LEN
#5	Service-ID på WriteDataByIdentifier anmodning	2E	WDBI
#6 til #7	recordDataIdentifier = [en værdi fra tabel 28]	xxxx	RDI_. . .
#8 til m+7	dataRecord[] = [data#1 : data#m]	xx : xx	DREC_DATA1 : DREC_DATAm
#m+8	Kontrolsum	00-FF	CS

Tabel 30

Positivt svar på WriteDataByIdentifier

Byte #	Parameternavn	Hex-værdi	Huskeværdi
#1	Formatbyte — fysisk adressering	80	FMT
#2	Adressebyte på destination	tt	TGT
#3	Adressebyte på kilde	EE	SRC
#4	Ekstra længdebyte	03	LEN
#5	Service-ID for positivt svar på WriteDataByIdentifier	6E	WDBIPR
#6 til #7	recordDataIdentifier = [samme værdi som byte #6 og #7 tabel 29]	xxxx	RDI_. . .
#8	Kontrolsum	00-FF	CS

Tabel 31

Negativ svarmeddelelse på WriteDataByIdentifier

Byte #	Parameternavn	Hex-værdi	Huskeværdi
#1	Formatbyte — fysisk adressering	80	FMT
#2	Adressebyte på destination	tt	TGT
#3	Adressebyte på kilde	EE	SRC
#4	Ekstra længdebyte	03	LEN
#5	Service-ID på NegativeResponse	7F	NR
#6	Service-ID på WriteDataByIdentifier anmodning	2E	WBDI
#7	ResponseCode = [requestOutOfRange	31	RC_ROOR
	incorrectMessageLength	13	RC_IML
	conditionsNotCorrect]	22	RC_CNC
#8	Kontrolsum	00-FF	CS

6.2.3. ***Parameterdefinition***

Parameteren recordDataIdentifier (RDI_) er defineret i tabel 28.

Parameteren dataRecord (DREC_) anvendes i anmodningen ReadDataByIdentifier til at hente de dataværdier, der er identificeret ved recordDataIdentifier, til serveren (køretøjsenheden). Dataformater er fastlagt i punkt 8.

7. KONTROL AF TESTIMPULSER — FUNKTIONSENHED FOR IND-/UDDATA STYRING

I følgende tabel beskrives de servicer, som er til rådighed:

Tabel 32

Funktionel enhed for ind-/uddatastyring

Servicens navn	Beskrivelse
InputOutputControlByIdentifier	Klienten anmoder om at måtte styre et sæt serverspecifikke ind-/uddata.

7.1. **InputOutputControlByIdentifier service**

7.1.1. ***Beskrivelse af meddelelser***

Testimpulser kan styres eller overvåges ved hjælp af en passende tester, som tilsluttes via det forreste stik.

CPR_058 Denne I/O signallinje for kalibrering kan konfigureres med ordrer over K-linjen ved hjælp af servicen InputOutputControlByIdentifier, med hvilken man vælger den ønskede ind- eller udlæsningsfunktion for linjen. Linjen kan have følgende status:

— frakoblet,

— speedSignalInput, hvor der gennem I/O signallinjen for kalibrering tilføres et hastighedssignal (testsignal), som erstatter hastighedssignalet fra bevægelsesføleren,

— realTimeSpeedSignalOutputSensor, hvor der gennem I/O signallinjen for kalibrering afgives et hastighedssignal fra bevægelsesføleren.

— RTCOutput, hvor der gennem I/O signallinjen for kalibrering afgives et UTC kloksignal.

CPR_059 Køretøjsenheden skal have indledt en justeringssession og skal være i CALIBRATION funktionsmåde for at linjens tilstand kan konfigureres. Når køretøjsenheden forlader justeringssession eller CALIBRATION funktionsmåde, skal den stille I/O signallinjen for kalibrering tilbage i »deaktiveret« tilstand (standardtilstanden).

CPR_060 Hvis der modtages hastighedsimpulser på køretøjsenhedens indgangslinje for tidstro hastighedssignal, mens I/O signallinjen for kalibrering er stillet på indgang, vil I/O-signallinjen blive stillet på udgang eller ført tilbage i deaktiveret tilstand.

CPR_061 Sekvensen skal være:

— Der oprettes kommunikation med StartCommunication servicen

— der åbnes en justeringssession med StartDiagnosticSession servicen og benyttes CALIBRATION måde (rækkefølgen af disse to operationer har ikke betydning).

— Tilstanden af uddata ændres med InputOutputControlByIdentifier servicen.

7.1.2. ***Meddelelsesformat***

CPR_062 Meddelelsesformaterne af InputOutputControlByIdentifier instruktionerne er givet i følgende tabeller.

Tabel 33

InputOutputControlByIdentifier anmodning

Byte #	Parameternavn	Hex-værdi	Huskeværdi
#1	Formatbyte — fysisk adressering	80	FMT
#2	Adressebyte på destination	EE	TGT
#3	Adressebyte på kilde	tt	SRC
#4	Ekstra længdebyte	xx	LEN
#5	Sid for InputOutputControlByIdentifier anmodning	2F	IOCBI
#6 and #7	InputOutputIdentifier = [CalibrationInputOutput]	F960	IOI_CIO
#8 eller #8 til #9	ControlOptionRecord = [		COR_. . .
	inputOutputControlParameter — én værdi fra tabel 36	xx	IOCP_. . .
	controlState — én værdi tabel 37 (se bemærkning nedenfor)]	xx	CS_. . .
#9 eller #10	Kontrolsum	00-FF	CS

Bemærkning: Parameteren controlState findes kun i visse tilfælde (se 7.1.3).

Tabel 34

Positiv svarmeddelelse på InputOutputControlByLocalIdentifier

Byte #	Parameternavn	Hex-værdi	Huskeværdi
#1	Formatbyte — fysisk adressering	80	FMT
#2	Adressebyte på destination	tt	TGT
#3	Adressebyte på kilde	EE	SRC
#4	Ekstra længdebyte	xx	LEN
#5	SId for positivt svar på inputOutputControlByIdentifier	6F	IOCBIPR
#6 and #7	inputOutputIdentifier = [CalibrationInputOutput]	F960	IOI_CIO
#8 eller #8 til #9	controlStatusRecord = [		CSR_
	inputOutputControlParameter (samme værdi som byte #8 tabel 33)	xx	IOCP_. . .
	controlState (samme værdi som byte #9 tabel 33)] (i givet fald)	xx	CS_. . .
#9 eller #10	Kontrolsum	00-FF	CS

Tabel 35

Negativ svarmeddelelse på InputOutputControlByIdentifier

Byte #	Parameternavn	Hex-værdi	Huskeværdi
#1	Formatbyte — fysisk adressering	80	FMT
#2	Adressebyte på destination	tt	TGT
#3	Adressebyte på kilde	EE	SRC
#4	Ekstra længdebyte	03	LEN
#5	Service-ID på negativeResponse	7F	NR
#6	Sid for anmodning om inputOutputControlByIdentifier	2F	IOCBI
#7	responseCode = [		
	incorrectMessageLength	13	RC_IML
	conditionsNotCorrect	22	RC_CNC
	requestOutOfRange	31	RC_ROOR
	deviceControlLimitsExceeded]	7A	RC_DCLE
#8	Kontrolsum	00-FF	CS

7.1.3. ***Parameterdefinition***

CPR_064 Parameteren inputOutputLocalIdentifier (IOCP_) er defineret i følgende tabel:

Tabel 36

Fastlæggelse af værdier af inputOutputControlParameter

Hex	Beskrivelse	Huskeværdi
00	ReturnControlToECU Denne værdi angiver over for serveren (køretøjsenheden), at testeren ikke længere kontrollerer ind/ud signallinjen for kalibrering.	RCTECU
01	ResetToDefault Denne værdi skal anmode serveren (køretøjsenheden) om at tilbagestille ind/ud signallinjen for kalibrering til dets standardtilstand.	RTD
03	ShortTermAdjustment Denne værdi skal fortælle serveren (køretøjsenheden), at den anmodes om at justere ind/ud signallinjen for kalibrering til den værdi, som er indeholdt i controlState parameteren.	STA

CPR_065 Parameteren controlState, som kun er tilstede, når inputOutputControlParameter er sat til ShortTermAdjustment, er fastlagt i følgende tabel:

Tabel 37

Definition af controlState-værdier

Funktionsmåde	Hex-værdi	Beskrivelse
Deaktivér	00	I/O-linjen er deaktiveret (standardtilstand)
Aktivér	01	Aktivér ind/ud linje for kalibrering som speedSignalInput
Aktivér	02	Aktivér ind/ud linje for kalibrering som realTimeSpeedSignalOutputSensor
Aktivér	03	Aktivér ind/ud linje for kalibrering som RTCOutput

8. FORMATER PÅ DATARECORDS

Dette punkt angiver:

— generelle regler, som gælder for områderne for de parametre, som overføres af køretøjsenheden til testeren,

— formater som skal anvendes til data, som overføres med de datatransmissionsservicer, der er beskrevet i punkt 6.

CPR_067 Alle angivne parametre skal være understøttet af køretøjsenheden.

CPR_068 De data, som overføres af køretøjsenheden til testeren som svar på en forespørgselsmeddelelse, skal være af den målte type (dvs. den aktuelle værdi af den anmodede parameter, således som den måles eller observeres af køretøjsenheden).

8.1. **Værdiområder for overførte parametre**

CPR_069 Tabel 38 fastlægger de områder, som anvendes til at bestemme gyldigheden af en overført parameter.

CPR_070 Værdierne i området »fejlindikator« giver køretøjsenheden mulighed for øjeblikkelig at angive, at der som følge af en fejl i kontrolapparatet ikke aktuelt forefindes gyldige parameterværdier.

CPR_071 Værdierne i området »forefindes ikke« giver køretøjsenheden mulighed for at overføre en meddelelse, som indeholder en parameter, som ikke er til rådighed eller ikke understøttes i den pågældende programenhed. Værdierne i området »ikke anmodet« giver en enhed mulighed for at overføre en kommandomeddelelse og fastlægge de parametre, for hvilke der ikke forventes noget svar fra den modtagende enhed.

CPR_072 Hvis der som følge af komponentsvigt ikke kan overføres gyldige data for en parameter, skal fejlindikatoren som beskrevet i tabel 38 anvendes i stedet for den pågældende parameters data. Men hvis de målte og beregnede data har resulteret i en værdi, som er gyldig, men falder uden for det fastlagte parameterområde, bør fejlindikatoren ikke benyttes. Data bør overføres med den pågældende minimum- eller maksimumværdi af parameteren.

Tabel 38

områder for dataRecords

Områdenavn	1 byte (Hex-værdi)	2 byte (Hex-værdi)	4 byte (Hex-værdi)	ASCII
Gyldigt signal	00 til FA	0000 til FAFF	00000000 til FAFFFFFF	1 til 254
Parameterspecifik indikator	FB	FB00 til FBFF	FB000000 til FBFFFFFF	intet
Område reserveret fremtidige indikatorbit	FC til FD	FC00 til FDFF	FC000000 til FDFFFFFF	intet
Fejlindikator	FE	FE00 til FEFF	FE000000 til FEFFFFFF	0
Foreligger ikke eller er ikke anmodet	FF	FF00 til FFFF	FF000000 til FFFFFFFF	FF

CPR_073 For parametre kodet i ASCII skal ASCII-tegnet »*« reserveres som skilletegn.

8.2. **formater til dataRecords**

Tabel 39 til tabel 42 nedenfor angiver de formater, som skal anvendes via servicerne ReadDataByIdentifier og WriteDataByIdentifier.

CPR_074 Tabel 39 giver længde, opløsning og arbejdsområde for hver parameter, som er identificeret ved sin recordDataIdentifier:

Tabel 39

Format af dataRecords

Parameternavn	Datalængde (byte)	Opløsning	Arbejdsområde
TimeDate	8	Se nærmere i tabel 40	
HighResolutionTotalVehicleDistance	4	forstærkning 5 m/bit, forskydning 0 m	0 til + 21 055 406 km
Kfactor	2	forstærkning 0,001 impulser/m/bit, forskydning 0	0 til 64 255 impulser/m
LfactorTyreCircumference	2	forstærkning 0,125 10^{-3} m/bit, forskydning 0	0 til 8 031 m
WvehicleCharacteristicFactor	2	forstærkning 0,001 impulser/m/bit, forskydning 0	0 til 64 255 impulser/m
TyreSize	15	ASCII	ASCII
NextCalibrationDate	3	Se nærmere i tabel 41	
SpeedAuthorised	2	forstærkning 1/256 km/h/bit, forskydning 0	0 til 250 996 km/h
RegisteringMemberState	3	ASCII	ASCII
VehicleRegistrationNumber	14	Se nærmere i tabel 42	
VIN	17	ASCII	ASCII

CPR_075 Tabel 40 angiver formater for de forskellige byte i TimeDate parameteren:

Tabel 40

Detaljeret format af TimeDate (recordDataIdentifier værdi # F00B)

Byte	Parameterdefinition	Opløsning	Arbejdsområde
1	Sekunder	Forstærkning 0,25 s/bit, forskydning 0 s	0 til 59,75 s
2	Minutter	Forstærkning 1 min/bit, forskydning 0 min	0 til 59 min
3	Timer	Forstærkning 1 h/bit, forskydning 0 h	0 til 23 h
4	Måned	Forstærkning 1 måned/bit, forskydning 0 måned	1 til 12 måneder
5	Dag	Forstærkning 0,25 dag/bit, forskydning 0 dage (se bemærkning under tabel 41)	0,25 til 31,75 dage
6	År	Forstærkning 1 år/bit, forskydning +1985 år se bemærkning under tabel 41	år 1985 til 2235
7	Lokal forskydning, minutter	Forstærkning 1 min/bit, forskydning — 125 min	– 59 til 59 min
8	Forskydning af lokalt timetal	Forstærkning 1 h/bit, forskydning — 125 h	– 23 til + 23 h

CPR_076 Tabel 41 angiver formater for de forskellige byte i NextCalibrationDate parameteren:

Tabel 41

Detaljeret format af NextCalibrationDate (recordDataIdentifier værdi # F022)

Byte	Parameterdefinition	Opløsning	Arbejdsområde
1	Måned	Forstærkning 1 måned/bit, forskydning 0 måned	1 til 12 måneder
2	Dag	Forstærkning 0,25 dag/bit, forskydning 0 dage (se Bemærkning nedenfor)	0,25 til 31,75 dage
3	År	Forstærkning 1 år/bit, forskydning +1985 år (se Bemærkning nedenfor)	år 1985 til 2235

Bemærkning vedrørende brug af parameteren »Dag«:
1. En værdi på 0 for datoen er ugyldig. Værdierne 1, 2, 3 og 4 anvendes til at angive første dag i måneden; 5, 6, 7 og 8 angiver anden dag i måneden, osv.
2. Denne parameter kan ikke påvirke eller ændre ovenstående timeparameter.

Bemærkning vedrørende brug af parameterbyten »År«:
En værdi på 0 for året angiver år 1985; en værdi på 1 angiver år 1986, osv.

CPR_078 Tabel 42 angiver formater for de forskellige byte i VehicleRegistrationNumber parameteren:

Tabel 42

Detaljeret format af VehicleRegistrationNumber (recordDataIdentifier værdi # F07E)

Byte	Parameterdefinition	Opløsning	Arbejdsområde
1	Tegntabel (som fastlagt i tillæg 1)	ASCII	01 til 0A
2 til 14	Køretøjets indregistreringsnummer (som defineret i tillæg 1)	ASCII	ASCII

Tillæg 9

TYPEGODKENDELSE — LISTE OVER MINDSTEKRAV TIL PRØVER

1. INDLEDNING

1.1. **Typegodkendelse**

EF-typegodkendelse for kontrolapparater (eller komponenter dertil) eller fartskriverkort bygger på:

— en sikkerhedsattestering, som udføres af en ITSEC-myndighed efter et sikkerhedsmål, som er i fuld overensstemmelse med tillæg 10 til dette bilag,

— en funktionel attestering, som udføres af en medlemsstats myndigheder, og ved hvilken det attesteres, at den afprøvede genstand opfylder forskrifterne i dette bilag hvad angår udførte funktioner, målenøjagtighed og miljøegenskaber,

— en interoperabilitetsattestering, som udføres af den kompetente myndighed, og som certificerer, at kontrolapparatet (eller fartskriverkortet) er gensidigt fuldt kompatibelt med den nødvendige type fartskriverkort (eller kontrolapparat) (se kapitel VIII i dette bilag).

I tillægget foreskrives det, hvilke prøver der som minimum skal udføres af medlemsstatens myndigheder ved funktionsprøverne, og hvilke prøver, der som minimum skal udføres af de kompetente myndigheder under interoperabilitetsprøverne. Der er ingen yderligere forskrifter for de procedurer, som skal følges ved udførelse af prøverne eller den pågældende type prøver.

Spørgsmål vedrørende sikkerhedsattestering er ikke omfattet af dette tillæg. Såfremt nogle af de prøver, som kræves til typegodkendelse, udføres som led i sikkerhedsvurdering og -attestering, behøver disse prøver ikke udføres igen. I så fald er det tilstrækkeligt kun at kontrollere resultaterne af disse sikkerhedsprøver. De krav, som der forventes prøvet for (eller nært beslægtede prøver foretaget) som led i sikkerhedsattesteringen, er mærket med »*« i tillægget.

I dette bilag er særskilt omhandlet typegodkendelse af bevægelsesfølere og køretøjsenhed som komponenter i kontrolapparatet. Indbyrdes kompatibilitet mellem hver type bevægelsesfølere og hver type køretøjsenhed kræves ikke, hvorfor typegodkendelse af en bevægelsesfølere kun kan ske i kombination med typegodkendelse af en køretøjsenhed og omvendt.

1.2. **Henvisninger**

I dette tillæg henvises til følgende referencer:

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 Vibrations wide band — Reprodutibility High. Modification 1: 1983.
IEC 529	Degrees of protection provided by enclosures (IP code). Edition 2: 1989.
IEC 61000-4-2	Electromagnetic Compatibility (EMC) — Testing and measurement techniques — Electrostatic discharge immunity test: 1995/Amendment 1: 1998
ISO 7637-1	Road vehicles — Electrical disturbance by conduction and coupling — Part 1: Passenger cars and light commercial vehicles with nominal 12 V supply voltage — Electrical transient conduction along supply lines only. Edition 2: 1990.

ISO 7637-2 Road vehicles — Electrical disturbance by conduction and coupling — Part 2: Commercial vehicles with nominal 24 V supply voltage — Electrical transient conduction along supply lines only. First edition: 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 Identification cards — Integrated circuit(s) cards with contacts — Part 1: Physical characteristics. First edition: 1998.

ISO/IEC 7816-2 Information technology — Identification cards — Integrated circuit(s) cards with contacts — Part 2: Dimensions and location of the contacts. First edition: 1999.

ISO/IEC 7816-3 Information technology — Identification cards — Integrated circuit(s) cards with contacts — Part 3: Electronic signals and transmission protocol. Edition 2: 1997.

ISO/IEC 10373 Identification cards — Test methods. First edition: 1993.

2. FUNKTIONSPRØVER FOR KØRETØJSENHED

Nej	Prøve	Beskrivelse	Tilknyttede krav
1.	**Administrativ undersøgelse**		
1.1.	Dokumentation	Dokumentationens korrekthed	
1.2.	Fabrikantens prøvningsresultater	Resultater af fabrikantens prøvning, udført med kombination. Eftervisning på papir	070, 071, 073
2.	**Besigtigelse**		
2.1.	Overensstemmelse med dokumentationen		
2.2.	Identifikation/mærkning		168, 169
2.3.	Materialer		163 til 167
2.4.	Plombering		251
2.5.	Eksterne grænseflader		
3.	**Funktionsprøver**		
3.1.	Ydede funktioner		002, 004, 244
3.2.	Funktionsmåder		006*, 007*, 008*, 009*, 106, 107
3.3.	Funktioner og ret til dataadgang		010*, 011*, 240, 246, 247
3.4.	Overvågning af isætning og udtagning af kort		013, 014, 015*, 016*, 106
3.5.	Måling af hastighed og tilbagelagt afstand		017 til 026
3.6.	Tidsmåling (prøvning udført ved 20 °C)		027 til 032

Nej	Prøve	Beskrivelse	Tilknyttede krav
3.7.	Overvågning af føreraktiviteter		033 til 043, 106
3.8.	Overvågning af kørestatus		044, 045, 106
3.9.	Manuel indlæsning		046 til 050b
3.10.	Forvaltning af virksomhedslåse		051 til 055
3.11.	Overvågning af kontrolaktiviteter		056, 057
3.12.	Detektion af hændelser og/eller fejl		059 to 069, 106
3.13.	Identifikationsdata for apparat		075*, 076*, 079
3.14.	Data vedrørende isætning og udtagning af førerkort		081* til 083*
3.15.	Føreraktivitetsdata		084* til 086*
3.16.	Steddata		087* til 089*
3.17.	Kilometertællerdata		090* til 092*
3.18.	Detaljerede hastighedsdata		093*
3.19.	Data vedrørende hændelser		094*, 095
3.20.	Data vedrørende fejl		096*
3.21.	Kalibreringsdata		097*, 098*
3.22.	Tidsjusteringsdata		100*, 101*
3.23.	Kontrolaktivitetsdata		102*, 103*
3.24.	Data vedrørende virksomhedslåse		104*
3.25.	Data vedrørende dataoverførselsaktivitet		105*
3.26.	Data vedrørende særlige omstændigheder		105a*, 105b*
3.27.	Registrering og lagring på fartskriverkort		108, 109*, 109a*, 110*, 111, 112
3.28.	Visning på skærm		072, 106, 113 til 128, PIC_001, DIS_001
3.29.	Udskrivning		072, 106, 129 til 138, PIC_001, PRT_001 til PRT_012
3.30.	Advarsel		106, 139 til 148, PIC_001
3.31.	Dataoverførsel til eksterne medier		072, 106, 149 til 151
3.32.	Udlæsning af data til supplerende eksterne enheder		152, 153
3.33.	Kalibrering		154*, 155*, 156*, 245
3.34.	Tidsjustering		157*, 158*
3.35.	Fravær af forstyrrelse af ekstra funktioner		003, 269

