

I

(Säädökset, jotka on julkaistava)

KOMISSION ASETUS (EY) N:o 1360/2002,

annettu 13 päivänä kesäkuuta 2002,

**tieliikenteen valvontalaitteista annetun neuvoston asetuksen (ETY) N:o 3821/85 mukauttamisesta
tekniikan kehitykseen seitsemännen kerran**

(ETA:n kannalta merkityksellinen teksti)

EUROOPAN YHTEISÖJEN KOMISSIO, joka

ottaa huomioon Euroopan yhteisön perustamissopimuksen,

ottaa huomioon tieliikenteen valvontalaitteista 20 päivänä joulukuuta 1985 annetun neuvoston asetuksen (ETY) N:o 3821/85 ⁽¹⁾, sellaisena kuin se on viimeksi muutettuna asetuksella (EY) N:o 2135/98 ⁽²⁾, ja erityisesti sen 17 ja 18 artiklan,

sekä katsoo seuraavaa:

- (1) Asetuksen (ETY) N:o 3821/85 liitteessä I B olevat tekniset eritelvät olisi mukautettava tekniseen kehitykseen kiinnittäen erityistä huomiota järjestelmän kokonaisturvallisuuteen sekä valvontalaitteiston ja kuljettajakorttien yhteentoimivuuteen.
- (2) Laitteiston mukauttaminen edellyttää, että mukautetaan myös asetuksen (ETY) N:o 3821/85 liite II, jossa määritellään merkit ja hyväksyntätodistukset.
- (3) Asetuksen (ETY) N:o 3821/85 18 artiklalla perustettu komitea ei antanut lausuntoa ehdotuksesta, joten komissio antoi kyseisistä toimenpiteistä ehdotuksen neuvostolle.
- (4) Neuvosto ei tehnyt päätöstä ehdotuksessa esitetyistä toimenpiteistä asetuksen (ETY) N:o 3821/85 18 artiklan 5 kohdan b alakohdassa säädetyin ajan kuluessa, joten toimenpiteistä päättäminen kuuluu komissiolle,

ON ANTANUT TÄMÄN ASETUKSEN:

1 artikla

Korvataan asetuksen (EY) N:o 2135/98 liite tämän asetuksen liitteellä.

2 artikla

Muutetaan asetuksen (ETY) N:o 3821/85 liite II seuraavasti:

1. Muutetaan I luvun 1 kohdan ensimmäinen alakohta seuraavasti:
 - Korvataan Kreikan tunnus "GR" tunnuksella "23";
 - Korvataan Irlannin tunnus "IRL" tunnuksella "24";
 - Lisätään Itävallan tunnus "12";
 - Lisätään Suomen tunnus "17";
 - Lisätään Ruotsin tunnus "5".
2. Muutetaan I luvun 1 kohdan toinen alakohta seuraavasti:
 - Lisätään ilmaisun "piirturilevyn" jälkeen ilmaisu "tai ajopiirturikortin".
3. Muutetaan I luvun 2 kohta seuraavasti:
 - Lisätään ilmaisun "piirturilevyssä" jälkeen ilmaisu "ja jokaisessa ajopiirturikortissa".
4. Lisätään II luvun otsikkoon ilmaisu "LIITTEEN I MUKAISILLE TUOTTEILLE".

⁽¹⁾ EYVL L 370, 31.12.1985, s. 8.

⁽²⁾ EYVL L 274, 9.10.1998, s. 1.

5. Lisätään III luku seuraavasti:

”III. TYYPPIHVÄKSYNTÄTODISTUS LIITTEEN I B MUKAISILLE TUOTTEILLE

Tyyppihyväksynnän antaneen jäsenvaltion on annettava hakijalle jäljempänä esitetyn mallin mukainen tyyppihyväksyntätodistus. Ilmoittaessaan muille jäsenvaltioille annetuista tyyppihyväksynnöistä tai tarvittaessa niiden peruuttamisista jäsenvaltion on käytettävä tämän todistuksen jäljennöksiä.

 TYYPPIHVÄKSYNTÄTODISTUS LIITTEEN I B MUKAISILLE TUOTTEILLE

Toimivaltaisen viranomaisen nimi

Ilmoitus (*):

- tyyppihyväksynnästä, joka koskee
- tyyppihyväksynnän peruuttamisesta, joka koskee
- valvontalaitemallia
- valvontalaitteen osaa (**)
- kuljettajakorttia
- korjaamokorttia
- yrityskorttia
- valvontakorttia

Tyyppihyväksyntänumero

1. Tuotenimi tai tavaramerkki
2. Mallinimi
3. Valmistajan nimi
4. Valmistajan osoite
5. Päivä, jona tyyppihyväksyntähakemus on esitetty
6. Tutkimuslaitos (-laitokset)
7. Testin (testien) päivämäärä ja numero
8. Hyväksymispäivä.....
9. Tyyppihyväksynnän peruuttamispäivä
10. Ne valvontalaitteen osien mallit, joiden kanssa käytettäväksi kyseinen osa on tarkoitettu
11. Paikka
12. Päiväys
13. Liitteenä olevat selventävät asiakirjat

14. Huomautuksia (myös tiedot mahdollisten sinettien sijainnista)

.....
(allekirjoitus)

(*) Rastittakaa oikeat vaihtoehdot.

(**) Yksilöikää ilmoituksen kohteena oleva osa.”

3 artikla

Tämä asetus tulee voimaan kahdentenakymmenentenä päivänä sen jälkeen, kun se on julkaistu *Euroopan yhteisöjen virallisessa lehdessä*.

Tämä asetus on kaikilta osiltaan velvoittava, ja sitä sovelletaan sellaisenaan kaikissa jäsenvaltioissa.

Tehty Brysselissä 13 päivänä kesäkuuta 2002.

Komission puolesta

Loyola DE PALACIO

Varapuheenjohtaja

LIITE

"LIITE I B

RAKENNETTA, TESTAUSTA, ASENNUSTA JA TARKASTUSTA KOSKEVAT VAATIMUKSET

Tässä liitteessä määritellyissä laitteissa käytettävien ohjelmistojen yhteentoimivuuden säilyttämiseksi tietyt tietokoneohjelmoinnin kirjainsanat, termit tai ilmaisut on jätetty tekstin alkukielelle eli englanniksi. Joidenkin näiden ilmaisujen perään on kuitenkin liitetty sulkeisiin tiedoksi sanatarkkoja käännoiksi ilmaisujen ymmärtämisen helpottamiseksi.

MÄÄRITELMÄT

I	MÄÄRITELMÄT	8
II	VALVONTALAITTEEN YLEISET OMINAISUUDET JA TOIMINNOT	12
	1. Yleiset ominaisuudet	12
	2. Toiminnot	12
	3. Toimintatilat	13
	4. Tietoturva	14
III	VALVONTALAITTEIDEN RAKENNETTA JA TOIMINTOJA KOSKEVAT VAATIMUKSET	14
	1. Korttien paikoilleen asetuksen ja poistamisen valvonta	14
	2. Nopeuden ja matkan mittaus	14
	2.1 Kuljetun matkan mittaus	15
	2.2 Nopeuden mittaus	15
	3. Ajanmittaus	15
	4. Kuljettajan toiminnan valvonta	16
	5. Ajoneuvon miehityksen valvonta	16
	6. Kuljettajan käsin syöttämät tiedot	16
	6.1 Tiedot paikasta, jossa päivän työaika alkaa ja/tai päättyy	16
	6.2 Kuljettajan toimintaan liittyvien tietojen syöttö käsin	16
	6.3 Erityisolosuhteisiin liittyvien tietojen syöttö	18
	7. Yritysten tekemien lukitusten hallinta	18
	8. Tarkastustoimien hallinta	18
	9. Tapauksien ja/tai vikojen havaitseminen	18
	9.1 'Kortti ei voimassa' -tapaus	18
	9.2 'Korttiristiriita'-tapaus	19
	9.3 'Aikojen päällekkäisyys' -tapaus	19
	9.4 'Ajo ilman asianmukaista korttia' -tapaus	19
	9.5 'Kortin paikoilleen asettaminen ajettaessa'-tapaus	19
	9.6 'Edellistä kortin käyttöjaksoa ei lopetettu oikein' -tapaus	19
	9.7 'Ylinopeus'-tapaus	19