Nej	Prøve	Beskrivelse	Tilknyttede krav
4.	**Miljøprøver**		
4.1.	Temperatur	Funktionaliteten eftervises gennem: — IEC 68-2-1, prøve Ad, med en prøvningsvarighed på 72 timer ved den lave temperatur (– 20 °C), 1 time med funktion, 1 time uden funktion, — IEC 68-2-2, prøve Bd, med en prøvningsvarighed på 72 timer ved den høje temperatur (+ 70 °C), 1 time med funktion, 1 time uden funktion Temperaturcykluser: Det kontrolleres, at køretøjsenheden kan modstå hurtige ændringer i den omgivende temperatur gennem IEC 68-2-14 prøve Na, 20 cykluser, hver med temperatur varierende fra den lave temperatur (– 20 °C) til den høje temperatur (+ 70 °C) og 2 timers fastholdelse af både den lave og den høje temperatur Et reduceret sæt prøvninger (af dem, som foreskrives i afsnit 3 af denne tabel) kan udføres ved den lave temperatur, den høje temperatur og med gennemgang af temperaturcyklu-serne	159
4.2.	Fugtighed	Det eftervises, at køretøjsenheden kan modstå en cyklisk fugtighedsprøve (varmeprøve) ved gennemgang af IEC 68-2-30, prøve Db, seks 24 timers cykluser, hvor hver temperatur varierer fra + 25 °C til + 55 °C, og hvor den relative fugtighed er 97 % ved + 25 °C og 93 % ved + 55 °C	160
4.3.	Vibration	1. Sinusvibrationer: det kontrolleres at køretøjsenheden kan modstå sinus-vibrationer med følgende egenskaber: Konstant skift mellem 5 og 11 Hz: Topværdi 10 mm konstant acceleration mellem 11 og 300 Hz: 5 g Prøvning for dette krav sker med IEC 68-2-6, prøve Fc, med en mindste prøvningsvarighed på 3 x 12 timer (12 timer for hver akseretning) 2. Tilfældige vibrationer: det kontrolleres, at køretøjsenheden kan modstå tilfæl-dige vibrationer med følgende egenskaber: Frekvens 5-150 Hz, niveau 0,02 g^2/Hz Prøvning for dette krav sker med IEC 68-2-35, prøve Ffda, med en mindste prøvningsvarighed på 3 x 12 timer (12 timer for hver akseretning), 1 time under drift, 1 time ude af drift De to ovenfor beskrevne prøvninger udføres på to forskel-lige prøveeksemplarer af den afprøvede apparattype	163
4.4.	Beskyttelse mod vand og fremmedlegemer	Det kontrolleres, at køretøjsenhedens beskyttelsesindeks i henhold til IEC 529 er mindst IP 40, når den er monteret under driftsomstændigheder på køretøjet	164, 165
4.5.	Overspændingsbeskyt-telse	Det kontrolleres at køretøjsenheden kan modstå en strøm-forsyning på: 24 V udførelse: 34 V ved + 40 °C 1 time 12 V udførelse: 17 V ved + 40 °C 1 time	161
4.6.	Beskyttelse mod omvendt polaritet	Det kontrolleres at køretøjsenheden kan modstå polvending af strømforsyningen	161
4.7.	Kortslutningsbeskyttelse	Det kontrolleres, at ind- og udgangssignaler er beskyttet mod kortslutning til strømforsyningen og til stel	161

Nej	Prøve	Beskrivelse	Tilknyttede krav
5.	**Prøver for elektromagnetisk kompatibilitet**		
5.1.	Strålingsemission og følsomhed	Overensstemmelse med direktiv 95/54/EØF	162
5.2.	Elektrostatisk udladning	Overensstemmelse med IEC 61000-4-2, ± 2 kV (niveau 1)	162
5.3.	Transient nedre ledningsoverførsel for strømforsyning	For 24 V udførelse: Overensstemmelse med ISO 7637-2: impuls 1a: Vs = – 100 V, Ri = 10 ohm impuls 2: Vs = + 100 V, Ri = 10 ohm impuls 3a: Vs = – 100 V, Ri = 50 ohm impuls 3b: Vs = + 100 V, Ri = 50 ohm impuls 4: Vs = – 16 V, Va = – 12 V, t6=100 ms impuls 5: Vs = + 120 V, Ri = 2,2 Ohm, td = 250 ms For 12 V udførelse: Overensstemmelse med ISO 7637-1: impuls 1: Vs = – 100 V, Ri = 10 ohm impuls 2: Vs = + 100 V, Ri = 10 ohm impuls 3a: Vs = – 100 V, Ri = 50 ohm Impuls 3b: Vs = + 100 V, Ri = 50 ohm impuls 4: Vs = – 6 V, Va = – 5 V, t6 = 15 ms impuls 5: Vs = + 65 V, Ri = 3 ohm, td = 100 ms Impuls 5 skal kun afprøves for køretøjsenheder bestemt til montering i køretøjer uden ekstern fælles overbelastnings-beskyttelse	162

3. FUNKTIONSPRØVER FOR BEVÆGELSESFØLER

Nej	Prøve	Beskrivelse	Tilknyttede krav
1.	**Administrativ undersøgelse**		
1.1.	Dokumentation	Dokumentationens korrekthed	
2.	**Besigtigelse**		
2.1.	Overensstemmelse med dokumentationen		
2.2.	Identifikation / mærkning		169, 170
2.3.	Materialer		163 til 167
2.4.	Plombering		251
3.	**Funktionsprøver**		
3.1.	Identifikationsdata for føler		077*
3.2.	Bevægelsesføler — samparring med køretøjsenhed		099*, 155
3.3.	Bevægelsesregistrering Nøjagtighed af bevægelsesmåling		 022 til 026

Nej	Prøve	Beskrivelse	Tilknyttede krav
4.	**Miljøprøver**		
4.1.	Arbejdstemperatur	Funktionaliteten (som defineret i prøve nr. 3.3) efterprøves i temperaturintervallet [– 40 °C; + 135 °C] gennem: — IEC 68-2-1 prøve Ad, med en prøvningsvarighed på 96 timer ved den laveste temperatur To_{min} — IEC 68-2-2 prøve Bd, med en prøvningsvarighed på 96 timer ved den højeste temperatur To_{max}	159
4.2.	Temperaturcykluser	Funktionsprøvning (som fastlagt i prøve nr. 3.3) gennem IEC 68-2-14 prøve Na, 20 cykluser, hver med temperatur varierende fra den lave temperatur (– 40 °C) til den høje temperatur (+135 °C) og 2 timers fastholdelse af både den lave og den høje temperatur Et reduceret sæt prøvninger (af dem, som er fastlagt i afsnit 3.3 af denne tabel) kan udføres ved den lave temperatur, den høje temperatur og under gennemgang af temperatur-cykluserne	159
4.3.	Fugtighedscykluser	Funktionsprøvning (som fastlagt i prøve nr. 3.3) gennem IEC 68-2-30, prøve Db, seks 24 timers cykluser, hvor hver temperatur varierer fra + 25 °C til + 55 °C og med en relativ fugtighed på 97 % ved + 25 °C og 93 % ved + 55 °C	160
4.4.	Vibration	Funktionsprøvning (som foreskrevet i prøvning 3.3) ved IEC 68-2-6, prøve Fc, med en prøvningsvarighed på 100 frekvenscykluser: Konstant skift mellem 10 og 57 Hz: 1,5 mm top konstant acceleration mellem 57 og 500 Hz: 20 g	163
4.5.	Mekanisk chok	Funktionsprøvning (som fastlagt i prøve 3.3) ved IEC 68-2-27, prøve Ea, 3 chok i begge retninger for hver af de tre ortogonale akser	163
4.6.	Beskyttelse mod vand og fremmedlegemer	Det kontrolleres, at køretøjsenhedens beskyttelsesindeks i henhold til IEC 529 er mindst IP 64, når den er monteret under driftsomstændigheder på køretøjet	165
4.7.	Beskyttelse mod omvendt polaritet	Det kontrolleres at bevægelsesføleren kan modstå polvending af strømforsyningen	161
4.8.	Kortslutningsbeskyttelse	Det kontrolleres, at ind- og udgangssignaler er beskyttet mod kortslutning til strømforsyningen og til stel	161
5.	**Elektromagnetisk kompatibilitet**		
5.1.	Strålingsemission og følsomhed	Overensstemmelse med direktiv 95/54/EØF	162
5.2.	Elektrostatisk udladning	Overensstemmelse med IEC 61000-4-2, ± 2 kV (niveau 1)	162
5.3.	Transient nedre ledningsoverførsel for datalinjerne)	Overensstemmelse med ISO7637-3 (niveau III)	162

4. FUNKTIONSPRØVER FOR FARTSKRIVERKORT

Nej	Prøve	Beskrivelse	Tilknyttede krav
1.	**Administrativ undersøgelse**		
1.1.	Dokumentation	Dokumentationens korrekthed	
2.	**Besigtigelse**		
2.1.		Det kontrolleres, at alle faciliteter til beskyttelse samt synlige data er korrekt udskrevet på kortet og overensstemmende	171 til 181
3.	Fysiske prøver		
3.1.	Kontroller kortets dimensioner og kontakternes placering		184 ISO/IEC 7816-1 ISO/IEC 7816-2
4.	**Protokolprøver**		
4.1.	ATR (svar på nulstilling)	Kontroller at ATR er overensstemmende	ISO/IEC 7816-3 TCS 304, 307, 308
4.2	T=0	Kontroller at T=0 protokollen er overensstemmende	ISO/IEC 7816-3 TCS 302, 303, 305
4.3.	PTS (valgt transmissions-protokol)	Kontroller at PTS-kommandoen er overensstemmende ved at sætte T=1 fra T=0.	ISO/IEC 7816-3 TCS 309 to 311
4.4.	T=1	Kontroller at T=1 protokollen er overensstemmende	ISO/IEC 7816-3 TCS 303, / 306
5.	**Kortets struktur**		
5.1.		Kontroller at kortets filstruktur er overensstemmende ved at kontrollere for tilstedeværelse af påbudte filer i kortet og adgangsbetingelserne til dem	TCS 312 TCS 400*, 401, 402, 403*, 404, 405*, 406, 407, 408*, 409, 410*, 411, 412, 413*, 414, 415*, 416, 417, 418*, 419
6.	**Funktionsprøver**		
6.1.	Normal behandling af data	Hver tilladt anvendelse af hver kommando kontrolleres mindst én gang (eksempel: Kommandoen UPDATE BINARY kontrolleres med CLA = '00', CLA = '0C' og med forskellige parametre P1, P2 og Lc). Kontroller at operationerne faktisk er udført på kortet (f.eks. ved at læse den fil, kommandoen er udført på)	TCS 313 til TCS 379
6.2.	Fejlmeddelelser	Hver fejlmeddelelse afprøves mindst én gang (som foreskrevet i tillæg 2) for hver kommando. Hver fælles fejl afprøves mindst én gang (bortset fra '6400' integritetsfejl, der kontrolleres som led i sikkerhedsattesteringen)	
7.	**Miljøprøver**		
7.1		Det kontrolleres, at kortene fungerer indenfor grænsebetingelserne, som er fastlagt i overensstemmelse med ISO/IEC 10373	185 til 188 ISO/IEC 7816-1

5. INTEROPERABILITETSPRØVER

Nej	Prøve	Beskrivelse
1.	Gensidig ægthedsbekræftelse	Kontroller at den gensidige ægthedsbekræftelse mellem køretøjsenheden og fartskriverkortet afvikles normalt
2.	Skrive/læseprøver	Gennemfør et typisk aktivitetsscenario på køretøjsenheden. Scenariet skal være tilpasset den afprøvede korttype og skal indebære skrivning på så mange af kortets elementærfiler som muligt Genem dataoverførsel fra kortet kontrolleres det, at alle de tilsvarende registreringer er udført korrekt Gennem en daglig udskrift fra kort kontrolleres, at alle de tilsvarende registreringer kan læses korrekt

Tillæg 10

FÆLLES SIKKERHEDSMÅL

Dette tillæg angiver det foreskrevne mindste indhold i sikkerhedsmålene for bevægelsesføler, køretøjsenhed og fartskriverkort.

For at opstille sikkerhedsmål, som der kan sikkerhedsattesteres efter, skal fabrikanterne efter behov udvikle og komplettere dokumenterne uden at ændre eller slette eksisterende risici, mål, proceduremæssige metoder eller forskrifter for sikkerhedsfunktioner.

FÆLLES SIKKERHEDSMÅL FOR BEVÆGELSESFØLERE

1. **Indledning**

Dette dokument indeholder en beskrivelse af bevægelsesføleren, de risici, den skal imødegå, og de sikkerhedsmæssige mål, den skal opfylde. Dokumentet angiver de foreskrevne sikkerhedsfunktioner. Det angiver den påberåbte mindste styrke af sikkerhedsmekanismerne og det nødvendige sikkerhedsniveau for udvikling og evaluering.

De krav, der henvises til i dokumentet, er dem, som er angivet i hoveddelen af bilag I, del B. Af klarhedshensyn vil kravene i hoveddelen af bilag I, del B i nogen grad blive gentaget i forskrifterne for sikkerhedsmål og omvendt. Ved eventuel modstrid mellem et foreskrevet sikkerhedsmål og de krav i hoveddelen af bilag I, del B, som der henvises til i det pågældende foreskrevne sikkerhedsmål, er kravet i hoveddelen af bilag I, del B afgørende.

De krav i hoveddelen af bilag I, del B, som der ikke henvises til i sikkerhedsmålene, er ikke omfattet af sikkerhedsfunktioner.

For at kunne spores til udviklings- og evalueringsdokumentationen er risici, mål, proceduremæssige midler og specifikationer af sikkerhedsfunktioner tildelt unikke etiketter.

2. **Forkortelser, definitioner og henvisninger**

2.1. ***Forkortelser***

ROM	Læselager (read only memory)
SEF	Sikkerhedsfunktion (security enforcing function)
TBD	Fastlægges (to be defined)
TOE	Evalueret system (target of evaluation)
VU	Køretøjsenhed (vehicle unit)

2.2. ***Definitioner***

Digital fartskriver	Kontrolapparat
Enhed	En anordning, som er tilsluttet bevægelsesføleren
Køredata	De data, som udveksles med køretøjsenheden og repræsenterer hastighed og tilbagelagt distance.
Fysisk adskilte dele	Fysiske komponenter, som tilhører bevægelsesføleren og er fordelt i køretøjet, modsat de fysiske komponenter, som er samlet i bevægelsesfølerens hus.

Sikkerhedsdata	De specifikke data, som er nødvendige til støtte for sikkerhedsfunktioner (f.eks. kryptografiske nøgler).
System	Apparater, personer eller organisationer, som på nogen måde er involveret i kontrolapparatet
Bruger	En person, som er bruger af bevægelsesføleren (når ordet ikke indgår i udtrykket »brugerdata«).
Brugerdata	Alle data, bortset fra køre- og sikkerhedsdata, som er registreret eller lagret af bevægelsesføleren.

2.3. ***Henvisninger***

ITSEC ITSEC Evalueringskriterier for informationsteknologi 1991 (Information Technology Security Evaluation Criteria 1991).

3. **Produktrationale**

3.1. ***Beskrivelse og anvendelse af bevægelsesføleren***

Bevægelsesføleren er bestemt til montering i køretøjer til vejtransport. Dens formål er at tilføre køretøjsenheden sikrede køredata, som er repræsentative for køretøjets hastighed og tilbagelagte distance.

Bevægelsesføleren er mekanisk forbundet med en bevægelig del af køretøjet, idet bevægelsen kan være repræsentativ for køretøjets hastighed eller tilbagelagte distance. Den kan være placeret i køretøjets gearkasse eller i enhver anden del af køretøjet.

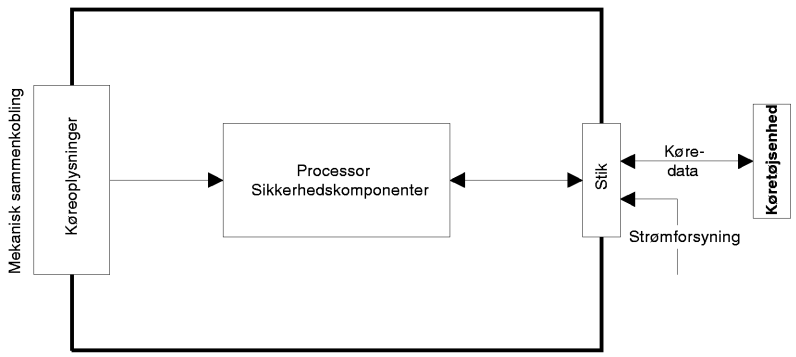
I driftstilstand er bevægelsesføleren tilsluttet en køretøjsenhed.

Den kan desuden være tilsluttet bestemt udstyr til styringsmæssigt formål (fastlægges af fabrikanten)

Den typiske bevægelsesføler er beskrevet i følgende figur:

Figur 1

Typisk bevægelsesføler

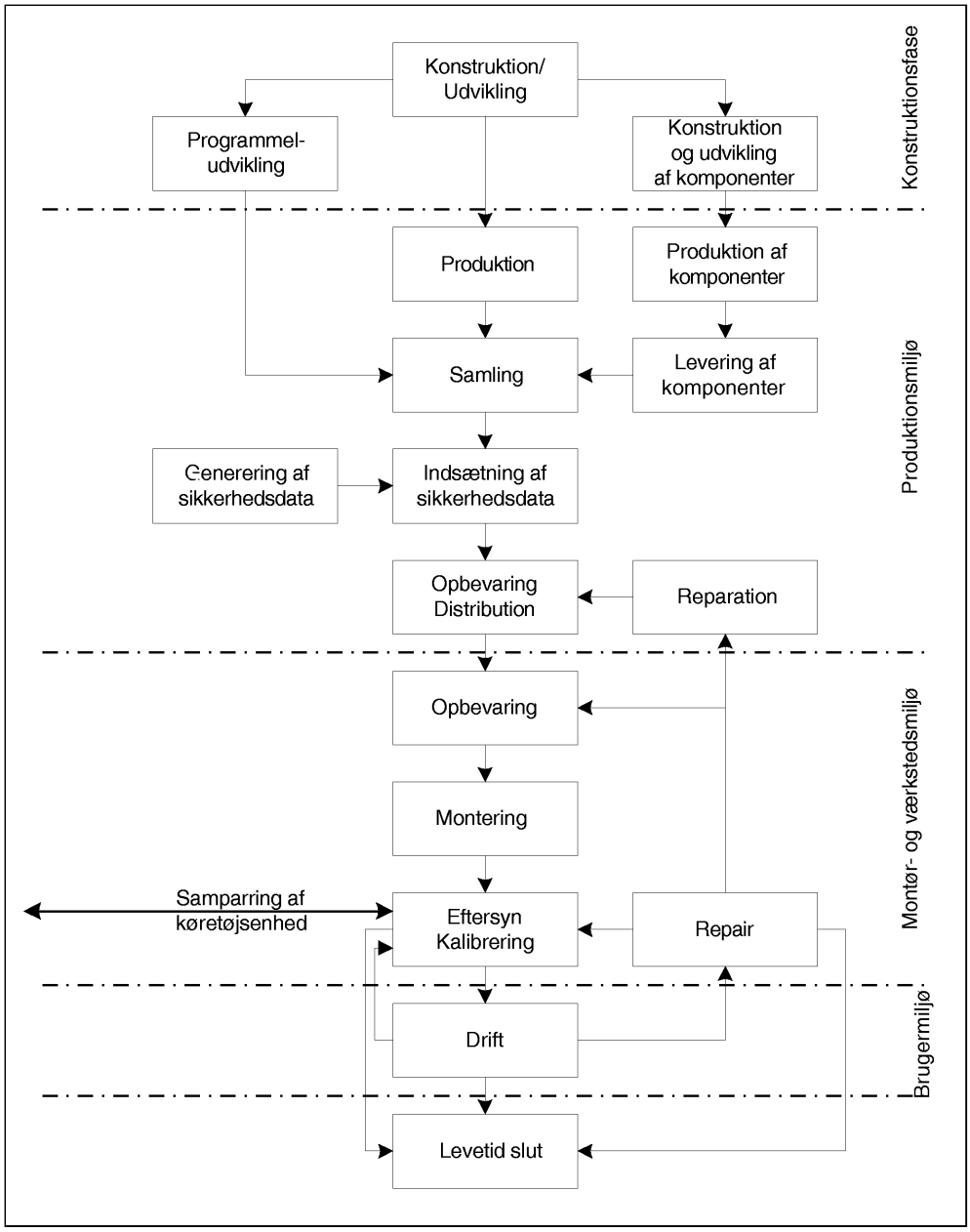


3.2. ***Bevægelsesfølerens levetidscyklus***

Den typiske levetidscyklus af en bevægelsesføler er beskrevet i følgende figur:

Figur 2

Typisk levetidscyklus for en bevægelsesføler



3.3. ***Risici***

Dette punkt beskriver de risici, som bevægelsesføleren kan være udsat for.

3.3.1. *Risiko rettet mod adgangskontrolregler*

T.Access	Brugere kan tænkes at forsøge at få adgang til funktioner, som de ikke har ret til at benytte.

3.3.2. *Konstruktionsbetingede risici*

T.Faults	Som følge af fejl i maskinel, programmel eller kommunikationsprocedurer kan bevægelsesføleren blive udsat for uventede betingelser, som forringer dens sikkerhed
T.Tests	Brug af ikke ugyldiggjorte prøvningsfunktionsmåder eller eksisterende bagdøre kan skade bevægelsesfølerens sikkerhed
T.Design	Brugere kan tænkes at forsøge at skaffe sig uretmæssigt kendskab til konstruktionen fra fabrikanten (ved tyveri, bestikkelse osv.) eller ved baglæns konstruktion

3.3.3. *Operationsorienterede risici*

T.Environment	Brugere kan forringe bevægelsesfølerens sikkerhed ved direkte påvirkning (termisk, elektromagnetisk, optisk, kemisk, mekanisk osv.)
T.Hardware	Brugere kan tænkes at forsøge at ændre bevægelsesfølerens maskinel
T.Mechanical_Origin	Brugere kan tænkes at forsøge at manipulere bevægelsesfølerens indgangssignal (f.eks ved at skrue den fri af gearkassen mv.)
T.Motion_Data	Brugere kan tænkes at forsøge at ændre køretøjets køredata (ved tilføjelse, ændring, sletning eller genafspilning af signal)
T.Power_Supply	Brugere kan tænkes at forsøge at forhindre bevægelsesføleren i at opfylde sine sikkerhedsmål ved at ændre (afbryde, nedsætte, øge) dens strømforsyning
T.Security_Data	Brugere kan tænkes at forsøge at skaffe sig uretmæssigt kendskab til sikkerhedsdata, når disse genereres, transporteres eller lagres i apparatet
T.Software	Brugere kan tænkes at forsøge at ændre bevægelsesfølerens programmel
T.Stored_Data	Brugere kan tænkes at forsøge at ændre lagrede data (sikkerhedsdata eller brugerdata)

3.4. ***Sikkerhedsmål***

De sikkerhedsmæssige hovedmål for det digitale fartskriversystem er følgende:

O.Main	Data, som skal kontrolleres af den tilsynsførende myndighed, skal være til rådighed og fuldstændigt og nøjagtigt afspejle de kontrollerede føreres og køretøjers aktiviteter hvad angår køre-, arbejde, rådigheds- og hvileperioder samt køretøjets hastighed

Derfor har bevægelsesføleren følgende sikkerhedsmæssige mål, som er et led i det overordnede sikkerhedsmål:

O.Sensor_Main	De af bevægelsesføleren overførte data skal være til rådighed for køretøjsenheden, så denne er i stand til fuldstændigt og nøjagtigt at fastlægge køretøjets bevægelse hvad angår hastighed og tilbagelagt distance

3.5. ***Informationsteknologiske sikkerhedsmål***

Bevægelsesføleren har følgende særlige informationsteknologiske sikkerhedsmål, som er et led i dens overordnede sikkerhedsformål:

O.Access	Bevægelsesføleren skal regulere de tilsluttede enheders adgang til funktioner og data
O.Audit	Bevægelsesføleren skal revidere for forsøg på at undergrave dens sikkerhed og skal spore dem til de tilknyttede enheder
O.Authentication	Bevægelsesføleren skal ægthedskontrollere de tilsluttede enheder

O.Processing	Bevægelsesføleren skal sikre, at behandlingen af indgangssignalet og de heraf afledte køredata er nøjagtige
O.Reliability	Bevægelsesføleren skal tilvejebringe en pålidelig service
O.Secured_Data_Exchange	Bevægelsesføleren skal sikre dataudveksling med køretøjsenheden

3.6. ***Fysiske, personalemæssige og proceduremæssige midler***

Dette afsnit beskriver fysiske, personalemæssige og proceduremæssige midler, som er et led i bevægelsesfølerens sikkerhed.