9.8	'Keskeytynyt virransyöttö' -tapaus	20
9.9	'Virhe liikedatassa' -tapaus	20
9.10	'Tietoturvan murtoyritys' -tapaus	20
9.11	'Kortti'-vikatapahtuma	20
9.12	'Valvontalaite'-vikatapahtuma	20
10.	Sisäänrakennetut ja laitteen itse suorittamat testit	20
11.	Tietojen haku datamuistista	21
12.	Tietojen kirjaaminen ja tallentaminen datamuistiin	21
12.1	Laitteen tunnistetiedot	21
12.1.1	Ajoneuvoyksikön tunnistetiedot	21
12.1.2	Liiketunnistimen tunnistetiedot	22
12.2	Tietoturvan osatekijät	22
12.3	Kuljettajakortin paikoilleen asetukseen ja poistamiseen liittyvät tiedot	22
12.4	Kuljettajan toimintaan liittyvät tiedot	23
12.5	Tiedot paikasta, jossa päivän työaika alkaa ja/tai päättyy	23
12.6	Matkamittarin tiedot	23
12.7	Yksityiskohtaiset nopeustiedot	23
12.8	Tapauksia koskevat tiedot	23
12.9	Vikoihin liittyvät tiedot	25
12.10	Kalibrointiin liittyvät tiedot	26
12.11	Ajan asetukseen liittyvät tiedot	26
12.12	Tarkastustoimiin liittyvät tiedot	26
12.13	Yritysten tekemiin lukituksiin liittyvät tiedot	27
12.14	Tietojen kopiointiin liittyvät tiedot	27
12.15	Erytisolosuhteisiin liittyvät tiedot	27
13.	Tietojen haku ajopiirturikorteilta	27
14.	Tietojen kirjaaminen ja tallentaminen ajopiirturikorteille	27
15.	Tietojen näyttö	28
15.1	Oletusarvoinen näyttö	28
15.2	Varoitusten näyttö	29
15.3	Valikkojen käyttö	29
15.4	Muut näytöt	29
16.	Tulostaminen	29
17.	Varoitukset	30
18.	Tietojen kopioiminen ulkoisille tietovälineille	31
19.	Tietojen tulostaminen muille ulkoisille välineille	31
20.	Kalibrointi	32
21.	Ajan asetukset	32

22.	Laitteen toimintaominaisuudet	32
23.	Materiaalit	32
24.	Merkinnät	33
IV.	AJOPIIRTURIKORTTIEN RAKENNETTA JA TOIMINTOJA KOSKEVAT VAATIMUKSET	33
1.	Näkyvässä olevat tiedot	33
2.	Tietoturva	36
3.	Standardit	36
4.	Ympäristöön liittyvät ja sähkötekniset eritelvät	36
5.	Tietojen tallennus	36
5.1	Kortin tunniste- ja turvatiedot	37
5.1.1	Sovellusten tunnistetiedot	37
5.1.2	Mikrosirujen tunnistetiedot	37
5.1.3	Sirukorttien tunnistetiedot	37
5.1.4	Tietoturvan osatekijät	37
5.2	Kuljettajakortti	37
5.2.1	Kortin tunnistetiedot	37
5.2.2	Kortin haltijan tunnistetiedot	38
5.2.3	Ajokorttiin liittyvät tiedot	38
5.2.4	Käytössä olleisiin ajoneuvoihin liittyvät tiedot	38
5.2.5	Kuljettajan toimintaan liittyvät tiedot	38
5.2.6	Tiedot paikasta, jossa päivän työaika alkaa ja/tai päättyy	39
5.2.7	Tapauksiin liittyvät tiedot	39
5.2.8	Vikoihin liittyvät tiedot	40
5.2	Tarkastustoimiin liittyvät tiedot	40
5.2.10	Kortin käyttöjaksoon liittyvät tiedot	40
5.2.11	Erytisolosuhteisiin liittyvät tiedot	40
5.3	Korjaamokortti	41
5.3.1	Tietoturvan osatekijät	41
5.3	Kortin tunnistetiedot	41
5.3.3	Kortin haltijan tunnistetiedot	41
5.3.4	Käytössä olleisiin ajoneuvoihin liittyvät tiedot	41
5.3.5	Kuljettajan toimintaan liittyvät tiedot	41
5.3.6	Päivän työajan alkamiseen ja/tai päättymiseen liittyvät tiedot	41
5.3.7	Tapauksiin ja vikoihin liittyvät tiedot	41
5.3.8	Tarkastustoimiin liittyvät tiedot	41
5.3.9	Kalibrointiin ja ajan asetukseen liittyvät tiedot	42
5.3.10	Erytisolosuhteisiin liittyvät tiedot	42
5.4	Valvontakortti	42

5.4.1	Kortin tunnistetiedot	42
5.4.2	Kortin haltijan tunnistetiedot	42
5.4.3	Tarkastustoimiin liittyvät tiedot	42
5.5	Yrityskortti	43
5.5.1	Kortin tunnistetiedot	43
5.5.2	Kortin haltijan tunnistetiedot	43
5.5.3	Yrityksen toimenpiteitä koskevat tiedot	43
V	VALVONTALAITTEEN ASENNUS	43
1.	Asennus	43
2.	Asennuskilpi	44
3.	Sinetöinti	44
VI	TARKASTUKSET, MÄÄRÄAIKAISTARKASTUKSET JA KORJAUKSET	45
1.	Asentajien tai testausasemien hyväksyminen	45
2.	Uusien tai korjattujen laitteiden tarkastaminen	45
3.	Asennuksen tarkastus	45
4.	Määräaikaistarkastukset	45
5.	Virheiden mittaaminen	46
6.	Korjaukset	46
VII	KORTTIEN MYÖNTÄMINEN	46
VIII	VALVONTALAITTEIDEN JA AJOPIIRTURIKORTTIEN TYYPIHYVÄKSYNTÄ	46
1.	Yleisiä asioita	46
2.	Tietoturvatodistus	47
3.	Toiminnallisuustodistus	47
4.	Yhteentoimivuustodistus	47
5.	Tyyppihyväksyntätodistus	48
6.	Poikkeusmenettely: ensimmäiset yhteentoimivuustodistukset	48
Lisäys 1	Datatermistö	
Lisäys 2	Ajopiirturiikorttien erittely	
Lisäys 3	Kuvakkeet	
Lisäys 4	Tulosteet	
Lisäys 5	Näyttö	
Lisäys 6	Ulkoiset liittämälaitteet	
Lisäys 7	Tietojen kopiointiprotokollat	
Lisäys 8	Kalibrointiprotokolla	
Lisäys 9	Tyyppihyväksyntä – luettelo vähimmäistä vaadittavista testeistä	
Lisäys 10	Yleiset tietoturvatavoitteet	
Lisäys 11	Yhteiset turvamekanismit	

I MÄÄRITELMÄT

Tässä liitteessä käytetään seuraavia määritelmiä:

a) **Aktivointi:**

Vaihe, jonka aikana valvontalaite saavuttaa täyden toimintatilan, ja sen kaikki toiminnot, mukaan lukien turvatoiminnot, ovat käytössä.

Valvontalaitteen aktivointiin tarvitaan korjaamokortti ja sen tunnusluku.

b) **Todentaminen:**

Toimi, jonka tarkoitus on selvittää ja varmentaa väitetty henkilöllisyys.

c) **Autenttisuus:**

Tiedon ominaisuus, jonka toteutuessa tieto on peräisin lähteestä, jonka henkilöllisyys voidaan varmentaa.

d) **Sisäänrakennettu testi:**

Testi, joka suoritetaan tarvittaessa, käyttäjän tai ulkoisten laitteiden käynnistämänä.

e) **Kalenterivuorokausi:**

Vuorokausi, joka alkaa klo 00.00 ja päättyy klo 24.00. Kaikki kalenterivuorokaudet lasketaan UTC-ajan (Greenwichin yleisajan) mukaan.

f) **Kalibrointi:**

Datamuistiin tallennettujen ajoneuvon parametrien päivittäminen tai vahvistaminen. Ajoneuvon parametreja ovat ajoneuvon tunnistetiedot (tunnistenumero, rekisteritunnus ja jäsenvaltio, jossa ajoneuvo on rekisteröity) sekä ajoneuvon ominaisuuksia koskevat tiedot (w-, k- ja l-kertoimien ja -vakioiden arvot, rengaskoko, nopeudenrajoittimen asetukset (jos sellainen on), oikea UTC-aika, matkamittarin lukema).