3.6.1. *Maskinellets konstruktion*

M.Development	Udviklere af bevægelsesfølere skal sikre, at ansvarsuddelegering i udviklingsfasen sker på en måde, som bevarer IT-sikkerheden
M.Manufacturing	Fabrikanter af bevægelsesfølere skal sørge for, at ansvarsuddelegering i produktionsfasen finder sted på en måde, som bevarer IT-sikkerheden, og at bevægelsesføleren under produktionsprocessen er sikret mod fysisk manipulation, som kan tænkes at forringe IT-sikkerheden

3.6.2. *Levering af maskinellet*

M.Delivery	Fabrikanter af bevægelsesfølere, køretøjsfabrikanter og montører eller værksteder skal sikre, at håndtering af bevægelsesføleren finder sted på en måde, som bevarer IT-sikkerheden

3.6.3. *Generering og afgivelse af sikkerhedsdata*

M.Sec_Data_Generation	Algoritmer til generering af sikkerhedsdata må kun være tilgængelige for autoriserede og betroede personer
M.Sec_Data_Transport	Sikkerhedsdata skal genereres, transporteres og indsættes i bevægelsesføleren på en sådan måde, at deres fortrolighed og integritet bevares

3.6.4. *Kontrolapparatets montering, kalibrering og eftersyn*

M.Approved_Workshops	Montering, kalibrering og reparation af kontrolapparater skal udføres af betroede og godkendte montører eller værksteder
M.Mechanical_Interface	Der skal være midler til detektion af ulovlige fysiske indgreb på den mekaniske sammenkobling (f.eks. plomber)
M.Regular_Inpections	Kontrolapparater skal regelmæssigt efterses og kalibreres

3.6.5. *Retlig kontrol*

M.Controls	Der skal regelmæssigt og på tilfældig måde gennemføres eftersyn, som skal indbefatte sikkerhedsrevision

3.6.6. *Opgraderinger af programmel*

M.Software_Upgrade	Reviderede versioner af programmel skal være sikkerhedscertificeret, før de må implementeres i en bevægelsesføler

4. **Sikkerhedsfunktioner**

4.1. ***Identificering og ægthedsbekræftelse***

UIA_101	Bevægelsesføleren skal for hver vekselvirkning kunne fastslå identiteten af enhver enhed, som den er tilsluttet

UIA_102 Identiteten af en tilsluttet enhed består af:

— en enhedsgruppe:

— køretøjsenhed,

— styringsanordning,

— andet,

— en enheds-ID (kun for køretøjsenheder).

UIA_103 Enheds-ID for en tilsluttet køretøjsenhed består af køretøjsenhedens godkendelsesnummer og køretøjsenhedens serienummer.

UIA_104 Bevægelsesføleren skal kunne bekræfte ægtheden af enhver køretøjsenhed og styringsanordning, som den er tilsluttet:

— ved tilslutningen til enheden,

— ved genetablering af strømforsyningen

UIA_105 Bevægelsesføleren skal periodisk kunne gentage ægthedsbekræftelsen af den køretøjsenhed, som den er tilsluttet.

UIA_106 Bevægelsesføleren skal konstatere og forhindre brug af ægthedsbekræftelsesdata, som er kopieret og genafspillet.

UIA_107 Efter at et antal (fastlægges af fabrikanten, dog højst 20) på hinanden følgende forsøg på ægthedsbekræftelse er konstateret, skal sikkerhedsfunktionen:

— oprette en revisionspost over hændelsen,

— advare enheden,

— fortsætte med at eksportere køredata i ikke sikret tilstand.

4.2. ***Adgangskontrol***

Adgangskontrollen sikrer, at kun de, der er autoriseret dertil, kan læse data fra eller oprette eller ændre data i det evaluerede system.

4.2.1. *Adgangskontrolregler*

ACC_101 Bevægelsesføleren skal kontrollere adgangen til funktionen og til data.

4.2.2. *Dataadgang*

ACC_102 Bevægelsesføleren skal sikre, at dens egne identifikationsdata kun kan skrives én gang (krav 078).

ACC_103 Bevægelsesføleren må kun acceptere og/eller lagre brugerdata fra ægthedsbekræftede enheder.

ACC_104 Bevægelsesføleren skal håndhæve behørig læse- og skriveadgangsret til sikkerhedsdata.

4.2.3. *Filstruktur og adgangsbetingelser*

ACC_105 Filstruktur og adgangsbetingelser for applikations- og datafiler skal oprettes i produktionen og derefter være spærret for enhver efterfølgende ændring og sletning.

4.3. ***Reviderbarhed***

ACT_101 Bevægelsesføleren skal i sin hukommelse have sine egne identifikationsdata (krav 077).

ACT_102 Installationsdata skal være lagret i bevægelsesfølerens hukommelse (krav 099).

ACT_103 Bevægelsesføleren skal kunne udlæse reviderbarhedsdata til ægthedsbekræftede enheder på anmodning af disse.

4.4. ***Revision***

AUD_101 Bevægelsesføleren skal oprette revisionsposter for hændelser, som forringer dens sikkerhed.

AUD_102 Hændelser, som forringer bevægelsesfølerens sikkerhed, er følgende:

— Forsøg på sikkerhedsbrud:

  — mislykket ægthedskontrol,

  — integritetsfejl i lagrede data,

  — fejl ved intern dataoverførsel,

  — ubehørig åbning af hus,

  — sabotage på maskinel og

— følerfejl,

AUD_103 Revisionsposter skal indeholde følgende data:

— dato og klokkeslæt for hændelsen,

— hændelsens art,

— identitet af den tilsluttede enhed,

når de ønskede data ikke foreligger, skal der gives en passende standardindikation (fastlægges af fabrikanten).

AUD_104 Bevægelsesføleren skal sende de revisionsposter, den opretter, til køretøjsenheden i samme øjeblik de oprettes, og kan desuden lagre dem i sin hukommelse.

AUD_105 Når bevægelsesføleren lagrer revisionsposter, skal den sikre, at der bibeholdes 20 revisionsposter uafhængigt af, om lagerpladsen til revisionsposter slipper op, og skal være i stand til at overføre lagrede revisionsposter til ægthedsbekræftede enheder på disses anmodning.

4.5. ***Nøjagtighed***

4.5.1. *Regler for dataudvekslingskontrol*

ACR_101 Bevægelsesføleren skal sikre, at kun det mekaniske indgangssignal fra føleren er grundlag for afledte køredata.

4.5.2. *Intern dataoverførsel*

Forskrifterne i dette afsnit finder kun anvendelse, hvis bevægelsesføleren anvender fysisk adskilte dele.

ACR_102 Ved overførsel af data mellem fysisk adskilte dele af bevægelsesføleren skal data være beskyttet mod ændring.

ACR_103 Konstateres der en dataoverførselsfejl under en intern overførsel, skal overførslen gentages og sikkerhedsfunktionen skal oprette en revisionspost for hændelsen.

4.5.3. *Integritet af lagrede data*

ACR_104 Bevægelsesføleren skal foretage integritetskontrol af de brugerdata, som ligger i dens hukommelse.

ACR_105 Konstateres der en integritetsfejl i lagrede brugerdata, skal sikkerhedsfunktionen oprette en revisionspost.

4.6. ***Pålidelighed af service***

4.6.1. *Prøvning*

RLB_101 Alle kommandoer, operationer og testpunkter, som særligt dækker prøvningsbehovet i produktionsfasen, skal være sat ud af kraft eller fjernet, inden produktionsfasen er slut. De må ikke kunne genetableres til senere brug.

RLB_102 Under den indledende opstart og under normal drift skal bevægelsesføleren foretage selvtest til efterprøvning af korrekt funktion. Bevægelsesfølerens selvtest skal omfatte integritetskontrol af sikkerhedsdata og integritetskontrol af lagret eksekverbar kode (hvis denne ikke ligger i ROM).

RLB_103 Konstateres en intern fejl under selvtest, skal sikkerhedsfunktionen oprette en revisionspost (følerfejl).

4.6.2. *Programmel*

RLB_104 Bevægelsesfølerens programmel må ikke på nogen måde kunne analyseres eller fejlrettes i marken.

RLB_105 Inddata fra eksterne kilder må ikke kunne accepteres som eksekverbar kode.

4.6.3. *Fysisk sikring*

RLB_106 Er bevægelsesføleren konstrueret, så den kan åbnes, skal føleren detektere enhver åbning af huset, selv uden ekstern strømtilførsel, i mindst 6 måneder. I så fald skal sikkerhedsfunktionen oprette en revisionspost for hændelsen. Det kan godtages, at revisionsposten genereres og lagres efter genoptagelse af strømforsyningen.

Er bevægelsesføleren således konstrueret, at den ikke kan åbnes, skal konstruktionen bevirke, at forsøg på fysiske indgreb let kan afsløres (f.eks. ved besigtigelse).

RLB_107 Bevægelsesføleren skal detektere nærmere angiven (angives af fabrikanten) sabotage på maskinellet.

RLB_108 I ovennævnte tilfælde skal sikkerhedsfunktionen oprette en revisionspost, og bevægelsesføleren skal: (angives af fabrikanten).

4.6.4. *Afbrydelser i strømforsyningen*

RLB_109 Bevægelsesføleren skal opretholde en sikker tilstand ved afbrydelser eller uregelmæssigheder i strømforsyningen.

4.6.5. *Nulstillingsbetingelser*

RLB_110 Ved eventuel afbrydelse af strømforsyningen, ved standsning af en transaktion, før den er fuldført, samt under alle andre nulstillingsbetingelser, skal føleren nulstilles fuldstændigt.

4.6.6. *Rådighed over data*

RLB_111 Bevægelsesføleren skal sikre, at der opnås adgang til systemets enheder, når det er nødvendigt, og at enhederne ikke er genstand for unødig anmodning eller opretholdelse.

4.6.7. *Flere applikationer samtidig*

RLB_112 Hvis bevægelsesføleren tilfører systemet andre applikationer end fartskriverapplikationen, skal alle applikationer være fysisk og/eller logisk adskilt fra hinanden. Sådanne applikationer må ikke dele sikkerhedsdata. Kun én opgave må være aktiv ad gangen.

4.7. ***Dataudveksling***

DEX_101 Bevægelsesføleren skal afgive køredata til køretøjsenheden med tilhørende sikkerhedsattributter, som sætter køretøjsenheden i stand til at verificere deres integritet og ægthed.

4.8. ***Kryptografisk støtte***

Forskrifterne i dette punkt finder kun anvendelse, når der er behov, alt efter de anvendte sikkerhedsmekanismer og de af fabrikanten anvendte løsninger.

CSP_101 Enhver kryptografisk operation, som udføres af bevægelsesføleren, skal være i overensstemmelse med en foreskreven algoritme og en foreskreven nøglestørrelse.

CSP_102 Hvis bevægelsesføleren opretter kryptografiske nøgler, skal dette ske i overensstemmelse med foreskrevne algoritmer til oprettelse af kryptografiske nøgler og med foreskrevne kryptografiske nøglestørrelser.

CSP_103 Hvis bevægelsesføleren distribuerer kryptografiske nøgler, skal dette ske i overensstemmelse med foreskrevne metoder til distribution af nøgler.

CSP_104 Giver bevægelsesføleren adgang til kryptografiske nøgler, skal dette ske i overensstemmelse med foreskrevne adgangsmetoder til nøgler.

CSP_105 Destruerer bevægelsesføleren kryptografiske nøgler, skal dette ske i overensstemmelse med foreskrevne metoder til destruktion af nøgler.

5. **Fastlæggelse af sikkerhedsmekanismer**

De sikkerhedsmekanismer, som varetager bevægelsesfølerens sikkerhedsfunktioner, fastlægges af bevægelsesfølerens fabrikant.

6. **Minimumstyrke af sikkerhedsmekanismer**

Den mindste styrke af bevægelsesfølerens sikkerhedsmekanismer er Høj som fastlagt i ITSEC.

7. **Sikkerhedsniveau**

Målet for bevægelsesfølerens sikkerhedsniveau er ITSEC niveau E3 som fastlagt i ITSEC.

8. **Rationale**

Følgende matricer giver et rationale for sikkerhedsfunktioner ved at angive:

— hvilke sikkerhedsfunktioner eller midler, der modvirker hvilke risici,

— hvilke sikkerhedsfunktioner, der opfylder hvilke IT-sikkerhedsmål.

	Risici												IT-mål					
	T.Access	T.Faults	T.Tests	T.Design	T.Environment	T.Hardware	T.Mechanical_Origin	T.Motion_Data	T.Power_Supply	T.Security_Data	T.Software	T.Stored_Data	O.Access	O.Audit	O.Authentication	O.Processing	O.Reliability	O.Secured_Data_Exchange
Fysiske, personalemæssige eller proceduremæssige midler																		
Udvikling		x	x	x														
Produktion			x	x														
Levering						x					x	x						
Generering af sikkerhedsdata										x								
Transport af sikkerhedsdata										x								
Godkendte værksteder							x											
Mekanisk tilkobling							x											
Regelmæssig inspektion						x	x		x		x							
Retlig kontrol					x	x	x		x	x	x							
Opgraderinger af programmel											x							
Sikkerhedsfunktioner																		
Identificering og ægthedsbekræftelse																		
UIA_101 Identifikation af enheder	x							x					x		x			x
UIA_102 Identitet af enheder	x												x		x			
UIA_103 Identitet af køretøjsenhed														x				
UIA_104 Ægthedsbekræftelse af enheder	x							x					x		x			x
UIA_105 Gentagelse af ægthedsbekræftelse	x							x					x		x			x
UIA_106 Forfalskningssikker ægthedsbekræftelse	x							x					x		x			
UIA_107 Svigt af ægthedskontrol								x						x			x	
Adgangskontrol																		
ACC_101 Adgangskontrolregler	x									x		x	x					
ACC_102 Bevægelsesføler-ID												x	x					

	Risici												IT-mål					
	T.Access	T.Faults	T.Tests	T.Design	T.Environment	T.Hardware	T.Mechanical_Origin	T.Motion_Data	T.Power_Supply	T.Security_Data	T.Software	T.Stored_Data	O.Access	O.Audit	O.Authentication	O.Processing	O.Reliability	O.Secured_Data_Exchange
ACC_103 Brugerdata												x	x					
ACC_104 Sikkerhedsdata										x		x	x					
ACC_105 Filstruktur og adgangsbetingelser	x									x		x	x					
Reviderbarhed																		
ACT_101 ID-data for bevægelsesføler														x				
ACT_102 Samparringsdata														x				
ACT_103 Reviderbarhedsdata														x				
Revision																		
AUD_101 Revisionsposter														x				
AUD_102 Revisionsliste over hændelser	x				x	x						x		x				
AUD_103 Revisionsdata														x				
AUD_104 Revisionsværktøjer														x				
AUD_105 Lagring af revisionsposter														x				
Nøjagtighed																		
ACR_101 Regler for dataudvekslingskontrol								x								x	x	
ACR_102 Intern dataoverførsel																x	x	
ACR_103 Intern dataoverførsel														x				
ACR_104 Integritet af lagrede data												x					x	
ACR_105 Integritet af lagrede data												x		x				
Pålidelighed																		
RLB_101 Prøvning i produktionen			x	x													x	
RLB_102 Selvtest		x				x			x		x						x	
RLB_103 Selvtest						x			x		x			x				
RLB_104 Programmelanalyse				x							x						x	
RLB_105 Indlæsning af programmel											x					x	x	
RLB_106 Åbning af hus				x	x	x				x	x	x					x	
RLB_107 Sabotage mod maskinel						x											x	
RLB_108 Sabotage mod maskinel						x								x				
RLB_109 Afbrydelser i strømforsyningen									x								x	
RLB_110 Nulstilling		x															x	
RLB_111 Rådighed over data																x	x	
RLB_112 Flere applikationer samtidig																	x	
Dataudveksling																		
DEX_101 Sikret eksport af køredata								x										x
Kryptografisk støtte																		
CSP_101 Algoritmer																	x	x
CSP_102 Nøglegenerering																	x	x
CSP_103 Nøgledistribution																	x	x
CSP_104 Nøgleadgang																	x	x
CSP_105 Nøgledestruktion																	x	x

FÆLLES SIKKERHEDSMÅL FOR KØRETØJSENHEDER

1. **Indledning**

Dette dokument indeholder en beskrivelse af køretøjsenheden, af de risici, den skal imødegå, og de sikkerhedsmæssige mål, den skal opfylde. Afsnittet angiver de foreskrevne sikkerhedsfunktioner. Den angiver den påberåbte styrke af sikkerhedsmekanismerne og det nødvendige sikkerhedsniveau under udvikling og evaluering.

De krav, der henvises til i dokumentet, er dem, som er angivet i hoveddelen af bilag I, del B. Af klarhedshensyn vil kravene i hoveddelen af bilag I, del B undertiden blive gentaget i forskrifterne for sikkerhedsmål, eller omvendt. I tilfælde af modstrid mellem en forskrift for sikkerhedsmål og de krav i hoveddelen af bilag I, del B, som der henvises til i dette krav til sikkerhedsmål, skal kravet i hoveddelen af bilag I, del B være afgørende.

De krav i hoveddelen af bilag I, del B, som der ikke henvises til i sikkerhedsmålene, er ikke omfattet af sikkerhedsfunktioner.

For at kunne spores til udviklings- og evalueringsdokumentationen er risici, mål, proceduremæssige midler og specifikationer af sikkerhedsfunktioner tildelt unikke etiketter.

2. **Forkortelser, definitioner og henvisninger**

2.1. ***Forkortelser***

PIN Personligt identifikationsnummer

ROM Læselager (read only memory)

SEF Sikkerhedsfunktion (security enforcing function)

TBD Fastlægges (to be defined)

TOE Evalueret system (target of evaluation)

VU Køretøjsenhed (vehicle unit)

2.2. ***Definitioner***

Digital fartskriver	Kontrolapparat
Køredata	De data, som udveksles med bevægelsesføleren og repræsenterer hastighed og tilbagelagt distance
Fysisk adskilte dele	Fysiske komponenter, som tilhører køretøjsenheden og er fordelt i køretøjet, modsat de fysiske komponenter, som er samlet i køretøjsenhedens hus
Sikkerhedsdata	De specifikke data, som er nødvendige til støtte for sikkerhedsfunktioner (f.eks. kryptografiske nøgler)
System	Apparater, personer eller organisationer, som på nogen måde er involveret i kontrolapparatet
Bruger	Ved brugere forstås personer, som anvender apparatet. Normale brugere af køretøjsenheden er førere, tilsynsførende, værksteder og virksomheder
Brugerdata	Alle data, bortset fra køre- og sikkerhedsdata, som registreres eller lagres af køretøjsenheden, og som foreskrives i kapitel III, punkt 12

2.3. ***Henvisninger***

ITSEC ITSEC Evalueringskriterier for informationsteknologi 1991 (Information Technology Security Evaluation Criteria 1991)

3. **Produktrationale**

3.1. ***Beskrivelse og anvendelse af køretøjsenheden***

Køretøjsenheden er bestemt til montering i køretøjer til vejtransport. Køretøjsenheden har til formål at registrere, gemme, vise, udprinte og udlæse data vedrørende førerens aktiviteter.

Den er tilsluttet en bevægelsesføler og udveksler køredata for køretøjet med denne.

Brugerne identificerer sig over for køretøjsenheden ved hjælp af fartskriverkort.

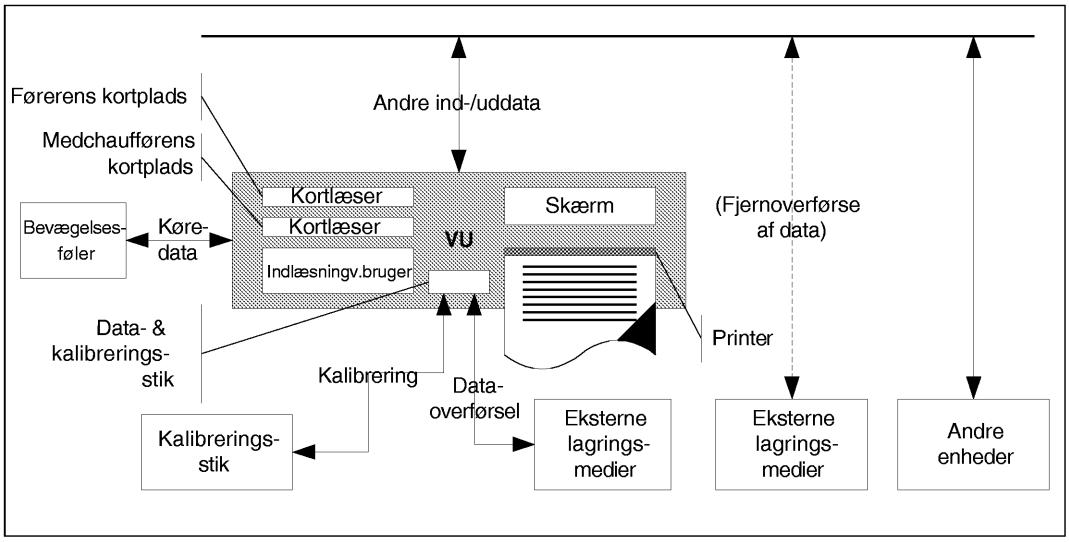
Køretøjsenheden registrerer og gemmer brugeraktivitetsdata i sit datalager og registrerer desuden brugeraktivitetsdata på fartskriverkortene.

Køretøjsenheden udlæser data til skærm, printer og eksterne enheder.

Det funktionelle miljø omkring den i køretøjet monterede køretøjsenhed er beskrevet i følgende figur:

Figur 1

Køretøjsenhedens funktionelle miljø



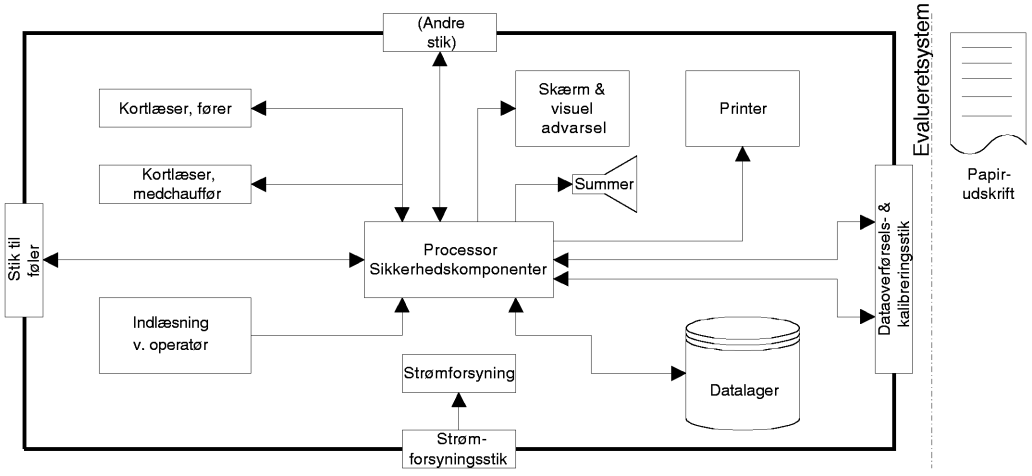
Køretøjsenhedens generelle egenskaber, funktioner og driftsform er beskrevet i kapitel II i bilag I, del B.

De funktionelle krav til køretøjsenheden er angivet i kapitel III af bilag I, del B.

Den typiske køretøjsenhed er beskrevet i følgende figur:

Figur 2

Typisk køretøjsenhed (. . .) ikke obligatorisk



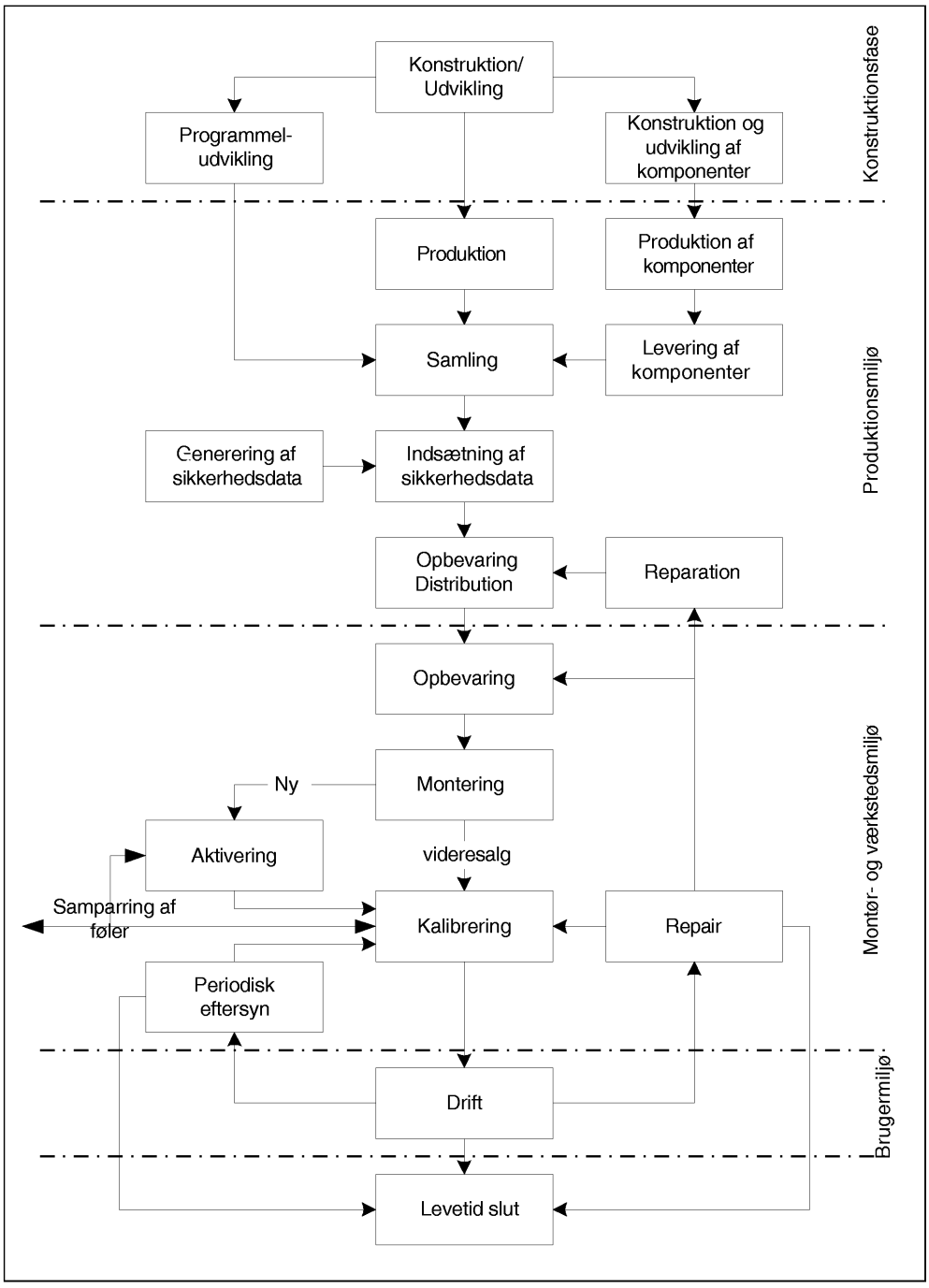
Det skal bemærkes, at skønt printermekanismen hører med til det evaluerede system, gør papirdokumentet det ikke, når først det er frembragt.

3.2. ***Køretøjsenhedens levetidscyklus***

Den typiske levetidscyklus af en køretøjsenhed er beskrevet i følgende figur:

Figur 3

Typisk levetidscyklus for køretøjsenhed



3.3. ***Risici***

Dette afsnit beskriver de risici, som køretøjsenheden kan være udsat for.

3.3.1. *Risici rettet mod regler for identifikation og adgangskontrol*

T.Access	Brugere kan tænkes at forsøge at skaffe sig adgang til funktioner, som de ikke har ret til at benytte (som f.eks. at føreren skaffer sig adgang til kalibreringsfunktionen)
T.Identification	Brugere kan tænkes at forsøge at bruge flere forskellige identifikationer eller undlade identifikation

3.3.2. *Konstruktionsbetingede risici*

T.Faults	Fejl i maskinel, programmel eller kommunikationsprocedurer kan sætte køretøjsenheden under uforudsete betingelser, så dens sikkerhed forringes
T.Tests	Brug af ikke ugyldiggjorte testfunktionsmåder eller eksisterende bagdøre kan skade køretøjsenhedens sikkerhed
T.Design	Brugere kan tænkes at forsøge at opnå uretmæssigt kendskab til konstruktionen fra fabrikanten (ved tyveri, bestikkelse osv.) eller ved baglæns konstruktion

3.3.3. *Operationsorienterede risici*

T.Calibration_Parameters	Brugere kan tænkes at forsøge at anvende fejlkalibreret udstyr (ved at ændre kalibreringsdata eller udnytte organisatoriske svagheder)
T.Card_Data_Exchange	Brugere kan tænkes at forsøge at ændre data, mens de udveksles mellem køretøjsenhed og fartskriverkort (tilføjelse, ændring, sletning, genafspilning af signal)
T.Clock	Brugere kan tænkes at forsøge at ændre det interne ur
T.Environment	Brugere kan tænkes at forringe køretøjsenhedens sikkerhed ved direkte påvirkning (termisk, elektromagnetisk, optisk, kemisk, mekanisk osv.)
T.Fake_Devices	Brugere kan tænkes at forsøge at tilslutte falske enheder (bevægelsesføler, chipkort) til køretøjsenheden
T.Hardware	Brugere kan tænkes at forsøge at ændre køretøjsenhedens maskinel
T.Motion_Data	Brugere kan tænkes at forsøge at ændre køredata for køretøjet (ved tilføjelse, ændring, sletning, genafspilning af signal)
T.Non_Activated	Brugere kan tænkes at anvende et ikke aktiveret apparat
T.Output_Data	Brugere kan tænkes at forsøge at ændre uddata (udskrift, visning på skærm eller dataoverførsel)
T.Power_Supply	Brugere kan tænkes at forsøge at forhindre køretøjsenheden i at opfylde sine sikkerhedsmål ved at ændre (afbryde, nedsætte, øge) dens strømforsyning
T.Security_Data	Brugere kan tænkes at forsøge at skaffe sig uretmæssigt kendskab til sikkerhedsdata, når disse genereres, transporteres eller lagres i apparatet
T.Software	Brugere kan tænkes at forsøge at ændre køretøjsenhedens programmel
T.Stored_Data	Brugere kan tænkes at forsøge at ændre lagrede data, (sikkerhedsdata eller brugerdata)

3.4. ***Sikkerhedsmål***

De sikkerhedsmæssige hovedmål for det digitale fartskriversystem er følgende:

O.Main	Data, som skal kontrolleres af den tilsynsførende myndighed, skal være til rådighed og fuldstændigt og nøjagtigt afspejle de kontrollerede føreres og køretøjers aktiviteter hvad angår køre-, arbejde, rådigheds- og hvileperioder samt køretøjets hastighed

For køretøjsenheden gælder derfor følgende sikkerhedsmæssige mål, som er et led i det overordnede sikkerhedsmål:

O.VU_Main	De data, som skal måles og registreres og derefter kontrolleres af den tilsynsførende myndighed, skal være til rådighed og fuldstændigt og nøjagtigt afspejle de kontrollerede føreres og køretøjers aktiviteter hvad angår køre-, arbejde, rådigheds- og hvileperioder samt køretøjets hastighed
O.VU_Export	Køretøjsenheden skal kunne eksportere data til eksterne lagermedier på en sådan måde, at deres integritet og ægthed af data kan verificeres

3.5. ***Informationsteknologiske sikkerhedsmål***

For køretøjsenheden gælder følgende særlige informationsteknologiske sikkerhedsmål som et led i dens sikkerhedsmæssige hovedmål:

O.Access	Køretøjsenheden skal kontrollere brugernes adgang til funktioner og data
O.Accountability	Køretøjsenheden skal indsamle nøjagtige reviderbarhedsdata
O.Audit	Køretøjsenheden skal revidere for forsøg på at undergrave systemets sikkerhed og spore dem til de tilknyttede brugere
O.Authentication	Køretøjsenheden skal ægthedskontrollere brugere og tilsluttede enheder (når det er nødvendigt at oprette en fortrolig sti mellem enhederne)
O.Integrity	Køretøjsenheden skal bevare integriteten af lagrede data
O.Output	Køretøjsenheden skal sikre, at udgående data nøje afspejler de målte eller lagrede data
O.Processing	Køretøjsenheden skal sikre, at behandlingen af indgående data til afledning af brugerdata er nøjagtig
O.Reliability	Køretøjsenheden skal tilvejebringe en pålidelig service
O.Secured_Data_Exchange	Køretøjsenheden skal sikre dataudveksling med bevægelsesføleren og med fartskriverkortene

3.6. ***Fysiske, personalemæssige og proceduremæssige midler***

Dette afsnit beskriver fysiske, personalemæssige og proceduremæssige midler, som er et led i køretøjsenhedens sikkerhed

3.6.1. *Maskinellets konstruktion*

M.Development	Udviklere af køretøjsenheder skal sørge for, at ansvarsuddelegering i udviklingsfasen finder sted på en måde, som bevarer IT-sikkerheden
M.Manufacturing	Fabrikanter af køretøjsenheder skal sørge for, at ansvarsuddelegering i produktionsfasen finder sted på en måde, som bevarer IT-sikkerheden, og at køretøjsenheden under produktionsprocessen er beskyttet mod fysisk manipulation, som kan forringe IT-sikkerheden

3.6.2. *Levering og aktivering af maskinellet*

M.Delivery	Fabrikanter af køretøjsenheder, køretøjsfabrikanter og montører eller værksteder skal sørge for, at håndtering af ikke aktiverede køretøjsenheder finder sted på en måde, som bevarer IT-sikkerheden
M.Activation	Køretøjsfabrikanter, montører eller værksteder skal aktivere køretøjsenheden efter at denne er monteret, inden køretøjet forlader de lokaler, hvor monteringen fandt sted

3.6.3. *Generering og levering af sikkerhedsdata*

M.Sec_Data_Generation	Algoritmer til generering af sikkerhedsdata må kun være tilgængelige for autoriserede og betroede personer
M.Sec_Data_Transport	Sikkerhedsdata skal genereres, transporteres og indsættes i køretøjsenheden på en sådan måde, at deres fortrolighed og integritet bevares

3.6.4. *Levering af kort*

M.Card_Availability	Fartskriverkort må stilles til rådighed og leveres alene til autoriserede personer
M.Driver_Card_Uniqueness	Førere må kun være i besiddelse af **ét** gyldigt førerkort på et givet tidspunkt
M.Card_Traceability	Levering af kort skal være sporbar (hvide lister, sorte lister), og ved sikkerhedsrevision skal anvendes sorte lister

3.6.5. *Kontrolapparatets montering, kalibrering og eftersyn*

M.Approved_Workshops	Montering, kalibrering og reparation af kontrolapparater skal udføres af betroede og godkendte montører eller værksteder
M.Regular_Inpections	Kontrolapparater skal regelmæssigt efterses og kalibreres
M.Faithful_Calibration	Godkendte montører og værksteder skal indlæse korrekte køretøjsparametre i kontrolapparatet under kalibrering

3.6.6. *Betjening af apparatet*

M.Faithful_Drivers	Førere skal efterleve gældende regler og optræde forsvarligt (f.eks. benytte deres førerkort, vælge korrekt aktivitet, når valget sker manuelt, osv.)

3.6.7. *Retlig kontrol*

M.Controls	Der skal regelmæssigt og på tilfældig måde gennemføres retlig kontrol, og heri skal indgå sikkerhedsrevision

3.6.8. *Opgraderinger af programmel*

M.Software_Upgrade	Reviderede versioner af programmel skal være sikkerhedscertificeret, før de må implementeres i en køretøjsenhed

4. **Sikkerhedsfunktioner**

4.1. ***Identificering og ægthedsbekræftelse***

4.1.1. *Identificering og ægthedsbekræftelse af bevægelsesføler*

UIA_201 Køretøjsenheden skal for hver vekselvirkning kunne fastslå identiteten af den bevægelsesføler, som den er tilsluttet.

UIA_202 Bevægelsesfølerens identitet består af følerens godkendelsesnummer og følerens serienummer.

UIA_203 Køretøjsenheden skal ægthedsbekræfte den bevægelsesføler, den er tilsluttet:

— Ved bevægelsesfølerens tilslutning,

— ved hver kalibrering af kontrolapparatet,

— ved genetablering af strømforsyningen.

Ægthedsbekræftelsen skal være gensidig og skal udløses af køretøjsenheden.

UIA_204 Køretøjsenheden skal periodisk (med intervaller som fastlægges af fabrikanten og hyppigere end én gang i timen) gentage identifikation og ægthedsbekræftelse af den bevægelsesføler, den er tilsluttet, og sikre, at den bevægelsesføler, som er identificeret ved den seneste kalibrering af kontrolapparatet, ikke er blevet udskiftet.

UIA_205 Køretøjsenheden skal konstatere og forhindre eventuel brug af ægthedsbekræftelsesdata, som er kopieret og genafspillet.

UIA_206 Efter at (et antal fastlagt af fabrikanten, dog højst 20) på hinanden følgende fejlslagne forsøg på ægthedsbekræftelse er konstateret, og/eller efter at det er konstateret, at bevægelsesfølerens identitet er ændret på et ikke tilladt tidspunkt (dvs. på et andet tidspunkt end under kalibrering af kontrolapparatet), skal sikkerhedsfunktionen:

— oprette en revisionspost over hændelsen,

— advare brugeren,

— fortsætte med at acceptere og benytte de ikke sikrede køredata, som afgives af bevægelsesføleren.

4.1.2. *Identificering og ægthedsbekræftelse af bruger*

UIA_207 Køretøjsenheden skal på permanent måde og selektivt spore identiteten af to brugere ved overvågning af de fartskriverkort, som indsættes i henholdsvis førerens og medchaufførens kortplads i apparatet.

UIA_208 Brugeridentiteten består af:

— en brugergruppe:

  — FØRER (førerkort),

  — TILSYNSFØRENDE (kontrolkort),

  — VÆRKSTED (værkstedskort),

  — VIRKSOMHED (virksomhedskort),

  — UKENDT (intet kort isat),

— en bruger-ID, bestående af:

  — den kortudstedende medlemsstats kode og kortnummeret,

  — UKENDT, hvis brugergruppen er UKENDT.

UKENDTE identiteter kan være implicit eller eksplicit kendte.

UIA_209 Køretøjsenheden skal ægthedsbekræfte sine brugere ved isætning af kortet.

UIA_210 Køretøjsenheden skal gentage ægthedsbekræftelsen af sine brugere:

— ved genetablering af strømforsyningen,

— periodisk eller efter indtræden af bestemte hændelser (fastlægges af fabrikanten, og hyppigere end én gang dagligt).

UIA_211 Ægthedsbekræftelse skal udføres på en måde, som godtgør, at det indsatte kort er et gyldigt fartskriverkort, hvorpå der ligger sikkerhedsdata, som kun systemet kan have distribueret. Ægthedsbekræftelsen skal være gensidig og skal udløses af køretøjsenheden.

UIA_212 Ud over ovenstående kræves, at værkstedet er ægthedsbekræftet ved en PIN-kode kontrol. PIN-koder skal være mindst 4-cifrede.

Bemærkning: I tilfælde, hvor PIN-koden overføres til køretøjsenheden fra udstyr uden for køretøjsenheden, placeret i nærheden af denne, behøver fortroligheden af PIN-koden ikke være beskyttet under overførslen.

UIA_213 Køretøjsenheden skal konstatere og forhindre eventuel brug af ægthedsbekræftelsesdata, som er kopieret og genafspillet.

UIA_214 Hvis der er konstateret 5 på hinanden følgende fejlslagne forsøg på ægthedsbekræftelse, skal sikkerhedsfunktionen:

— oprette en revisionspost over hændelsen,

— advare brugeren,

— antage at brugeren er UKENDT og kortet ugyldigt (definition z og krav 007).

4.1.3. *Identificering og ægthedsbekræftelse af en fjerntilsluttet virksomhed*

Mulighed for fjerntilslutning af virksomheder er ikke obligatorisk. Dette punkt finder derfor kun anvendelse, hvis denne facilitet er implementeret.

UIA_215 Ved enhver udveksling med en fjerntilsluttet virksomhed skal køretøjsenheden kunne fastslå virksomhedens identitet.

UIA_216 Den fjerntilsluttede virksomheds identitet består af koden for den medlemsstat, som har udstedt virksomhedskortet, samt dettes nummer.

UIA_217 Køretøjsenheden skal have ægthedsbekræftet den fjerntilsluttede virksomhed, før den tillader nogen overførsel af data til denne.

UIA_218 Ægthedsbekræftelse skal udføres på en måde, som godtgør, at virksomheden er indehaver af et gyldigt virksomhedskort, hvorpå der ligger sikkerhedsdata, som kun systemet kan have distribueret.

UIA_219 Køretøjsenheden skal konstatere og forhindre eventuel brug af ægthedsbekræftelsesdata, som er kopieret og genafspillet.

UIA_220 Hvis der er konstateret 5 på hinanden følgende fejlslagne forsøg på ægthedsbekræftelse, skal køretøjsenheden:

— advare den fjerntilsluttede virksomhed.

4.1.4. *Identificering og ægthedsbekræftelse af en styringsanordning*

Fabrikanter af køretøjsenheder kan tage højde for dedikerede anordninger bestemt til supplerende styrefunktioner for køretøjsenheden (f.eks. opgradering af programmel, genindlæsning af sikkerhedsdata mv.). Dette punkt finder derfor kun anvendelse, hvis denne facilitet er implementeret.

UIA_221 Ved enhver udveksling med en styringsanordning skal køretøjsenheden kunne fastslå anordningens identitet.

UIA_222 Før køretøjsenheden tillader yderligere vekselvirkning, skal den have bekræftet styringsanordningens ægthed.

UIA_223 Køretøjsenheden skal konstatere og forhindre brug af ægthedsbekræftelsesdata, som er kopieret og genafspillet.

4.2. ***Adgangskontrol***

Adgangskontrollen sikrer, at kun de, der er autoriseret dertil, kan læse data fra eller oprette eller ændre data i det evaluerede system.

Det skal bemærkes, at de brugerdata, som er registreret af køretøjsenheden, ikke er fortrolige, skønt de kan indeholde oplysninger, som tilhører privatlivets fred eller er kommercielt følsomme. Derfor er det funktionelle krav i forbindelse med læseadgang til data (krav 011) ikke omfattet af en sikkerhedsfunktion.

4.2.1. *Adgangskontrolregler*

ACC_201 Køretøjsenheden skal forvalte og kontrollere adgangen til funktioner og til data.

4.2.2. *Adgang til funktioner*

ACC_202 Køretøjsenheden skal håndhæve reglerne for valg af funktionsmåde (krav 006 til 009).

ACC_203 Køretøjsenheden skal med funktionsmåden håndhæve reglerne for kontrol med adgang til funktionerne (krav 010).

4.2.3. *Adgang til data*

ACC_204 Køretøjsenheden skal håndhæve reglerne for skriveadgang til køretøjsenhedens identifikationsdata (krav 076)

ACC_205 Køretøjsenheden skal håndhæve reglerne for skriveadgang til identifikationsdata for en samparret bevægelsesføler (krav 079 og 155)

ACC_206 Efter aktivering af køretøjsenheden skal denne sikre, at det kun i kalibreringsfunktion er muligt at indlæse kalibreringsdata i køretøjsenheden og gemme dem i dens datalager (krav 154 og 156).

ACC_207 Efter aktivering af køretøjsenheden skal denne håndhæve reglerne for skriveadgang til og sletning af kalibreringsdata (krav 097).

ACC_208 Efter aktivering af køretøjsenheden skal denne sikre, at det kun i kalibreringsfunktion er muligt at indlæse justeringsdata i køretøjsenheden og gemme dem i dens datalager (dette krav finder ikke anvendelse på de små tidsjusteringer, som krav 157 og 158 giver mulighed for).

ACC_209 Efter aktivering af køretøjsenheden skal denne håndhæve reglerne for adgang til at skrive og slette tidsjusteringsdata (krav 100).

ACC_210 Køretøjsenheden skal håndhæve passende regler for læse- og skriveadgang til sikkerhedsdata (krav 080).

4.2.4. *Filstruktur og adgangsbetingelser*

ACC_211 Filstruktur og adgangsbetingelser for applikations- og datafiler skal etableres i produktionsfasen og skal derefter være spærret for enhver efterfølgende ændring eller sletning.

4.3. ***Reviderbarhed***

ACT_201 Køretøjsenheden skal sikre, at føreres aktiviteter er eftervisbare (krav 081, 084, 087, 105a, 105b, 109 og 109a).

ACT_202 Køretøjsenheden skal opbevare permanente identifikationsdata (krav 075).

ACT_203 Køretøjsenheden skal sikre, at værksteders aktiviteter er eftervisbare (krav 098, 101 og 109).

ACT_204 Køretøjsenheden skal sikre, at tilsynsførendes aktiviteter kan eftervises (krav 102, 103 og 109).

ACT_205 Køretøjsenheden skal registrere kilometerstandsdata (krav 090) og detaljerede hastighedsdata (krav 093).

ACT_206 Køretøjsenheden skal sikre, at brugerdata vedrørende krav 081 til 093 og 102 til 105b inkl. ikke ændres, når først de er registreret, bortset fra at ældste lagrede data udskiftes med nye.