Valvontalaitteen kalibrointiin tarvitaan korjaamokortti.

g) **Kortin numero:**

16 aakkosnumeerista merkkiä sisältävä tunnus, joka yksilöi jäsenvaltiossa käytettävän ajopiirturikortin. Kortin numero sisältää haltijakohtaisen sarjanumeron (jos sellainen on käytössä), korvausnumeron sekä uusintanumeron.

Näin ollen kortin myöntäneen jäsenvaltion tunnus ja kortin numero yksilöivät kortin täydellisesti.

h) **Kortin haltijakohtainen sarjanumero:**

Kortin numeron neljästoista aakkosnumeerinen merkki, jolla erotetaan toisistaan eri yrityksen tai yhteisön eri kortit. Yritykselle tai yhteisölle voidaan myöntää useampia ajopiirturikortteja. Korttitunnuksen 13 ensimmäistä merkkiä yksilöivät täysin kyseisen yrityksen tai yhteisön.

i) **Kortin uusintanumero:**

Kortin numeron kuudestoista aakkosnumeerinen merkki, jonka arvoa suurennetaan aina, kun ajopiirturikortti uusitaan.

j) **Kortin korvausnumero:**

Kortin numeron viidestoista aakkosnumeerinen merkki, jonka arvoa suurennetaan aina, kun ajopiirturikortti korvataan kaksoiskappaleella.

k) **Ajoneuvon ominaiskerroin:**

Numeerinen tunnusluku, jolla ilmaistaan sen lähtösignaalin arvo, jonka ajoneuvon se osa lähettää, joka yhdistää ajoneuvon valvontalaitteeseen (vaihteiston ulostuloakseli) silloin, kun ajoneuvo kulkee yhden kilometrin matkan normaaleissa testausolosuhteissa (ks. VI luvun 5 jakso). Ominaiskerroin ilmaistaan impulsseina kilometriä kohden (w = ... imp/km).

l) **Yrityskortti:**

Ajopiirturikortti, jonka jäsenvaltion viranomaiset myöntävät valvontalaittein varustettujen ajoneuvojen omistajalle tai haltijalle.

Yrityskortti yksilöi yrityksen ja sen avulla voidaan näyttää, kopioida ja tulostaa tiedot, jotka on tallennettu tämän yrityksen lukitsemaan valvontalaitteeseen.

m) **Valvontalaitteen vakio:**

Numeerinen tunnusluku, jolla ilmaistaan sen tulosignaalin arvo, joka tarvitaan yhden kuljetun kilometrin matkan näyttämiseksi ja tallentamiseksi. Tämä vakio on ilmaista impulssina kilometriä kohden ($k = \dots \text{imp/km}$).

n) **Keskeytymätön ajoaika valvontalaitteen laskemana ⁽¹⁾:**

Tietyn kuljettajan kokonaisajoaika hänen viimeisen vähintään 45 minuuttia kestäneen AVAILABILITY (varallaolo)- tai BREAK/REST (tauko/lepo)- tai UNKNOWN (tuntematon) ⁽²⁾ -jaksonsa jälkeen (tämä jakso saattaa olla useina, vähintään 15 minuutin pituisina osina). Kyseisissä laskelmissa otetaan tarpeen mukaan huomioon kuljettajakortille tallennetut aiemmat tapahtumat. Jos kuljettaja ei ole asettanut korttiaan laitteeseen, laskelmat perustuvat niihin datamuistin tietoihin, jotka liittyvät kuluvaan jaksoon, jolloin korttia ei ollut asetettuna laitteen asianmukaiseen aukkoon.

o) **Valvontakortti:**

Ajopiirturikortti, jonka jäsenvaltion viranomaiset myöntävät kansalliselle, toimivaltaiselle tarkastusviranomaiselle.

Valvontakortti yksilöi tarkastuselimen sekä mahdollisesti tarkastavan virkailijan, ja sen avulla voidaan datamuistiin tai kuljettajakortteihin tallennetut tiedot lukea, tulostaa ja/tai kopioida.

p) **Yhteenlaskettu taukoajaksi valvontalaitteen laskemana ⁽¹⁾:**

Tietyn kuljettajan yhteenlaskettu taukoajaksi, joka lasketaan vähintään 15 minuuttia kestävästä AVAILABILITY- tai BREAK/REST- tai UNKNOWN ⁽²⁾ -jaksoista, jotka on vietetty hänen viimeisimmän vähintään 45 minuuttia kestäneen AVAILABILITY- tai BREAK/REST- tai UNKNOWN ⁽²⁾ -jaksonsa jälkeen (tämä jakso saattaa olla useina, vähintään 15 minuutin pituisina osina).

Kyseisissä laskelmissa otetaan tarpeen mukaan huomioon kuljettajakortille tallennetut aiemmat tapahtumat. Tuntemattomia jaksoja, joiden kesto on negatiivinen (tuntemattoman jakson alku on myöhempi kuin tuntemattoman jakson loppu) eri valvontalaitteiden aikojen päällekkäisyyksien vuoksi, ei oteta laskelmissa huomioon.

Jos kuljettaja ei ole asettanut korttiaan laitteeseen, laskelmat perustuvat niihin datamuistin tietoihin, jotka liittyvät kuluvaan jaksoon, jolloin korttia ei ollut asetettuna laitteen asianmukaiseen aukkoon.

q) **Datamuisti:**

Elektroninen tietojen tallennuslaite, joka on osa valvontalaitetta.

r) **Digitaalinen allekirjoitus:**

Tietokenttään lisätty data tai tietokentän salakirjoitukseksi muunnettu sisältö, jonka avulla vastaanottaja voi varmistautua tietokentän sisällön muuttamattomuudesta ja eheydestä.

s) **Kopiointi:**

Ajoneuvon datamuistiin tai ajopiirturikortin muistiin tallennettujen tietojen osittainen tai täydellinen kopioiminen digitaalisesti allekirjoitettuna.

Kopiointi ei saa muuttaa tai poistaa tallennettuja tietoja.

⁽¹⁾ Tämän keskeytymättömän ajoajan ja yhteenlasketun taukoajan laskutavan ansiosta valvontalaitteet kykenevät laskemaan keskeytymättömän ajoajan ylityksestä annettavan varoituksen. Se ei kuitenkaan kumoaa näiden aikojen lainmukaista tulkintaa.

⁽²⁾ Tuntemattomat jaksot ovat jaksoja, jolloin kuljettajan kortti ei ole ollut asetettuna valvontalaitteeseen ja joita vastaavia kuljettajan toimintaa koskevia tietoja ei ole syötetty käsin.

t) **Kuljettajakortti:**

Ajopiirturikortti, jonka jäsenvaltion viranomaiset ovat myöntäneet tietyille kuljettajalle.

Kuljettajakortti yksilöi kuljettajan ja sen avulla voidaan tallentaa tietoja kuljettajan toiminnasta.

u) **Pyörien renkaiden tehollinen ympärysmitta:**

Ajoneuvoa liikkuttavien pyörien (vetävien pyörien) yhden täyden kierroksen aikana kulkemien matkojen keskiarvo. Nämä matkat on mitattava tavanomaisissa testausolosuhteissa (ks. VI luvun 5 jakso) ja ilmaistava muodossa: $l = \dots$ mm. Ajoneuvojen valmistajat voivat näiden matkojen mittaamisen sijaan tehdä teoreettisen laskelman, jossa otetaan huomioon painon jakautuminen akselleille ajoneuvon ollessa kuormaamaton ja normaalissa ajokunnossa⁽¹⁾. Jäsenvaltioiden toimivaltaiset viranomaiset hyväksyvät tällaisissa teoreettisissa laskelmissa käytettävät menetelmät.

v) **Tapaus:**

Valvontalaitteen havaitsema epänormaali toiminta, joka saattaa olla seurausta väärinkäytöksen yrityksestä.