ACT_207 Køretøjsenheden skal sikre, at den ikke ændrer data, som i forvejen er lagret på et fartskriverkort (krav 109 og 109a), bortset fra udskiftning af ældste lagrede data med nye (krav 110) og det i bemærkningen til punkt 2.1 i tillæg 1 beskrevne tilfælde.

4.4. ***Revision***

Revisionsmulighed kræves kun for hændelser, som kan tyde på manipulation eller forsøg på sikkerhedsbrud. Der kræves ikke mulighed for revision af normal brug af rettigheder, selv om det er sikkerhedsmæssigt relevant.

AUD_201 Hændelser vedrørende køretøjsenhedens sikkerhed skal af køretøjsenheden registreres sammen med de tilhørende data (krav 094, 096 og 109).

AUD_202 Hændelser, som berører køretøjsenhedens sikkerhed, er følgende:

— Forsøg på sikkerhedsbrud:

  — Ægthedsbekræftelse for bevægelsesføler ikke lykkedes,

  — ægthedsbekræftelse for fartskriverkort ikke lykkedes,

  — ubeføjet skift af bevægelsesføler,

  — integritetsfejl i indlæste kortdata,

  — integritetsfejl i lagrede brugerdata,

  — fejl ved intern dataoverførsel,

  — ubehørig åbning af hus,

  — sabotage på maskinel,

— Seneste kortsession ikke korrekt afsluttet,

— Hændelsen fejl i køredata,

— Hændelsen afbrydelse af strømforsyning,

— Intern fejl i køretøjsenhed,

AUD_203 Køretøjsenheden skal håndhæve reglerne for lagring af revisionsposter (krav 094 og 096).

AUD_204 Køretøjsenheden skal i sit datalager opbevare revisionsposter, som er oprettet af bevægelsesføleren.

AUD_205 Revisionsposter skal kunne udskrives, vises på skærm og overføres.

4.5. ***Genbrug af objekter***

REU_201 Køretøjsenheden skal sikre, at midlertidigt lagrede objekter kan genbruges, uden at dette medfører uantagelig strøm af data.

4.6. ***Nøjagtighed***

4.6.1. *Regler for dataudvekslingskontrol*

ACR_201 Køretøjsenheden skal sikre, at brugerdata vedrørende krav 081, 084, 087, 090, 093, 102, 104, 105, 105a og 109 kun behandles ud fra de korrekte inddatakilder:

— køredata for køretøjet,

— køretøjsenhedens tidstro ur,

— kontrolapparatets kalibreringsparametre,

— fartskriverkort,

— brugerinddata.

ACR_201a Køretøjsenheden skal sikre, at brugerdata vedrørende krav 109a kun kan indlæses for perioden fra seneste udtagning af kort til aktuel isætning (krav 050a).

4.6.2. *Intern dataoverførsel*

Forskrifterne i dette afsnit finder kun anvendelse, hvis køretøjsenheden anvender fysisk adskilte dele.

ACR_202 Ved overførsel af data mellem fysisk adskilte dele af køretøjsenheden skal data være beskyttet mod ændring.

ACR_203 Ved konstatering af en dataoverførselsfejl under en intern overførsel skal overførslen gentages, og sikkerhedsfunktionen skal oprette en revisionspost for hændelsen.

4.6.3. *Integritet af lagrede data*

ACR_204 Køretøjsenheden skal kontrollere de brugerdata, som er lagret i dens hukommelse, for integritetsfejl.

ACR_205 Konstateres der en integritetsfejl i lagrede brugerdata, skal sikkerhedsfunktionen oprette en revisionspost.

4.7. ***Pålidelighed af service***

4.7.1. *Prøvning*

RLB_201 Alle kommandoer, operationer og testpunkter, som specielt tilhører produktionsfasen for køretøjsenheden, skal være sat ud af kraft eller fjernet, inden køretøjsenheden aktiveres. De må ikke kunne genetableres til senere brug.

RLB_202 Køretøjsenheden skal køre selvtest under den indledende opstart og under normal drift for at efterprøve, at den fungerer korrekt. Køretøjsenhedens selvtest skal omfatte integritetskontrol og sikkerhedsdata og integritetskontrol af lagret eksekverbar kode (hvis denne ikke ligger i ROM).

RLB_203 Ved detektion af en intern fejl under selvtest skal sikkerhedsfunktionen:

— oprette en revisionspost (undtagen i kalibreringsfunktion) (intern fejl i køretøjsenheden),

— Bevare integriteten af de lagrede data.

4.7.2. *Programmel*

RLB_204 Programmellet må ikke på nogen måde kunne analyseres eller fejlrettes i marken efter aktivering af køretøjsenheden.

RLB_205 Inddata fra eksterne kilder må ikke kunne accepteres som eksekverbar kode.

4.7.3. *Fysisk sikring*

RLB_206 Er køretøjsenheden konstrueret, så den kan åbnes, skal den detektere enhver åbning af huset, selv uden ekstern strømtilførsel, i mindst 6 måneder. I så fald skal sikkerhedsfunktionen oprette en revisionspost (det kan godtages, at revisionsposten oprettes og lagres efter genetablering af strømforsyningen).

Er køretøjsenheden således konstrueret, at den ikke kan åbnes, skal konstruktionen bevirke, at forsøg på fysisk manipulation let kan afsløres (f.eks. ved besigtigelse).

RLB_207 Efter aktivering skal køretøjsenheden detektere nærmere angivet (*angivet af fabrikanten*) sabotage på maskinel.

RLB_208 I ovennævnte tilfælde skal sikkerhedsfunktionen oprette en revisionspost, og bevægelsesføleren skal: (angives af fabrikanten).

4.7.4 *Afbrydelser i strømforsyningen*

RLB_209 Køretøjsenheden skal detektere afvigelser fra de foreskrevne værdier af strømforsyningen, herunder afbrydelse.

RLB_210 I ovennævnte tilfælde skal sikkerhedsfunktionen:

— oprette en revisionspost (undtagen i kalibreringsfunktion),

— bibeholde den sikre tilstand af køretøjsenheden,

— opretholde sikkerhedsfunktioner vedrørende de komponenter eller processer, som stadig er operationelle,

— bevare integriteten af de lagrede data.

4.7.5. *Nulstillingsbetingelser*

RLB_211 Ved afbrydelse af strømforsyningen, ved standsning af en transaktion før den er fuldført, samt ved enhver anden nulstillingsbetingelse skal køretøjsenheden nulstilles fuldstændig.

4.7.6. *Rådighed over data*

RLB_212 Køretøjsenheden skal sikre, at der er adgang til systemets enheder ved behov, og at systemets enheder ikke er genstand for unødig anmodning eller bibeholdelse.

RLB_213 Køretøjsenheden skal sikre, at der ikke kan frigives kort, før relevante data er lagret på dem (krav 015 og 016)

RLB_214 I ovennævnte tilfælde skal sikkerhedsfunktionen oprette en revisionspost for hændelsen.

4.7.7 *Flere applikationer samtidig*

RLB_215 Hvis køretøjsenheden tilfører systemet andre applikationer end fartskriverapplikationen, skal alle applikationer være fysisk og/eller logisk adskilt fra hinanden. Sådanne applikationer må ikke dele sikkerhedsdata. Kun én opgave må være aktiv ad gangen.

4.8. ***Dataudveksling***

Dette afsnit vedrører dataudveksling mellem køretøjsenheden og tilsluttede anordninger.

4.8.1. *Dataudveksling med bevægelsesføler*

DEX_201 Køretøjsenheden skal efterprøve integritet og ægthed af køredata, som er importeret fra bevægelsesføleren

DEX_202 Hvis der konstateres en integritets- eller ægthedsfejl ved køredata, skal sikkerhedsfunktionen:

— Oprette en revisionspost,

— fortsætte med at anvende importerede data.

4.8.2. *Dataudveksling med fartskriverkort*

DEX_203 Køretøjsenheden skal efterprøve integritet og ægthed af data, som er importeret fra fartskriverkort.

DEX_204 Ved konstatering af integritets- eller ægthedsfejl ved kortdata skal køretøjsenheden:

— Oprette en revisionspost,

— undlade at anvende de pågældende data.

DEX_205 Køretøjsenheden skal til fartskriverens chipkort afgive køredata med tilknyttede sikkerhedsattributter, som sætter kortet i stand til at verificere deres integritet og ægthed.

4.8.3 *Dataudveksling med eksterne lagermedier (downloading funktion))*

DEX_206 Køretøjsenheden skal generere oprindelsesdokumentation for data overført til eksterne medier.

DEX_207 Køretøjsenheden skal være i stand til at verificere oprindelsesdokumentationen for data overført til modtageren.

DEX_208 Køretøjsenheden skal overføre data til eksterne lagermedier med tilhørende sikkerhedsattributter, som gør det muligt at verificere integritet og ægthed af de overførte data.

4.9 ***Kryptografisk støtte***

Forskrifterne i dette punkt finder kun anvendelse, når der er behov, alt efter de anvendte sikkerhedsmekanismer og de af fabrikanten anvendte løsninger.

CSP_201 Enhver kryptografisk operation, som udføres af køretøjsenheden, skal være i overensstemmelse med en foreskreven algoritme og en foreskreven nøglestørrelse.

CSP_202 Hvis køretøjsenheden genererer kryptografiske nøgler, skal dette ske i overensstemmelse med foreskrevne algoritmer til generering af kryptografiske nøgler og foreskrevne kryptografiske nøglestørrelser.

CSP_203 Hvis køretøjsenheden distribuerer kryptografiske nøgler, skal dette ske i overensstemmelse med foreskrevne metoder til distribution af nøgler.

CSP_204 Giver køretøjsenheden adgang til kryptografiske nøgler, skal dette ske i overensstemmelse med foreskrevne metoder til nøgleadgang.

CSP_205 Hvis køretøjsenheden destruerer kryptografiske nøgler, skal dette ske i overensstemmelse med foreskrevne metoder til destruktion af nøgler.

5. **Fastlæggelse af sikkerhedsmekanismer**

De foreskrevne sikkerhedsmekanismer er angivet i tillæg 11.

Alle øvrige sikkerhedsmekanismer skal fastlægges af fabrikanterne.

6. **Minimumstyrke af sikkerhedsmekanismer**

Den mindste styrke af køretøjsenhedens sikkerhedsmekanismer er Høj i henhold til ITSEC.

7. **Sikkerhedsniveau**

Målet for køretøjsenhedens sikkerhedsniveau er ITSEC niveau E3, som defineret i henvisningen til ITSEC.

8. **Rationale**

Følgende matricer giver et rationale for sikkerhedsfunktioner ved at angive:

— hvilke sikkerhedsfunktioner eller midler, der modvirker hvilke risici,

— hvilke sikkerhedsfunktioner, der opfylder hvilke IT-sikkerhedsmål.

	Risici																		IT-mål								
	T.Access	T.Identification	T.Faults	T.Tests	T.Design	T.Calibration_Parameters	T.Card_Data_Exchange	T.Clock	T.Environment	T.Fake_Devices	T.Hardware	T.Motion_Data	T.Non_Activated	T.Output_Data	T.Power_Supply	T.Saturation	T.Security_Data	T.Software	T.Stored_Data	O.Access	O.Accountability	O.Audit	O.Authentication	O.Integrity	O.Output	O.Processing	O.Reliability	O.Secured_Data_Exchange
Fysiske, personalemæssige eller proceduremæssige midler																											
Udvikling			x	x	x																						
Produktion				x	x																						
Levering													x														
Aktivering	x												x														
Generering af sikkerhedsdata																	x										
Transport af sikkerhedsdata																	x										
Rådighed over kort		x																									
Et førerkort		x																									
Sporbarhed af kort		x																									
Godkendte værksteder						x		x																			
Regelmæssig kalibrering ved inspektion						x		x			x				x			x									
Pålidelige værksteder						x		x																			
Pålidelige førere		x														x											
Retlig kontrol		x				x		x	x		x		x		x		x	x									
Opgraderinger af programmel																		x									
Sikkerhedsfunktioner																											
Identificering og ægthedsbekræftelse																											
UIA_201 Identifikation af føler										x		x											x				x
UIA_202 Identitet af føler										x		x											x				
UIA_203 Ægthedsbekræftelse af føler										x		x											x				x
UIA_204 Gentagelse af identifikation og af ægthedsbekræftelse af føler										x		x											x				x
UIA_205 Forfalskningssikker ægthedsbekræftelse										x		x											x				
UIA_206 Svigt af ægthedsbekræftelse										x		x										x				x	
UIA_207 Identifikation af brugere	x	x								x										x			x				x
UIA_208 Brugeridentitet	x	x								x										x			x				
UIA_209 Ægthedsbekræftelse af bruger	x	x								x										x			x				x
UIA_210 Gentagelse af ægthedsbekræftelse af bruger	x	x								x										x			x				x
UIA_211 Midler til ægthedsbekræftelse	x	x								x										x			x				
UIA_212 PIN-kodekontrol	x	x				x		x												x			x				
UIA_213 Forfalskningssikker ægthedsbekræftelse	x	x								x										x			x				

	Risici																			IT-mål							
	T.Access	T.Identification	T.Faults	T.Tests	T.Design	T.Calibration_Parameters	T.Card_Data_Exchange	T.Clock	T.Environment	T.Fake_Devices	T.Hardware	T.Motion_Data	T.Non_Activated	T.Output_Data	T.Power_Supply	T.Saturation	T.Security_Data	T.Software	T.Stored_Data	O.Access	O.Accountability	O.Audit	O.Authentication	O.Integrity	O.Output	O.Processing	O.Reliability	O.Secured_Data_Exchange
UIA_214 Svigt af ægthedsbekræftelse	x	x								x												x					
UIA_215 Identifikation af fjernbruger	x	x																		x			x					x
UIA_216 Identitet af fjernbruger	x	x																		x			x					
UIA_217 Ægthedsbekræftelse af fjernbruger	x	x																		x			x					x
UIA_218 Midler til ægthedsbekræftelse	x	x																		x			x					
UIA_219 Forfalskningssikker ægthedsbekræftelse	x	x																		x			x					
UIA_220 Svigt af ægthedsbekræftelse	x	x																										
UIA_221 Identifikation af styringsanordning	x	x																		x			x					
UIA_222 Ægthedsbekræftelse af styringsanordning	x	x																		x			x					
UIA_223 Forfalskningssikker ægthedsbekræftelse	x	x																		x			x					
Adgangskontrol																												
ACC_201 Adgangskontrolregler	x					x		x									x		x	x								
ACC_202 Adgang til funktioner	x					x		x												x								
ACC_203 Adgang til funktioner	x					x		x												x								
ACC_204 VU ID																			x	x								
ACC_205 ID af tilsluttet føler										x									x	x								
ACC_206 Kalibreringsdata	x					x													x	x								
ACC_207 Kalibreringsdata						x													x	x								
ACC_208 Tidsjusteringsdata								x											x	x								
ACC_209 Tidsjusteringsdata								x											x	x								
ACC_210 Sikkerhedsdata																	x		x	x								
ACC_211 Filstruktur og adgangsbetingelser	x					x											x		x	x								
Reviderbarhed																												
ACT_201 Sporbarhed af førere																					x							
ACT_202 ID-data for køretøjsenheder																					x	x						
ACT_203 Reviderbarhed af værksteder																					x							
ACT_204 Reviderbarhed af tilsynsførende																					x							
ACT_205 Reviderbarhed af køretøjsbevægelser																					x							
ACT_206 Ændring af reviderbarhedsdata																			x				x			x		
ACT_207 Ændring af reviderbarhedsdata																			x				x			x		

	Risici																		IT-mål							
	T.Access	T.Identification	T.Faults	T.Tests	T.Design	T.Calibration_Parameters	T.Card_Data_Exchange	T.Clock	T.Environment	T.Fake_Devices	T.Hardware	T.Motion_Data	T.Non_Activated	T.Output_Data	T.Power_Supply	T.Saturation	T.Security_Data	T.Software	T.Stored_Data	O.Access	O.Accountability	O.Audit	O.Authentication	O.Integrity	O.Output	O.Processing	O.Reliability	O.Secured_Data_Exchange
Revision																												
AUD_201 Revisionsposter																						x						
AUD_202 Revisionsliste over hændelser	x						x				x	x		x	x				x			x						
AUD_203 Regler for lagring af revisionsposter																						x						
AUD_204 Revisionsposter for føler																						x						
AUD_205 Revisionsværktøjer																						x						
Genbrug																												
REU_201 Genbrug																	x									x	x	
Nøjagtighed																												
ACR_201 Regler for dataudvekslingskontrol							x			x		x														x	x	
ACR_202 Intern dataoverførsel														x											x	x	x	
ACR_203 Intern dataoverførsel														x								x						
ACR_204 Integritet af lagrede data																			x					x			x	
ACR_205 Integritet af lagrede data																			x			x						
Reviderbarhed																												
RLB_201 Prøvning i produktionen				x	x																						x	
RLB_202 Selvtest			x								x				x			x									x	
RLB_203 Selvtest											x				x			x				x						
RLB_204 Programmelanalyse					x													x									x	
RLB_205 Indlæsning af programmel																		x							x	x	x	
RLB_206 Åbning af hus					x			x		x			x			x	x	x							x		x	
RLB_207 Sabotage mod maskinel											x																x	
RLB_208 Sabotage mod maskinel											x											x						
RLB_209 Afbrydelser i strømforsyningen															x												x	
RLB_210 Afbrydelser i strømforsyningen															x							x						
RLB_211 Nulstilling			x																								x	
RLB_212 Rådighed over data																										x	x	
RLB_213 Frigivelse af kort																											x	
RLB_214 Kortsession ikke korrekt afsluttet																						x						
RLB_215 Flere applikationer samtidig																											x	
Dataudveksling																												
DEX_201 Sikret import af køredata												x																x
DEX_202 Sikret import af køredata												x										x						
DEX_203 Sikret import af kortdata							x																					x

	Risici																			IT-mål								
	T.Access	T.Identification	T.Faults	T.Tests	T.Design	T.Calibration_Parameters	T.Card_Data_Exchange	T.Clock	T.Environment	T.Fake_Devices	T.Hardware	T.Motion_Data	T.Non_Activated	T.Output_Data	T.Power_Supply	T.Saturation	T.Security_Data	T.Software	T.Stored_Data	O.Access	O.Accountability	O.Audit	O.Authentication	O.Integrity	O.Output	O.Processing	O.Reliability	O.Secured_Data_Exchange
DEX_204 Sikret import af kortdata							x															x						
DEX_205 Sikret dataeksport til kort							x																					x
DEX_206 Oprindelsesdokumentation														x											x			
DEX_207 Oprindelsesdokumentation														x											x			
DEX_208 Sikret eksport til eksterne medier														x											x			
Kryptografisk støtte																												
CSP_201 Algoritmer																											x	x
CSP_202 Nøglegenerering																											x	x
CSP_203 Nøgledistribution																											x	x
CSP_204 Nøgleadgang																											x	x
CSP_205 Nøgledestruktion																											x	x

FÆLLES SIKKERHEDSMÅL FOR FARTSKRIVERKORT

1. **Indledning**

Dette dokument indeholder en beskrivelse af fartskriverkortet, af de risici, det skal kunne imødegå, og af de sikkerhedsmæssige mål, det skal opfylde. Afsnittet angiver de foreskrevne sikkerhedsfunktioner. Det angiver den påberåbte minimumstyrke af sikkerhedsmekanismerne og det nødvendige sikkerhedsniveau under udvikling og evaluering.

De krav, der henvises til i dokumentet, er dem, som er angivet i hoveddelen af bilag I, del B. Af klarhedshensyn vil kravene i hoveddelen af bilag I, del B, undertiden blive gentaget i forskrifterne for sikkerhedsmål eller omvendt. Ved eventuel modstrid mellem en forskrift for sikkerhedsmål og de krav i hoveddelen af bilag I, del B, som der henvises til i dette krav til sikkerhedsmål, skal kravet i hoveddelen af bilag I, del B være afgørende.

De krav i hoveddelen af bilag I, del B, som der ikke henvises til i sikkerhedsmålene, er ikke omfattet af sikkerhedsfunktioner.

Et fartskriverkort er et sædvanligt chipkort, som bærer en dedikeret fartskriverapplikation og skal opfylde tidssvarende funktions- og sikkerhedskrav, som finder anvendelse på chipkort. Dette sikkerhedsmål omfatter derfor kun de ekstra sikkerhedskrav, som nødvendiggøres af fartskriverapplikationen.

For at kunne spores til udviklings- og evalueringsdokumentationen er risici, mål, proceduremæssige midler og specifikationer af sikkerhedsfunktioner tildelt unikke etiketter.

2. **Forkortelser, definitioner og henvisninger**

2.1. ***Forkortelser***

IC	Integreret kreds (elektronisk komponent, som er i stand til at behandle og/eller lagre data)
OS	Styresystem (operating system)
PIN	Personligt identifikationsnummer
ROM	Læselager (read only memory)
SFP	Regler for sikkerhedsfunktioner (security functions policy)
TBD	Fastlægges (to be defined)
TOE	Evalueret system (target of evaluation)
TSF	Sikkerhedsfunktion for evalueret system (TOE security function)
VU	Køretøjsenhed. (vehicle unit)

2.2. ***Definitioner***

Digital fartskriver	Kontrolapparat
Følsomme data	Data, som er lagret på fartskriveren og har behov for beskyttelse af hensyn til integritet, uautoriserede ændringer og fortrolighed (når dette er relevant for sikkerhedsdata). Følsomme data omfatter sikkerhedsdata og brugerdata
Sikkerhedsdata	De specifikke data, som er nødvendige til støtte for sikkerhedsfunktioner (f.eks. kryptografiske nøgler)
System	Apparater, personer eller organisationer, som på nogen måde er involveret i kontrolapparatet
Bruger	Enhver enhed (person eller ekstern IT-enhed) uden for det evaluerede system, som vekselvirker med det evaluerede system (når ordet ikke indgår i udtrykket »brugerdata«).

Brugerdata	Følsomme data, som er lagret på fartskriverkortet, bortset fra sikkerhedsdata. Brugerdata omfatter identifikationsdata og aktivitetsdata
Identifikationsdata	Identifikationsdata omfatter kortets identifikationsdata og kortindehaverens identifikationsdata
Kortidentifikationsdata	Brugerdata vedrørende identifikation af kort som defineret ved krav 190, 191, 192, 194, 215, 231 og 235
Kortindehaverens identifikationsdata	Brugerdata vedrørende identifikation af kortindehaver som defineret ved krav 195, 196, 216, 232 and 236
Aktivitetsdata	Aktivitetsdata omfatter aktivitetsdata for kortindehaver, data vedrørende hændelser og fejl samt kontrolaktivitetsdata
Aktivitetsdata for kortindehaver	Brugerdata vedrørende kortindehavers aktiviteter som defineret ved krav 197, 199, 202, 212, 212a, 217, 219, 221, 226, 227, 229, 230a, 233 og 237
Data vedrørende hændelser og fejl	Brugerdata vedrørende hændelser og fejl som defineret ved krav 204, 205, 207, 208 og 223
Kontrolaktivitetsdata	Brugerdata knyttet til retlig kontrol som fastlagt ved krav 210 og 225

2.3. ***Henvisninger***

ITSEC ITSEC Evalueringskriterier for informationsteknologi 1991 (Information Technology Security Evaluation Criteria 1991)

IC PP Smartcard Integrated Circuit Protection Profile — version 2.0 — issue September 1998. Registreret hos det franske certificeringsorgan under nummer PP/9806

ES PP Smart Card Integrated Circuit With Embedded Software Protection Profile — version 2.0 — issue June 99. Registreret hos det franske certificeringsorgan under nummer PP/9911

3. **Produktrationale**

3.1. ***Beskrivelse og anvendelse af fartskriverkortet***

Et fartskriverkort er et chipkort, som svarer til beskrivelsen i henvisning IC PP og henvisning ES PP, og som indeholder en applikation, der er bestemt til anvendelse af kortet sammen med kontrolapparatet.

Fartskriverkortets basisfunktioner er følgende:

— at lagre identifikationsdata for kort og for kortindehaver. Disse data anvendes af køretøjsenheden til at identificere kortindehaveren, til at tilvejebringe funktioner og dataadgang i henhold dertil, og til at sikre reviderbarhed af kortindehaverens aktiviteter.

— at lagre aktivitetsdata for kortindehaver, data vedrørende hændelser og fejl samt kontrolaktivitetsdata vedrørende kortindehaveren.

Et fartskriverkort er således bestemt til at anvendes i køretøjsenhedens kortlæser. Det kan endvidere benyttes i enhver anden kortlæser (f.eks i en PC), som skal have fuld læseadgang til alle brugerdata.

I anvendelsesfasen af et fartskriverkorts levetidscyklus (fase 7 af levetidscyklusen som beskrevet i ES PP) må køretøjsenheder kun skrive brugerdata på kortet.

De funktionelle krav til fartskriverkort er angivet i hoveddelen af bilag I, del B og tillæg 2.

3.2. ***Fartskriverkortets levetidscyklus***

Fartskriverkortets levetidscyklus er i overensstemmelse med levetidscyklus for chipkort som beskrevet i henvisning ES PP.

3.3. ***Risici***

Ud over de generelle risici mod chipkortet, som er angivet i ES PP og henvisning IC PP, kan fartskriverkortet være udsat for følgende risici.

3.3.1. *Endeligt mål*

Angribernes endelige mål vil være at ændre i brugerdata, som er lagret i det evaluerede system.

T.Ident_Data	Hvis det var muligt at ændre i de identifikationsdata, som ligger i det evaluerede system (f.eks kortets art, kortets udløbsdato eller kortindehaverens identifikationsdata), ville det give mulighed for svigagtig brug af det evaluerede system, hvilket ville udgøre en alvorlig trussel mod systemets overordnede sikkerhedsmål
T.Activity_Data	Hvis der kan ændres i de aktivitetsdata, der er lagret i det evaluerede system, vil dette være en trussel mod sikkerheden af det evaluerede system
T.Data_Exchange	Hvis der (ved tilføjelse, sletning eller ændring) kan ændres i aktivitetsdata under import eller eksport, vil dette være en sikkerhedstrussel mod det evaluerede system

3.3.2. *Angrebsveje*

Det evaluerede system kan angribes af:

— forsøg på at opnå uretmæssigt kendskab til udformningen af maskinel og programmel i det evaluerede system, specielt dets sikkerhedsfunktioner eller sikkerhedsdata. Uretmæssigt kendskab kan opnås ved angreb på konstruktørens eller fabrikantens materiale (tyveri, bestikkelse osv.) eller ved direkte undersøgelse af det evaluerede system (fysisk sondering, interferensanalyse mv.).

— udnyttelse af konstruktionsmæssige eller produktionsmæssige svagheder i det evaluerede system (udnyttelse af maskinelfejl, programmelfejl, dataoverførselsfejl, fejl fremkaldt af miljøbelastning, udnyttelse af svagheder i sikkerhedsfunktioner som ægthedsbekræftelse, dataadgangskontrol, kryptografiske operationer osv.).

— ændringer af det evaluerede system eller dets sikkerhedsfunktioner gennem fysiske, elektriske eller logiske angreb eller en kombination deraf.

3.4. ***Sikkerhedsmål***

De sikkerhedsmæssige hovedmål for det samlede digitale fartskriversystem er følgende:

O.Main	Data, som skal kontrolleres af den tilsynsførende myndighed, skal være til rådighed og fuldstændigt og nøjagtigt afspejle de kontrollerede føreres og køretøjers aktiviteter hvad angår køre-, arbejde, rådigheds- og hvileperioder samt køretøjets hastighed.

Det evaluerede system har derfor følgende sikkerhedsmæssige mål som led i dette overordnede sikkerhedsmål:

O.Card_Identification_Data	Det evaluerede system skal bevare kortidentifikationsdata og kortindehaverens identifikationsdata, som er lagret under personaliseringen af kortet
O.Card_Activity_Storage	Det evaluerede system skal opbevare brugerdata, som gemmes på kortet af køretøjsenheder

3.5. ***Informationsteknologiske sikkerhedsmål***

Ud over de generelle sikkerhedsmål for chipkort, som er angivet i henvisning ES PP og henvisning IC PP, har det evaluerede system følgende særlige IT-sikkerhedsmål, som indgår i dets sikkerhedsmæssige hovedmål i anvendelsesfasen af dets levetidscyklus:

O.Data_Access	Det evaluerede system skal indskrænke brugernes adgang til at skrive data til ægthedsbekræftede køretøjsenheder.
O.Secure_Communications	Når applikationen gør det nødvendigt, skal det evaluerede system understøtte protokoller og procedurer for sikker kommunikation mellem kort og kortlæser.

3.6. ***Fysiske, personalemæssige og proceduremæssige midler***

De fysiske, personalemæssige og proceduremæssige midler, som er et led i sikkerheden af det evaluerede system, er angivet i henvisning ES PP og henvisning IC PP (inddeling af sikkerhedsmål for miljøet).

4. **Sikkerhedsfunktioner**

I dette afsnit videreudvikles visse af de tilladte operationer som tilordning eller valg af henvisning ES PP, og der fastsættes supplerende funktionskrav til sikkerhedsfunktioner.

4.1. ***Overensstemmelse med sikringsprofiler***

CPP_301 Det evaluerede system skal være i overensstemmelse med henvisning IC PP.

CPP_302 Det evaluerede system skal være i overensstemmelse med henvisning ES PP, når dette er videreudviklet.

4.2. ***Identificering og ægthedsbekræftelse af bruger***

Kortet skal identificere den enhed, som det er indsat i, og skal fastslå, om det er en ægthedsbekræftet køretøjsenhed eller ikke. Kortet kan eksportere alle brugerdata uanset hvilken enhed, det er tilsluttet, bortset fra kontrolkortet, som kan eksportere kortindehaverens identifikationsdata alene til ægthedsbekræftede køretøjsenheder (derved kan den tilsynsførende ved at se sit navn på skærmen eller på udskrifterne forvisse sig om, at køretøjsenheden ikke er falsk).

4.2.1. *Identifikation af bruger*

Tilordning (FIA_UID.1.1) *Liste over operationer formidlet af sikkerhedsfunktioner*: Ingen.

Tilordning (FIA_ATD.1.1) *Liste over sikkerhedsattributter*:

USER_GROUP: VEHICLE_UNIT, NON_VEHICLE_UNIT,

USER_ID: Køretøjets indregistreringsnummer (VRN) og den registrerende medlemsstats kode (USER_ID kendes kun for USER_GROUP = VEHICLE_UNIT).

4.2.2. *Ægthedsbekræftelse af bruger*

Tilordning (FIA_UAU.1.1) *Liste over operationer formidlet af sikkerhedsfunktioner*:

— Fører- og værkstedskort: Eksportere brugerdata med sikkerhedsattributter (dataoverførsel fra kort),

— Kontrolkort: Eksportere brugerdata uden sikkerhedsattributter undtagen kortindehavers identifikationsdata.

UIA_301 Ægthedsbekræftelse af en køretøjsenhed skal udføres ved at eftervise, at den indeholder sikkerhedsdata, som kun systemet kan have distribueret.

Valg (FIA_UAU.3.1 and FIA_UAU.3.2): Forebygge.

Tilordning (FIA_UAU.4.1) *Identificerede mekanismer til ægthedsbekræftelse*: Enhver mekanisme til ægthedsbekræftelse.

UIA_302 Værkstedskortet skal tilvejebringe en supplerende mekanisme til ægthedsbekræftelse gennem PIN-kode kontrol. (Hensigten med denne mekanisme er, at køretøjsenheden skal garantere kortindehaverens identitet, ikke at mekanismen skal sikre indholdet af værkstedskortet).

4.2.3. *Svigt af ægthedsbekræftelse*

Følgende tilordninger beskriver kortets reaktion på hver enkelt fejlslagen ægthedsbekræftelse af brugeren.

Tilordning (FIA_AFL.1.1) *Nummer*: 1, *liste over hændelser i forbindelse med ægthedsbekræftelse*: Ægthedsbekræftelse af en kortlæser.

Tilordning (FIA_AFL.1.2) *Liste over operationer*:

— advare den tilsluttede enhed,

— regne brugeren for en NON_VEHICLE_UNIT.

Følgende tilordninger beskriver kortets reaktion ved fejlslagen gennemførelse af den ekstra ægthedsbekræftelsesmekanisme, som kræves i UIA_302.

Tilordning (FIA_AFL.1.1) *Nummer*: 5, *liste over hændelser i forbindelse med ægthedsbekræftelse*: PIN-kontrol (værkstedskort).

Tilordning (FIA_AFL.1.2) *Liste over operationer*:

— advare den tilsluttede enhed,

— spærre PIN-kodekontrollen, så ethvert efterfølgende PIN-kodeforsøg vil slå fejl,

— kunne angive grunden til spærringen over for efterfølgende brugere.

4.3. ***Adgangskontrol***

4.3.1. *Adgangskontrolregler*

I anvendelsesfasen af sin levetidscyklus er fartskriverkortet genstand for ét sæt sikkerhedsfunktionsregler for adgangskontrol, som benævnes AC_SFP.

Tilordning (FDP_ACC.2.1) *Sikkerhedsfunktionsregler for adgangskontrol*: AC_SFP.

4.3.2. *Adgangskontrolfunktioner*

Tilordning (FDP_ACF.1.1) *Sikkerhedsfunktionsregler for adgangskontrol:* AC_SFP.

Tilordning (FDP_ACF.1.1) *Benævnt gruppe sikkerhedsattributter*: USER_GROUP.

Tilordning (FDP_ACF.1.2) *Regler for adgangsstyring for kontrollerede personer og kontrollerede objekter, som anvender kontrollerede operationer på kontrollerede objekter*:

— GENERAL_READ: Brugerdata kan læses fra det evaluerede system af enhver bruger, bortset fra kortindehaverens identifikationsdata, som alene kan læses fra kontrolkortene af VEHICLE_UNIT.

— IDENTIF_WRITE: Identifikationsdata kan kun skrives én gang og inden slutningen af fase 6 i kortets levetidscyklus. Ingen bruger kan skrive eller ændre identifikationsdata i anvendelsesfasen af kortets levetidscyklus.

— ACTIVITY_WRITE: Kun VEHICLE_UNIT kan skrive til det evaluerede system.

— SOFT_UPGRADE: Ingen bruger må opgradere programmellet i det evaluerede system.

— FILE_STRUCTURE: Filstruktur og adgangsbetingelser for applikations- og datafiler skal være etableret før slutningen af fase 6 i levetidscyklusen for det evaluerede system og skal derefter være spærret for enhver efterfølgende ændring eller sletning foretaget af nogen bruger.

4.4. ***Reviderbarhed***

ACT_301 Det evaluerede system skal indeholde permanente identifikationsdata.

ACT_302 Der skal være en angivelse af dato og klokkeslæt for personaliseringen af det evaluerede system. Denne angivelse må til stadighed ikke kunne ændres.

4.5. ***Revision***

Området under evaluering skal overvåge hændelser, som tyder på en eventuel trussel mod dets sikkerhed.

Tilordning (FAU_SAA.1.2) *Subsæt af definerede reviderbare hændelser*:

— mislykket ægthedsbekræftelse af kortindehaver (5 på hinanden følgende fejlslagne PIN-kodeforsøg),

— selvtestfejl,

— integritetsfejl i lagrede data,

— integritetsfejl i indlæste aktivitetsdata.

4.6. ***Nøjagtighed***

4.6.1. *Integritet af lagrede data*

Tilordning (FDP_SDI.2.2) *Nødvendige tiltag*: Advar den tilsluttede enhed,

4.6.2. *Ægthedsbekræftelse af basisdata*

Tilordning (FDP_DAU.1.1) *Liste over objekter eller informationstyper*: Identifikationsdata.

Tilordning (FDP_DAU.1.2) *Liste over personer*: En vilkårlig.

4.7. ***Pålidelighed af service***

4.7.1. *Prøver*

Valg (FPT_TST.1.1): Ved den indledende opstart, og periodisk under normal drift.

Bemærkning: »Under den indledende opstart« vil sige: Før programkoden eksekveres (og ikke nødvendigvis under proceduren svar på nulstilling).

RLB_301 Selvtest for det evaluerede system skal omfatte integritetskontrol af al programkode, som ikke ligger i læselageret.

RLB_302 Ved konstatering af en selvtestfejl skal sikkerhedsfunktionen advare den tilsluttede enhed.

RLB_303 Når prøvning af styresystemet er gennemført, skal alle prøvningsspecifikke kommandoer og operationer sættes ud af kraft eller fjernes. Det må ikke være muligt at tilsidesætte disse styreredskaber og genetablere dem til senere brug. Når en kommando udelukkende er knyttet til én tilstand i levetidscyklusen, må der aldrig være adgang til kommandoen i nogen anden tilstand.

4.7.2. *Programmel*

RLB_304 Programmellet for det evaluerede system må ikke på nogen måde kunne analyseres eller fejlrettes i marken.

RLB_305 Inddata fra eksterne kilder må ikke kunne accepteres som eksekverbar kode.

4.7.3. *Strømforsyning*

RLB_306 Ved afbrydelse eller uregelmæssigheder i strømforsyningen skal det evaluerede system opretholde en sikker tilstand.

4.7.4. *Nulstillingsbetingelser*

RLB_307 Ved afbrydelse eller styrkevariationer af strømforsyningen til det evaluerede system, ved standsning af en transaktion, før den er fuldført, samt ved enhver anden nulstillingsbetingelse skal det evaluerede system nulstilles fuldstændigt.

4.8. ***Dataudveksling***

4.8.1. *Dataudveksling med en køretøjsenhed*

DEX_301 Det evaluerede system skal efterprøve integritet og ægthed af data, som er importeret fra en køretøjsenhed.

DEX_302 Ved konstatering af en integritetsfejl på importerede data skal det evaluerede system:

— Advare den enhed, der sender de pågældende data,

— undlade at anvende de pågældende data.

DEX_303 Det evaluerede system skal afgive brugerdata til køretøjsenheden med tilknyttede sikkerhedsattributter, som sætter køretøjsenheden i stand til at verificere integritet og ægthed af de modtagne data.

4.8.2. *Eksport af data til andet end en køretøjsenhed (downloading-funktion)*

DEX_304 Det evaluerede system skal generere oprindelsesdokumentation for data overført til eksterne medier.

DEX_305 Det evaluerede system skal være i stand til at verificere oprindelsesdokumentationen for data overført til modtageren.

DEX_306 Det evaluerede system skal overføre data til eksterne lagermedier med tilhørende sikkerhedsattributter, som gør det muligt at verificere integriteten af de overførte data.

4.9. ***Kryptografisk støtte***

CSP_301 Hvis sikkerhedsfunktionen genererer kryptografiske nøgler, skal dette ske i overensstemmelse med foreskrevne algoritmer til generering af kryptografiske nøgler og foreskrevne kryptografiske nøglestørrelser. Genererede kryptografiske sessionsnøgler skal have et begrænset antal (antallet angives af fabrikanten og må højst være 240) mulige anvendelser.

CSP_302 Hvis sikkerhedsfunktionen distribuerer kryptografiske nøgler, skal dette ske i overensstemmelse med foreskrevne metoder til distribution af kryptografiske nøgler.

5. **Fastlæggelse af sikkerhedsmekanismer**

De foreskrevne sikkerhedsmekanismer er angivet i tillæg 11.

Alle øvrige sikkerhedsmekanismer skal fastlægges af fabrikanten af området under evaluering.

6. **Påberåbt minimumstyrke af mekanismer**

Den mindste styrke af fartskriverkortets sikkerhedsmekanismer er Høj i henhold til ITSEC.

7. **Sikkerhedsniveau**

Målet for fartskriverkortets sikkerhedsniveau er ITSEC niveau E3, som defineret i henvisningen til ITSEC.

8. **Rationale**

Følgende matricer giver et rationale for ekstra sikkerhedsfunktioner ved at angive:

— hvilke sikkerhedsfunktioner, der modvirker hvilke risici,

— hvilke sikkerhedsfunktioner, der opfylder hvilke IT-sikkerhedsmål.

	Risici											IT-mål								
	T.CLON*	T.DIS_ES2	T.T_ES	T.T_CMD	T.MOD_SOFT*	T.MOD_LOAD	T.MOD_EXE	T.MOD_SHARE	T.Ident_Data	T.Activity_Data	T.Data_Exchange	O.TAMPER_ES	O.CLON*	O.OPERATE*	O.FLAW*	O.DIS_MECHANISM2	O.DIS_MEMORY*	O.MOD_MEMORY*	O.Data_Access	O.Secured_Communications
UIA_301 Midler til ægthedsbekræftelse																			x	
UIA_302 PIN-kodekontrol																			x	
ACT_301 Identifikationsdata																				
ACT_302 Personaliseringsdato																				
RLB_301 Integritet af programmel												x		x						
RLB_302 Selvtest												x		x						
RLB_303 Prøvning i produktionen					x	x						x		x						
RLB_304 Programmelanalyse					x		x	x				x		x						
RLB_305 Indlæsning af programmel					x	x		x				x		x						
RLB_306 Strømforsyning									x	x		x		x						
RLB_307 Nulstilling												x		x						
DEX_301 Sikret import af data											x									x
DEX_302 Sikret import af data											x									x
DEX_303 Sikret eksport af data til køretøjsenhed											x									x
DEX_304 Oprindelsesdokumentation											x									x
DEX_305 Oprindelsesdokumentation											x									x
DEX_306 Sikret eksport til eksterne medier											x									x
CSP_301 Nøglegenerering												x								x
CSP_302 Nøgledistribution												x								x

Tillæg 11

FÆLLES SIKKERHEDSMEKANISMER

1. GENERELT

Dette tillæg foreskriver de sikkerhedsmekanismer, som sikrer:

— den gensidige ægthedskontrol mellem køretøjsenheder og fartskriverkort, herunder aftale om sessionsnøgle,

— fortrolighed, integritet og ægthed af data overført mellem køretøjsenheder og fartskriverkort,

— integritet og ægthed af data overført fra køretøjsenheder til eksterne lagermedier,

— integritet og ægthed af data overført fra fartskriverkort til eksterne lagermedier.

1.1. **Henvisninger**

I dette tillæg henvises til følgende referencer:

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. Udkast 1999
TDES-OP	ANSI X9.52, Triple Data Encryption Algorithm Modes of Operation. 1998
ISO/IEC 7816-4	Information Technology — Identification cards — Integrated circuit(s) cards with contacts — Part 4: Interindustry commands for interexchange. Første udgave: 1995 + Ændring 1: 1997
ISO/IEC 7816-6	Information Technology — Identification cards — Integrated circuit(s) cards with contacts — Part 6: Interindustry data elements. Første udgave: 1996 + Cor 1: 1998
ISO/IEC 7816-8	Information Technology — Identification cards — Integrated circuit(s) cards with contacts — Part 8: Security related interindustry commands. Første udgave 1999
ISO/IEC 9796-2	Information Technology — Security techniques — Digital signature schemes giving message recovery — Part 2: Mechanisms using a hash function. Første udgave: 1997
ISO/IEC 9798-3	Information Technology — Security techniques — Entity authentication mechanisms — Part 3: Entity authentication using a public key algorithm. Anden udgave 1998
ISO 16844-3	Road vehicles — Tachograph systems — Part 3: Motion sensor interface

1.2. **Notation og forkortelser**

I dette tillæg bruges følgende notation og forkortelser:

(K_a, K_b, K_c)	Et nøglebundt til brug for den tredobbelte datakrypteringsalgoritme
CA	Certificeringsmyndighed (Certification authority)
CAR	Henvisning til certificeringsmyndighed (Certification authority reference)
CC	Kryptografisk kontrolsum
CG	Kryptogram
CH	Kommandoheader
CHA	Certifikatindehavers autorisation (Certificate holder authorisation)
CHR	Henvisning til certifikatindehaver (Certificate holder reference)
D()	Dekryptering med DES
DE	Dataelement
DO	Dataobjekt
d	Privat RSA-nøgle, privat eksponent
e	Offentlig RSA-nøgle, offentlig eksponent
E()	Kryptering med DES
EQT	Udstyr (Equipment)
Hash()	Sætte hash-værdi på et *Hash*-resultat
Hash	Hash-funktion
KID	Nøgleidentifikator (Key identifier)
Km	TDES-nøgle, hovednøgle defineret i ISO 16844-3
Km_{VU}	TDES-nøgle indsat i køretøjsenheder.
Km_{WC}	TDES-nøgle indsat i værkstedskort.
m	Repræsenterer en meddelelse, heltal mellem 0 og *n*-1
n	RSA-nøgler, modulus
PB	Udfyldningsbytes (Padding bytes)
PI	Udfyldningsindikatorbyte (til brug i kryptogram til fortrolighedsdataobjekt)
PV	Ordinær dataværdi (Plain value)
s	Repræsenterer en underskrift, et heltal mellem 0 og *n*-1
SSC	Sendesekvenstæller (Send sequence counter)
SM	Sikker meddelelsesoverførsel
TCBC	TDEA kryptografering med blokkædningsfunktion (TDEA cipher block chaining mode of operation)
TDEA	Algoritme til tredobbelt datakryptering (Triple data encryption algorithm)
TLV	Mærkatlængde (Tag length value)
FE	Køretøjsenhed (Vehicle unit)
X.C	Certifikat for bruger X, udstedt af en certificeringsmyndighed
X.CA	Certificeringsmyndighed for bruger X
$X.CA.PK_oX.C$	Operation, som består i at udpakke et certifikat for at uddrage en offentlig nøgle. Der er tale om en operator af infix-typen, der som venstre operand har certificeringsmyndighedens offentlige nøgle og som højre operand certifikatet udstedt af den pågældende certificeringsmyndighed. Resultatet er den offentlige nøgle for brugeren X, hvis certifikat er den højre operand

X.PK	Offentlig RSA-krypteringsnøgle for bruger X
X.PK[I]	RSA-krypteringen af en vilkårlig oplysning I ved hjælp af den offentlige nøgle fra bruger X
X.SK	Privat RSA-nøgle for bruger X
X.SK[I]	RSA-kryptering af en vilkårlig oplysning I ved hjælp af den private nøgle fra bruger X
'xx'	Hexadecimal værdi
||	Sammenkædningsoperator

2. KRYPTOGRAFISKE SYSTEMER OG ALGORITMER

2.1. **Kryptografiske systemer**

CSM_001 Køretøjsenheder og fartskriverkort skal anvende et kryptografisk system med en klassisk offentlig RSA-nøgle til at tilvejebringe følgende sikkerhedsmekanismer:

— ægthedsbekræftelse mellem køretøjsenheder og kort,

— transport af tredobbelte DES-sessionsnøgler mellem køretøjsenheder og fartskriverkort,

— digital underskrift af data, som er overført fra køretøjsenhederne eller fra fartskriverkort til eksterne medier.

CSM_002 I køretøjsenheder og fartskriverkort skal anvendes et tredobbelt symmetrisk DES-kryptograferingssystem til sikring af dataintegritet under udveksling af brugerdata mellem køretøjsenheder og fartskriverkort og til, i givet fald, at sikre fortroligheden af dataoverførsel mellem køretøjsenheder og fartskriverkort.

2.2. **Kryptografiske algoritmer**

2.2.1. ***RSA-algoritme***

CSM_003 RSA-algoritmen er fuldt defineret ved følgende relationer:

$$X.SK[m] = s = m^d \bmod n$$

$$X.PK[s] = m = s^e \bmod n$$

En mere fuldstændig beskrivelse af RSA-funktionen findes i henvisning PKCS1.

2.2.2. ***Hash-algoritme***

CSM_004 Mekanismerne til digital underskrift skal anvende SHA-1 hashalgoritmen som defineret i henvisning SHA-1.

2.2.3. ***Algoritme til datakryptering***

CSM_005 Der skal anvendes DES-baserede algoritmer i blokkædnings-funktionsmåde.

3. NØGLER OG CERTIFIKATER

3.1. **Generering og distribution af nøgler**

3.1.1. ***Generering og distribution af RSA-nøgler***

CSM_006 RSA-nøgler skal genereres i tre funktionelle hierarkiske niveauer:

— europæisk niveau,

— medlemsstatsniveau,

— apparatniveau.

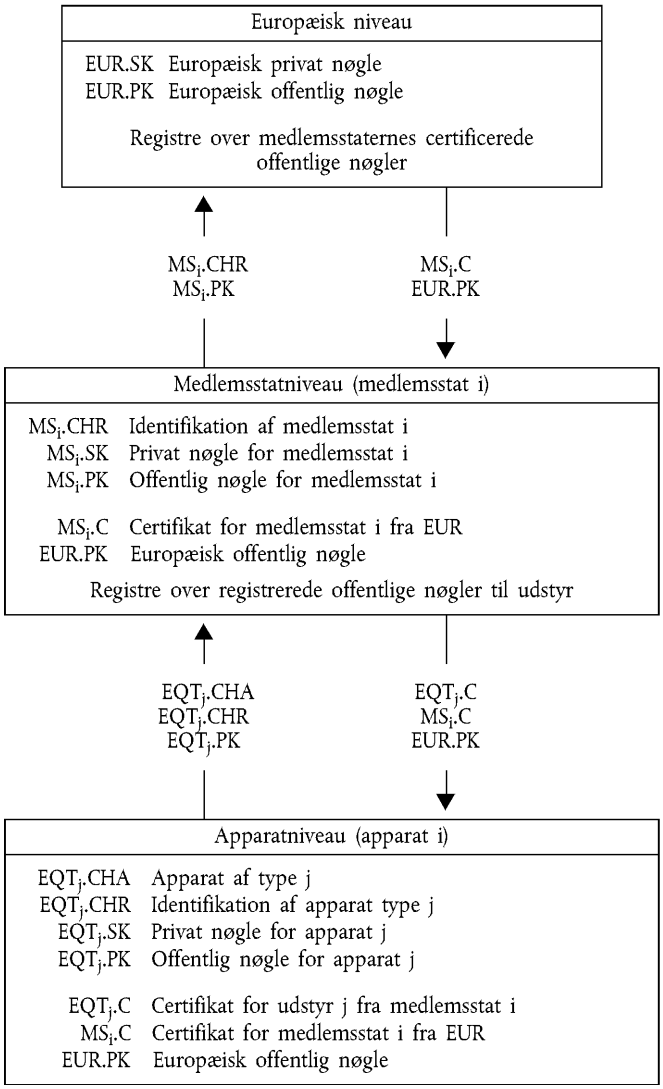
CSM_007 På europæisk niveau skal der genereres et enkelt europæisk nøglepar (EUR.SK og EUR.PK). Den europæiske private nøgle skal anvendes til at certificere medlemsstaternes offentlige nøgler. Der skal føres registre over alle certificerede nøgler. Disse opgaver udføres af en europæisk certificeringsmyndighed under Europa-Kommissionens myndighed og ansvar.

CSM_008 På medlemsstatniveau skal der genereres et medlemsstat-nøglepar (MS.SK og MS.PK). Medlemsstaternes offentlige nøgler skal være certificeret af den europæiske certificeringsmyndighed. Den private medlemsstatnøgle anvendes til at certificere de offentlige nøgler, som skal indsættes i udstyret (køretøjsenhed eller fartskriverkort). Der skal føres register over alle certificerede offentlige nøgler med identifikation af det udstyr, de er bestemt til. Disse opgaver varetages af en medlemsstats certificeringsmyndighed. En medlemsstat kan jævnligt skifte sit nøglepar.

CSM_009 På apparatniveau skal der genereres et enkelt nøglepar (EQT.SK og EQT.PK), som indsættes i hvert apparat. Apparatets offentlige nøgler skal certificeres af en medlemsstats certificeringsmyndighed. Disse opgaver kan varetages af udstyrsfabrikanter, af leverandører af individuelle tilpasninger af udstyr eller af medlemsstaternes myndigheder. Dette nøglepar anvendes til ægthedsbekræftelse, digital underskrift og og krypteringstjenester.

CSM_010 De private nøglers fortrolighed skal bibeholdes under generering, eventuel transport og opbevaring.

Følgende billede sammenfatter datastrømmen under denne proces:



3.1.2. ***RSA-prøvenøgler***

CSM_011 Til afprøvning af udstyr (herunder interoperabilitetsprøvning) skal den europæiske certificeringsmyndighed generere et uens par europæiske prøvenøgler og mindst to par medlemsstatprøvenøgler, af hvilke de offentlige nøgler skal certificeres med den europæiske private prøvenøgle. I det udstyr, som skal typegodkendes, skal fabrikanterne indsætte prøvenøgler, som er certificeret med en af medlemsstaternes prøvenøgler.

3.1.3. ***Nøgler til bevægelsesføler***

Generering, eventuel transport og opbevaring af de tre nedenfor beskrevne TDES-nøgler skal ske under iagttagelse af fuld fortrolighed.

For at understøtte kontrolapparater, som er i overensstemmelse med ISO 16844, skal den europæiske certificeringsmyndighed og medlemsstaternes certificeringsmyndigheder endvidere sikre følgende:

CSM_036 Den europæiske certificeringsmyndighed genererer Km_{VU} og Km_{WC}, to uafhængige og unikke tredobbelte DES nøgler, og generere Km som:

$$Km = Km_{VU} \text{ XOR } Km_{WC}$$

Den europæiske certificeringsmyndighed fremsender disse nøgler under brug af tilbørligt sikrede procedurer til medlemsstaternes certificeringsmyndigheder på disses anmodning.

CSM_037 Medlemsstaternes certificeringsmyndigheder skal:

— Anvende Km til kryptering af bevægelsesfølerdata, som begæres af fabrikanter af bevægelsesfølere (de data som skal krypteres med Km, er fastlagt i ISO 16844-3),

— Fremsende Km_{VU} fabrikanterne af køretøjseneheder under brug af behørigt sikrede procedurer, til indsætning i køretøjsenheder,

— Sørge for at Km_{WC} indsættes i alle værkstedskort (`SensorInstallationSecData` i elementærfilen `Sensor_Installation_Data`) under personalisering af kortet.

3.1.4. ***Generering og distribution af T-DES-sessionsnøgler***

CSM_012 Køretøjsenheder og fartskriverkort skal som del af den gensidige ægthedskontrol generere og udveksle de nødvendige data til udarbejdning af en tredobbelt fælles DES-sessionsnøgle. Denne dataudveksling skal være fortrolighedsbeskyttet ved RSA-kryptering.

CSM_013 Denne nøgle skal anvendes til alle efterfølgende kryptografiske operationer, hvor der anvendes sikker meddelelsesoverførsel. Dens gyldighed skal udløbe ved sessionens afslutning (udtagning eller genindsætning af kort) og/eller efter 240 anvendelser (én anvendelse af nøglen = én kommando med sikker meddelelsesoverførsel sendt til kortet, samt det tilhørende svar).

3.2. **Nøgler**

CSM_014 RSA-nøgler skal (uanset niveau) have følgende længde: modulus *n* 1024 bit, offentlig eksponent *e* maks. 64 bit, privat eksponent *d* 1024 bit.

CSM_015 Tredobbelte DES-nøgler skal have formen (K_a, K_b, K_a), hvor K_a og K_b er uafhængige 64 bit lange nøgler. Der skal ikke sættes paritetsbit.

3.3. **Certifikater**

CSM_016 Certifikater med offentlig RSA-nøgle skal være »ikke selvdeskriptive« og »verificerbare med kort« (Ref.: ISO/IEC 7816-8)

3.3.1. ***Certifikaters indhold***

CSM_017 Certifikater med offentlig RSA-nøgle er opbygget med følgende data i følgende rækkefølge:

Data	Format	Bytes	Bemærkninger
CPI	INTEGER	1	Certifikatprofil-identifikator ('01' for denne version)
CAR	OCTET STRING	8	Henvisning til certificeringsmyndighed (Certification authority reference)
CHA	OCTET STRING	7	Certifikatindehavers autorisation (Certificate holder authorisation)
EOV	TimeReal	4	Certifikatets udløbsdato (End of validity). Ikke obligatorisk, udfyldt med 'FF' hvis det ikke benyttes.
CHR	OCTET STRING	8	Henvisning til certifikatindehaver (Certificate holder reference)
n	OCTET STRING	128	Offentlig nøgle (modulus)
e	OCTET STRING	8	Offentlig nøgle (offentlig eksponent)
		164	

Bemærkninger:

1. »Certifikatprofil-identifikatoren« (CPI) beskriver den nøjagtige opbygning af et ægthedscertifikat. Den kan bruges som intern identifikator for udstyret i en relevant headerliste, som beskriver sammenkædningen af dataelementer i certifikatet.

   Den headerliste, der er knyttet til indholdet af dette certifikat, er som følger:

'4D'	'16'	'5F 29'	'01'	'42'	'08'	'5F 4B'	'07'	'5F 24'	'04'	'5F 20'	'08'	'7F 49'	'05'	'81'	'81 80'	'82'	'08'
Mærkat for udvidet headerliste	Længde af headerliste	Mærkat for CPI	CPI-længde	CAR-mærkat	CAR-længde	CHA-mærkat	CHA-længde	EOV-mærkat	EOV-længde	CHR-mærkat	CHR-længde	Mærkat for offentlig nøgle (konstrueret)	Længde af efter følgende dataobjekter	Modulus-mrkat	Modulus-længde	Mærkat for offentlig nøgle	Længde af offentlig eksponent

2. »Henvisning til certificeringsmyndighed« (CAR) har til formål at identificere den certifikatudstedende myndighed på en sådan måde, at dataelementet samtidig kan anvendes som identifikator for en myndigheds nøgle og henvise til certificeringsmyndighedens offentlige nøgle (vedrørende kodning henvises til nøgleidentifikatoren nedenfor).

3. »Certifikatindehavers autorisation« (CHA) anvendes til at identificere certifikatindehaverens rettigheder. Den består af fartskriverapplikationens ID og af den art udstyr, som certifikatet er bestemt til (i henhold til dataelementet `EquipmentType`, »00« for en medlemsstat).

4. »Henvisning til certifikatindehaver« (CHR) har til formål at identificere certifikatindehaveren entydigt, således at dataelementet på én gang kan anvendes som identifikator for en persons nøgle og henvise til certifikatindehaverens offentlige nøgle.

5. Nøgleidentifikatorer identificerer entydigt certifikatindehaver eller certificeringsmyndigheder. De kodes som følger:

   5.1. Udstyr (køretøjsenhed eller kort):

Data	Udstyrets serienummer	Dato	Type	Fabrikant
Længde	4 bytes	2 bytes	1 bytes	1 bytes
Værdi	Heltal	mm yy binær decimalkode	Fabrikatnspecifik	Fabrikantkode

For en køretøjsenhed kan producenten, når han anmoder om certifikater, være vidende eller uvidende om identifikationen af det udstyr, nøglerne vil blive indsat i.

I første tilfælde sender fabrikanten identifikationen af udstyret med den offentlige nøgle til den pågældende medlemsstats myndigheder til certificering. Certifikatet vil derefter indeholde identifikationen af udstyret, og fabrikanten skal sikre, at nøgler og certifikat indsættes i det udstyr, det er bestemt for. Nøgleidentifikatoren har den ovenfor viste form.

I sidstnævnte tilfælde skal fabrikanten entydigt identificere hver forespørgsel om certifikat og sende denne identifikation med den offentlige nøgle til den pågældende medlemsstats myndigheder til certificering. Certifikatet vil indeholde identifikationen af anmodningen. Fabrikanten skal melde tilbage til myndighederne i sin medlemsstat med tilordning af nøgle til udstyr (dvs. identifikation af anmodning om certifikat, identifikation af udstyr) efter installation af nøglen i udstyret. Nøgleidentifikatoren har følgende form:

Data	Serienummer på anmodning om certifikat	Dato	Type	Fabrikant
Længde	4 bytes	2 bytes	1 byte	1 byte
Værdi	BCD-kodning	mm yy BCD-kode	'FF'	Fabrikantkode

5.2. Certificeringsmyndighed:

Data	Identifikation af myndighed	Serienummer på nøgle	Supplerende oplysninger	Identifikator
Længde	4 bytes	1 byte	2 bytes	1 byte
Værdi	1 byte numerisk nation-kode 3 bytes alfanumerisk nation-kode	Heltal	Supplerende kode (specifik for certificeringsmyndigheden) 'FF FF' hvis det ikke anvendes	'01'

Nøglens serienummer anvendes til at skelne mellem en medlemsstats forskellige nøgler i tilfælde af, at nøglen ændres.

6. Certifikatkontrollører skal implicit vide, at den certificerede offentlige nøgle er en RSA-nøgle, som er relevant for ægthedsbekræftelse, verificering af digital underskrift og kryptering til fortrolighedstjenester (certifikatet indeholder ingen objektidentifikator til specificering heraf).

3.3.2. ***Udstedte certifikater***

CSM_018 Det udstedte certifikat er en digital underskrift med delvis genetablering af certifikatets indhold i overensstemmelse med ISO/IEC 9796-2, med »henvisning til certificeringsmyndighed« vedhæftet.

$$X.C = X.CA.SK['6A' \,||\, C_r \,||\, Hash(Cc) \,||\, 'BC'] \,||\, C_n \,||\, X.CAR$$

Med certifikatindhold $= Cc = \underset{106\ bytes}{C_r} \,||\, \underset{58\ bytes}{C_n}$

Bemærkninger:

1. Dette certifikat er 194 bytes langt.

2. Henvisning til certificeringsmyndigheden (CAR), som er skjult af underskriften, er ligeledes vedhæftet underskriften, således at certificeringsmyndighedens offentlige nøgle kan vælges til verificering af certifikatet.

3. Certifikatkontrolløren skal implicit kende den algoritme, der af certificeringsmyndigheden er anvendt til at underskrive certifikatet.

4. Den headerliste, der er knyttet til dette udstedte certifikat, er som følger:

'7F 21'	'09'	'5F 37'	'81 80'	'5F 38'	'3A'	'42'	'08'
Mærkat for CV-certifikat (konstrueret)	Længde af efterfølgende dataobjekter	Underskriftmærkat	Underskriftlængde	Restmærkat	Restlængde	Mærkat for henvisning til certificeringsmyndighed (CAR)	Længde af henvisning til certificeringsmyndighed (CAR)

3.3.3. ***Verificering og udpakning af certifikater***

Certifikatverificering og -udpakning består i verificering af underskriften i overensstemmelse med ISO/IEC 9796-2, hentning af certifikatets indhold og den deri indeholdte offentlige nøgle: X.PK = X.CA.PK$_o$X.C, samt verificering af certifikatets validitet.

CSM_019 Der indgår heri følgende trin:

Verificering af underskrift og hentning af indhold:

— fra X.C hent Sign, C_n' og CAR': X.C = Sign (128 Bytes) || C_n' (58 Bytes) || CAR' (8 Bytes)

— fra henvisning til certificeringsmyndighed (CAR), vælg korrekt offentlig nøgle for certificeringsmyndighed (hvis dette ikke er sket før på anden måde)

— åben Sign med certificeringsmyndigheden offentlige nøgle: Sr' = X.CA.PK [Sign],

— kontrollér at Sr' begynder med '6A' og ender på 'BC'

— beregn Cr' og H' af: Sr' = '6A' || C_r' (106 Bytes) || H' (20 Bytes) || 'BC'

— genetabler certifikatindhold C' = C_r' || C_n',

— kontrollér, at *Hash*(C') = H'

Giver kontrollerne tilfredsstillende resultat, er certifikatet ægte, dets indhold er C'.

Verificer gyldighed. Fra C':

— kontrollér i givet fald udløbsdatoen,

Hent og gem offentlig nøgle, nøgleidentifikator, certifikatindehavers autorisation og certifikatudløbsdato fra C':

— X.PK = *n* || *e*

— X.KID = CHR

— X.CHA = CHA

— X.EOV = EOV

4. MEKANISME TIL GENSIDIG ÆGTHEDSBEKRÆFTELSE

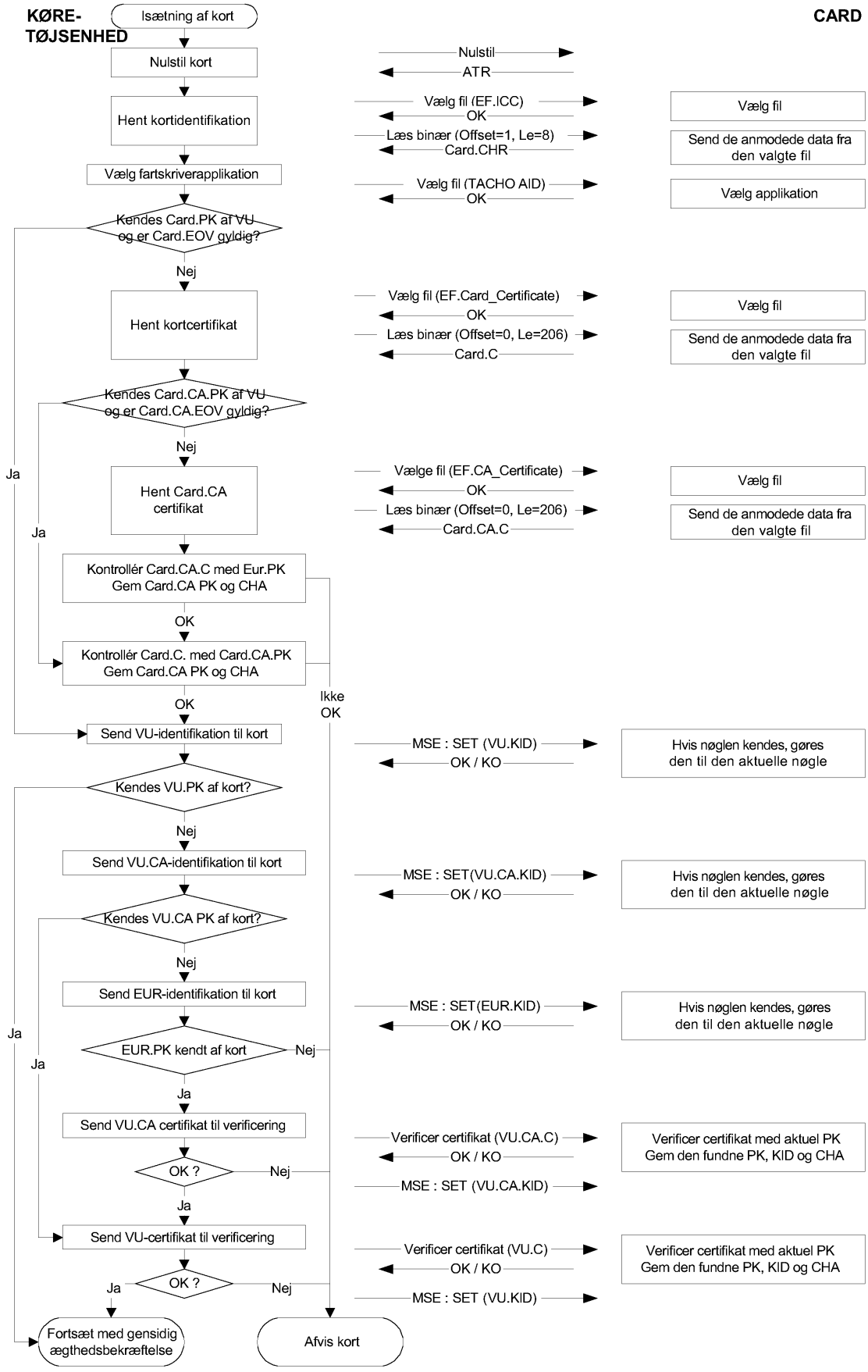
Gensidig ægthedsbekræftelse mellem kort og køretøjsenheder bygger på følgende princip:

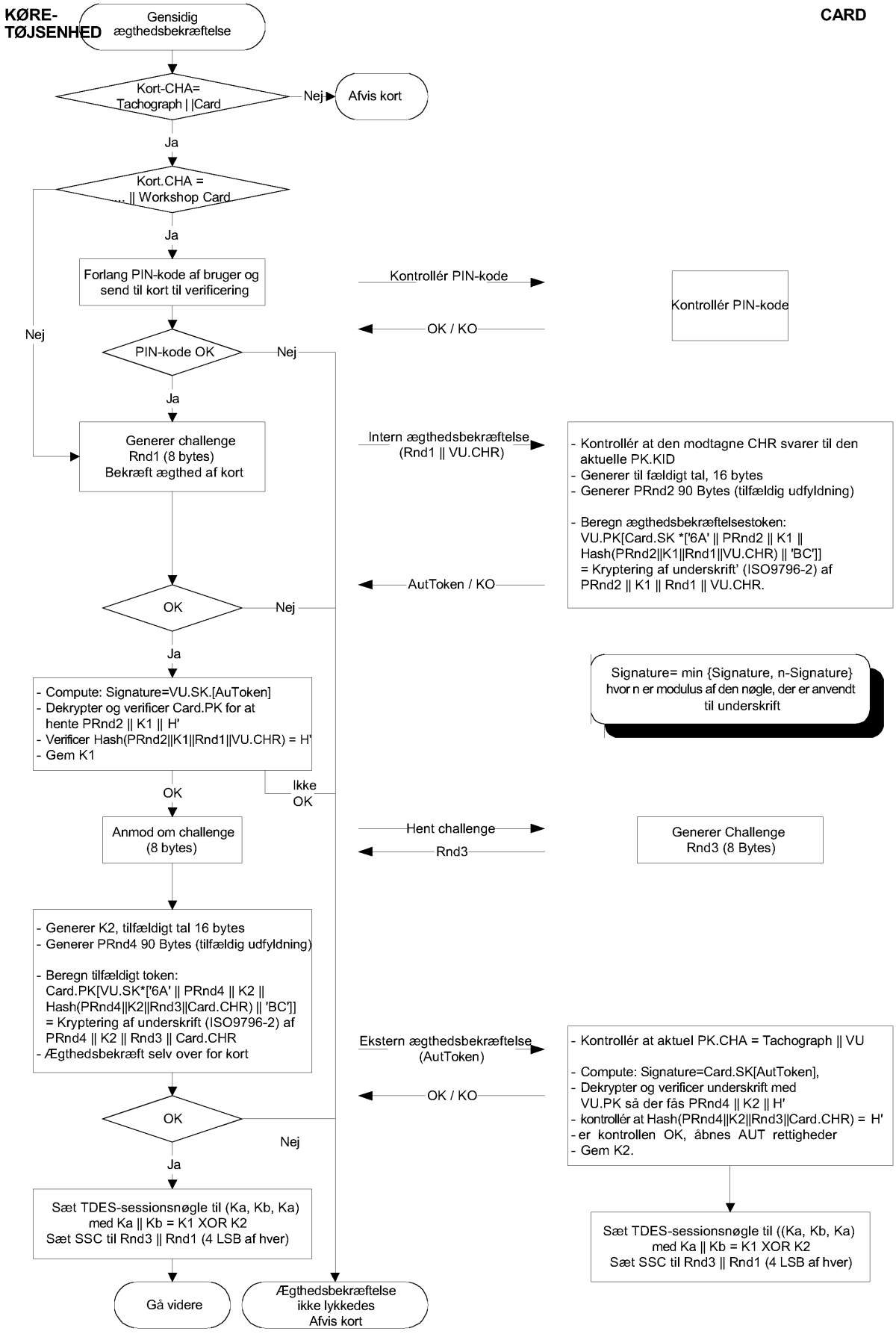
Hver part skal over for den anden godtgøre, at den er indehaver af en gyldig nøgle, af hvilken den offentlige nøgle er certificeret af en af medlemsstaternes certificeringsmyndigheder, som selv er certificeret af den europæiske certificeringsmyndighed.

Dette sker ved, at der med den private nøgle underskrives et tilfældigt tal, afsendt af den anden part, som derefter skal genfinde det afsendte tilfældige tal ved verificering af denne underskrift.

Mekanismen udløses af køretøjsenheden ved isætningen af kortet. Den begynder med udveksling af certifikater og udpakning af offentlige nøgler og slutter med indsætning af en sessionsnøgle.

CSM_020 Der skal anvendes følgende protokol (pilene angiver kommandoer og udvekslede data (se tillæg 2)):




KØRE-TØJSENHED
CARD
Gensidig ægthedsbekræftelse
Kort-CHA= Tachograph | |Card
Nej
Afvis kort
Ja
Kort.CHA = ... || Workshop Card
Ja
Forlang PIN-kode af bruger og send til kort til verificering
Kontrollér PIN-kode
OK / KO
Kontrollér PIN-kode
Nej
PIN-kode OK
Nej
Ja
Generer challenge Rnd1 (8 bytes) Bekræft ægthed af kort
Intern ægthedsbekræftelse (Rnd1 || VU.CHR)
- Kontrollér at den modtagne CHR svarer til den aktuelle PK.KID
- Generer til fældigt tal, 16 bytes
- Generer PRnd2 90 Bytes (tilfældig udfyldning)
- Beregn ægthedsbekræftelsestoken: VU.PK[Card.SK *['6A' || PRnd2 || K1 || Hash(PRnd2||K1||Rnd1||VU.CHR) || 'BC']] = Kryptering af underskrift' (ISO9796-2) af PRnd2 || K1 || Rnd1 || VU.CHR.
AutToken / KO
OK
Nej
Ja
Signature= min {Signature, n-Signature} hvor n er modulus af den nøgle, der er anvendt til underskrift
- Compute: Signature=VU.SK.[AuToken]
- Dekrypter og verificer Card.PK for at hente PRnd2 || K1 || H'
- Verificer Hash(PRnd2||K1||Rnd1||VU.CHR) = H'
- Gem K1
OK
Ikke OK
Anmod om challenge (8 bytes)
Hent challenge
Rnd3
Generer Challenge Rnd3 (8 Bytes)
- Generer K2, tilfældigt tal 16 bytes
- Generer PRnd4 90 Bytes (tilfældig udfyldning)
- Beregn tilfældigt token: Card.PK[VU.SK*['6A' || PRnd4 || K2 || Hash(PRnd4||K2||Rnd3||Card.CHR) || 'BC']] = Kryptering af underskrift (ISO9796-2) af PRnd4 || K2 || Rnd3 || Card.CHR
- Ægthedsbekræft selv over for kort
Ekstern ægthedsbekræftelse (AutToken)
- Kontrollér at aktuel PK.CHA = Tachograph || VU
- Compute: Signature=Card.SK[AutToken],
- Dekrypter og verificer underskrift med VU.PK så der fås PRnd4 || K2 || H'
- kontrollér at Hash(PRnd4||K2||Rnd3||Card.CHR) = H'
- er kontrollen OK, åbnes AUT rettigheder
- Gem K2.
OK / KO
OK
Nej
Ja
Sæt TDES-sessionsnøgle til (Ka, Kb, Ka) med Ka || Kb = K1 XOR K2
Sæt SSC til Rnd3 || Rnd1 (4 LSB af hver)
Sæt TDES-sessionsnøgle til ((Ka, Kb, Ka) med Ka || Kb = K1 XOR K2
Sæt SSC til Rnd3 || Rnd1 (4 LSB af hver)
Gå videre
Ægthedsbekræftelse ikke lykkedes Afvis kort

5. MEKANISMER TIL FORTROLIGHED, INTEGRITET OG ÆGTHEDSKONTROL VED DATAOVERFØRSEL PÅ KØRETØJENHEDENS KORT

5.1. **Sikker meddelelsesoverførsel**

CSM_021 Ved overførsler af data på kort i køretøjsenheder skal dataintegriteten beskyttes gennem sikker meddelelsesoverførsel i overensstemmelse med henvisning ISO/IEC 7816-4 og ISO/IEC 7816-8.

CSM_022 Når der er behov for beskyttelse af data under overførsel, skal et dataobjekt med kryptografisk kontrolsum vedhæftes de dataobjekter, der udsendes inden for kommandoen eller svaret. Den kryptografiske kontrolsum skal verificeres af modtageren.

CSM_023 Den kryptografiske kontrolsum af data sendt inden for en kommando skal indeholde kommandoens header og alle de afsendte dataobjekter (= > CLA = '0C', og alle dataobjekter skal være indkapslet med mærkater, i hvilke b1 = 1).

CSM_024 Informationsbytes for svarstatus skal være beskyttet af en kryptografisk kontrolsum, når svaret ikke indeholder noget datafelt.

CSM_025 Kryptografiske kontrolsummer skal være 4 bytes lange.

Kommandoer og svar har derfor følgende struktur ved brug af sikker meddelelsesoverførsel:

De anvendte dataobjekter er et delsæt af de dataobjekter for sikker meddelelsesoverførsel, som er beskrevet i ISO/IEC 7816-4:

Mærkat	Huskeværdi	Betydning
'81'	T_{PV}	Ordinær værdi af ikke BER-TLV kodede data (skal beskyttes med kryptografisk kontrolsum)
'97'	T_{LE}	Værdien af Le i den ikke sikrede kommando (skal beskyttes med kryptografisk kontrolsum)
'99'	T_{SW}	Status (skal beskyttes med kryptografisk kontrolsum)
'8E'	T_{CC}	Kryptografisk kontrolsum
'87'	$T_{PI\ CG}$	Indikatorbyte for udfyldning || Kryptogram (ordinær værdi ikke kodet i BER-TLV)

Givet et ikke sikret kommando/svar par:

Kommandoheader	Kommandoindhold
CLA INS P1 P2	[$L_c$field] [Data field] [L_e field]
fire bytes	L bytes, benævnt B_1 til B_L

Svarindhold	Svarefterskrift
[Datafelt]	SW1 SW2
L_r databytes	to bytes

Det tilsvarende sikrede kommando/svar par er:

Sikret kommando:

Kommandoheader (CH)	Kommandoindhold										
CLA INS P1 P2	[NytL_c felt]	[Nytfelt]									[NytL_e felt]
'OC'	Længde af nyt datafelt	T_{PV}	L_{PV}	PV	T_{LE}	L_{LE}	L_e	T_{CC}	L_{CC}	CC	'00'
		'81'	L_c	Data field	'97'	'01'	L_e	'8E'	'04'	CC	

Data som skal indgå i kontrolsum = CH || PB || T_{PV} || L_{PV} || PV || T_{LE} || L_{LE} || L_e || PB

PB = Udfyldningsbytes (80 .. 00) i overensstemmelse med ISO-IEC 7816-4 og ISO 9797 metode 1.

Dataobjekterne PV og LE er kun tilstede, når der er nogle tilsvarende data i den ikke sikrede kommando.

Sikret svar:

1. Tilfælde hvor svar-datafeltet ikke er tomt og ikke behøver være fortrolighedsbeskyttet:

Svarindhold						Svarefterskrift
[Nyt datafelt]						Ny SW1 SW2
T_{PV}	L_{PV}	PV	T_{CC}	L_{CC}	CC	
'81'	L_r	Datafelt	'8E'	'04'	CC	

Data som skal indgå i kontrolsum = T_{PV} || L_{PV} || PV || PB

2. Tilfælde hvor svar-datafeltet ikke er tomt og behøver være fortrolighedsbeskyttet:

Svarindhold						Svarefterskrift
[Nyt datafelt]						Ny SW1 SW2
$T_{PI\ CG}$	$L_{PI\ CG}$	PI CG	T_{CC}	L_{CC}	CC	
'87'		PI || CG	'8E'	'04'	CC	

Data som skal bæres af CG: ikke BER-TLV kodede data og udfyldningsbytes.

Data som skal indgå i kontrolsum = $T_{PI\ CG}$ || $L_{PI\ CG}$ || PI CG || PB

3. Tilfælde hvor svardatafeltet er tomt:

Svarindhold						Svarefterskrift
[Nyt datafelt]						Nyt SW1 SW2
T_{SW}	L_{SW}	SW	T_{CC}	L_{CC}	CC	
'99'	'02'	Ny SW1 SW2	'8E'	'04'	CC	

Data som skal indgå i kontrolsum = T_{SW} || L_{SW} || SW || PB

5.2. **Håndtering af fejl ved sikker meddelelsesoverførsel**

CSM_026 Når fartskriverkortet konstaterer en fejl i sikker meddelelsesoverførsel under fortolkning af en kommando, skal statusbytes returneres uden sikker meddelelsesoverførsel. I henhold til ISO/IEC 7816-4 er defineret følgende statusbytes til angivelse af fejl i sikker meddelelsesoverførsel:

'66 88': Verificering af kryptografisk kontrolsum ikke lykkedes,

'69 87': Forventede dataobjekter i sikker meddelelsesoverførsel mangler,

'69 88': Dataobjekter i sikker meddelelelsesoverførsel fejlbehæftede.

CSM_027 Når fartskriverkortet returnerer statusbytes uden dataobjekter for sikker meddelelsesoverførsel (SM) eller med et fejlbehæftet SM-dataobjekt, skal sessionen afbrydes af køretøjsenheden.

5.3. **Algoritme til beregning af kryptografiske kontrolsummer**

CSM_028 Kryptografiske kontrolsummer er opbygget med anvendelse af en sædvanlig MAC i overensstemmelse med ANSI X9.19 med DES:

— indledende trin: Den indledende kontrolblok y0 er E(Ka, SSC),

— sekventielt trin: Kontrolblokkene y1, . . ., yn beregnes ved hjælp af Ka,

— sluttrin: Den kryptografiske kontrolsum beregnes ved hjælp af den sidste kontrolblok yn på følgende måde: E(Ka, D(Kb, yn)).

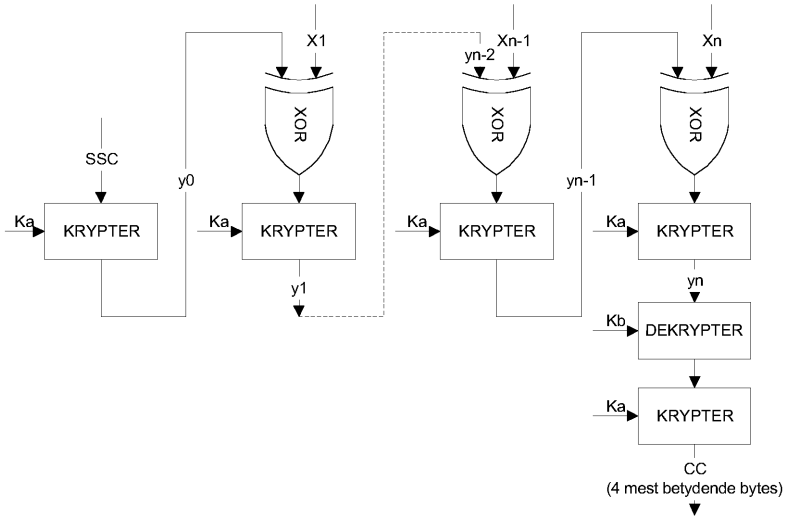
hvor E() betyder kryptering med DES, og D() betyder dekryptering med DES.

De fire mest betydende bytes i den kryptografiske kontrolsum overføres

CSM_029 Sendesekvenstælleren (SSC) skal, mens nøgler aftales, initialiseres med: Startværdi af SSC: Rnd3 (4 mindst betydende bytes) || Rnd1 (4 mindst betydende bytes).

CSM_030 Sendesekvenstælleren skal hver gang øges med 1 inden beregning af en MAC (dvs. SSC for den første kommando er startværdien af SSC + 1, SSC for det første svar er startværdien af SSC + 2).

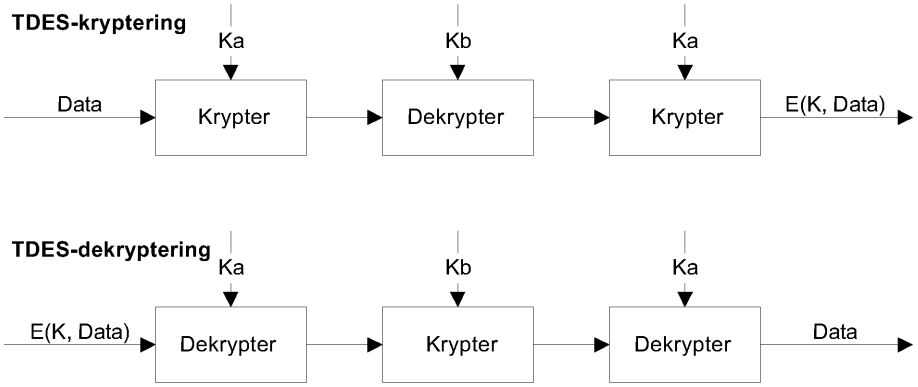
Følgende figur viser beregningen af MAC:



5.4. **Algoritme til beregning af kryptogrammer til fortrolighedsdataobjekter**

CSM_031 Kryptogrammer beregnes ved hjælp af TDEA i TCBC-funktionsmåde i overensstemmelse med henvisning TDES og TDES-OP og med nulvektoren som startværdiblok.

Følgende figur viser anvendelsen af nøgler i TDES:



6. MEKANISMER TIL DIGITAL UNDERSKRIFT AF DATAOVERFØRSLER

CSM_032 Det intelligente dedikerede udstyr (IDE) lagrer data, som er modtaget fra én enhed (køretøjsenhed eller kort) under én overførselssession, inden for én fysisk datafil. Denne fil skal indeholde certifikaterne MS_i.C og EQT.C. Filen indeholder digitale underskrifter af datablokke som foreskrevet i tillæg 7 (Protokoller for dataoverførsel).

CSM_033 I digitale underskrifter af overførte data skal anvendes et digitalt underskriftssystem med appendiks, således at overførte data om ønsket kan læses uden dechifrering.

6.1. **Generering af underskrifter**

CSM_034 Ved generering af dataunderskrift skal udstyret følge underskriftssystemet med appendiks som fastlagt i henvisning PKCS1 med SHA-1 hash-funktionen:

$$\text{Underskrift} = \text{EQT.SK}['00' \,||\, '01' \,||\, PS \,||\, '00' \,||\, \text{DER}(\text{SHA-1}(\text{Data}))]$$

PS = Udfyldningsstreng af oktetter, der har værdien 'FF', så at længden er 128.

DER(SHA-1(M)) er kodningen af hash-funktionen algoritme-ID og hash-værdien til en ASN.1-værdi af typen `DigestInfo` (distinguished encoding rules):

'30'||'21'||'30'||'09'||'06'||'05'||'2B'||'0E'||'03'||'02'||'1A'||'05'||'00'||'04'||'14'||Hash-værdi.

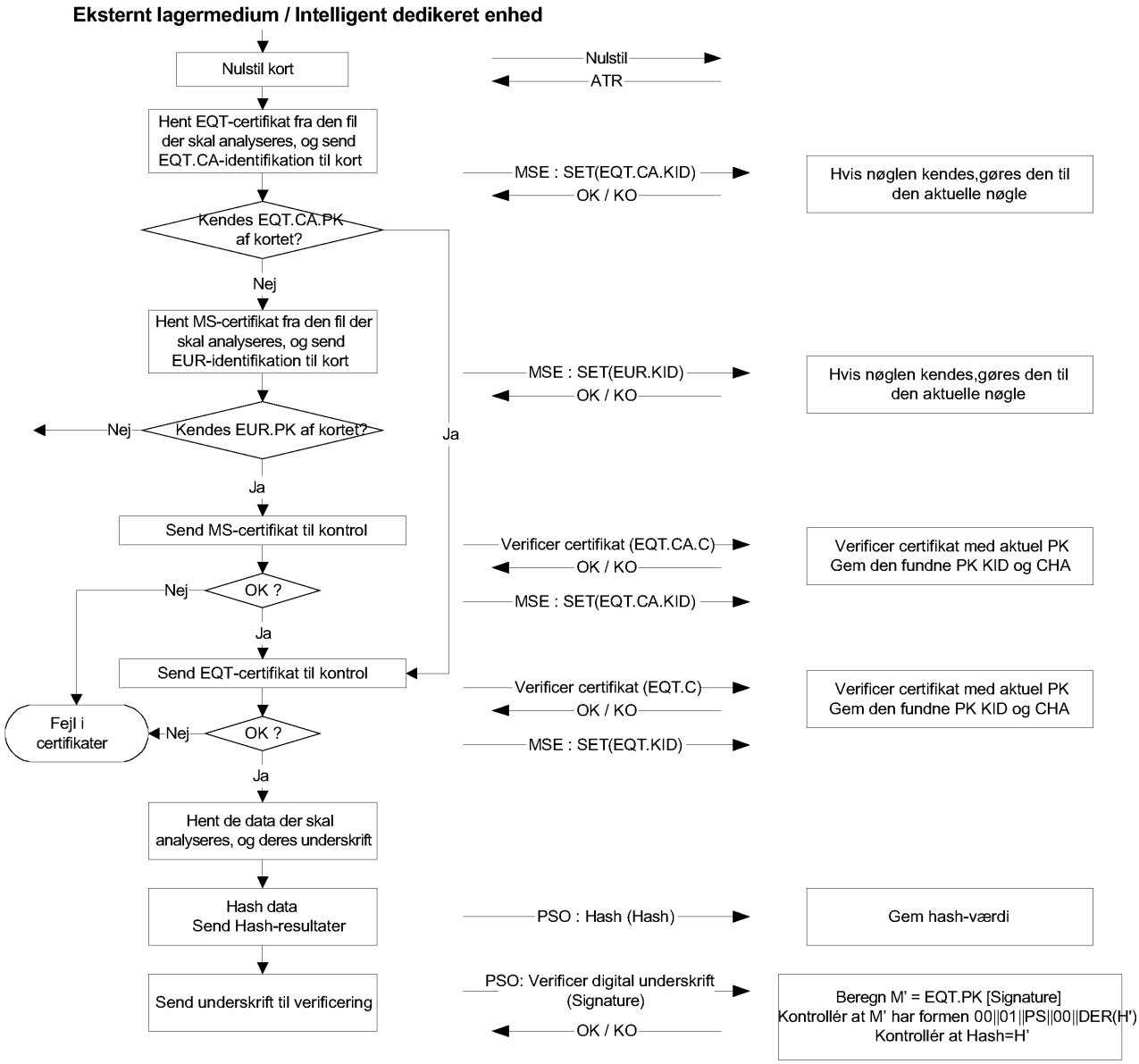
6.2. **Verificering af underskrift**

CSM_035 Ved verificering af dataunderskrift på overførte data skal udstyret følge underskriftssystemet med appendiks som defineret i henvisning PKCS1 med SHA-1 hash-funktionen.

Den europæiske offentlige nøgle EUR.PK må uafhængigt (og betroet) kendes af kontrolløren.

Følgende tabel illustrerer den protokol, som en intelligent dedikeret enhed (IDE) med kontrolkort kan følge ved verificering af integriteten af data, som er overført og lagret på eksterne lagermedier. Kontrolkortet anvendes til at udføre dechifreringen af digitale underskrifter. Denne funktion behøver i dette tilfælde ikke være implementeret i det pågældende IDE.

Det udstyr, som har overført og underskrevet de data, der skal analyseres, benævnes EQT (equipment).


Eksternt lagermedium / Intelligent dedikeret enhed
Nulstil kort
Nulstil
ATR
Hent EQT-certifikat fra den fil der skal analyseres, og send EQT.CA-identifikation til kort
MSE : SET(EQT.CA.KID)
OK / KO
Hvis nøglen kendes,gøres den til den aktuelle nøgle
Kendes EQT.CA.PK af kortet?
Nej
Ja
Hent MS-certifikat fra den fil der skal analyseres, og send EUR-identifikation til kort
MSE : SET(EUR.KID)
OK / KO
Hvis nøglen kendes,gøres den til den aktuelle nøgle
Nej
Kendes EUR.PK af kortet?
Ja
Send MS-certifikat til kontrol
Verificer certifikat (EQT.CA.C)
OK / KO
Verificer certifikat med aktuel PK
Gem den fundne PK KID og CHA
Nej
OK ?
MSE : SET(EQT.CA.KID)
Ja
Send EQT-certifikat til kontrol
Verificer certifikat (EQT.C)
OK / KO
Verificer certifikat med aktuel PK
Gem den fundne PK KID og CHA
Fejl i certifikater
Nej
OK ?
MSE : SET(EQT.KID)
Ja
Hent de data der skal analyseres, og deres underskrift
Hash data
Send Hash-resultater
PSO : Hash (Hash)
Gem hash-værdi
Send underskrift til verificering
PSO: Verificer digital underskrift (Signature)
OK / KO
Beregn M' = EQT.PK [Signature]
Kontrollér at M' har formen 00||01||PS||00||DER(H')
Kontrollér at Hash=H'

«