w) **Vikatapahtuma:**

Valvontalaitteen havaitsema epänormaali toiminta, joka saattaa olla seurausta laitteen virheellisestä toiminnasta tai rikkoutumisesta.

x) **Asennus:**

Valvontalaitteen asentaminen ajoneuvoon.

y) **Liiketunnistin:**

Valvontalaitteen osa, joka tuottaa ajoneuvon nopeutta ja/tai sen kulkemaa matkaa kuvaavan signaalin.

z) **Kortti, joka ei ole voimassa:**

Kortti, joka on havaittu vialliseksi tai jonka alkuvarmennus epäonnistui tai jonka voimassaoloaika ei ole vielä alkanut tai jonka voimassaoloaika on loppunut.

aa) **Asetuksen piiriin kuulumaton:**

Tilanne, jossa neuvoston asetuksen (ETY) N:o 3820/85 mukaisesti ei edellytetä valvontalaitteen käyttöä.

bb) **Ylinopeus:**

Ajoneuvolle sallitun nopeuden ylittäminen, joksi määritellään mikä hyvänsä 60 sekuntia ylittävä aika, jonka kuluessa ajoneuvon nopeus ylittää sellaisen nopeudenrajoittimen asetusrajat, josta on säädetty tiettyjen moottoriajoneuvoluokkien nopeudenrajoittimien asentamisesta ja käytöstä yhteisössä 10 päivänä helmikuuta 1992 annetussa neuvoston direktiivissä 92/6/ETY⁽²⁾.

cc) **Määräaikaistarkastus:**

Toimenpide, jonka tarkoituksena on tarkastaa, että valvontalaite toimii asianmukaisesti ja että sen asetukset vastaavat ajoneuvon arvoja.

dd) **Tulostin:**

Valvontalaitteen osa, jolla tulostetaan tallennettuja tietoja.

ee) **Valvontalaitteisto:**

Kaikki ne laitteet, jotka on tarkoitettu asennettaviksi tieliikenneajoneuvoihin ja joiden avulla voidaan osoittaa, tallentaa ja säilyttää muistissa automaattisesti tai puoliautomaattisesti kyseisten ajoneuvojen liikkumista ja niiden kuljettajien tiettyjä työaikoja koskevat yksityiskohdat.

⁽¹⁾ Euroopan parlamentin ja neuvoston direktiivi 97/27/EY, annettu 22 päivänä heinäkuuta 1997, tiettyihin luokkiin kuuluvien moottoriajoneuvojen ja niiden perävaunujen massoista ja mitoista ja direktiivin 70/156/ETY muuttamisesta (EYVL L 233, 25.8.1997, s. 1).

⁽²⁾ EYVL L 57, 2.3.1992, s. 27.

ff) **Uusiminen:**

Uuden ajopiirturikortin myöntäminen entisen vanhentuuessa tai silloin, kun entinen toimii virheellisesti ja on palautettu sen myöntäneelle viranomaiselle. Uusimistapauksissa on aina oltava varmuus siitä, ettei samanaikaisesti ole olemassa kahta voimassa olevaa korttia.

gg) **Korjaus:**

Sellainen liiketunnistimen tai ajoneuvoyksikön korjaustoimenpide, joka edellyttää niiden kytkemistä irti virtalähteestään tai muista valvontalaitteen osista tai niiden avaamista.

hh) **Korvaus:**

Ajopiirturikortin myöntäminen korvaamaan entinen kortti, joka on ilmoitettu kadonneeksi, varastetuksi tai epäkuntoiseksi ja jota ei ole palautettu sen myöntäneelle viranomaiselle. Korvaustapauksissa on aina olemassa vaara, että samanaikaisesti on olemassa kaksi voimassa olevaa korttia.

ii) **Turvavarmennus:**

ITSEC ⁽¹⁾-sertifiointielimen suorittama toimenpide sen varmentamiseksi, että tutkittava valvontalaite (tai sen osa) tai ajopiirturikortti täyttää ne tietoturva vaatimukset, jotka on määritelty lisäyksessä 10 'Yleiset tietoturvatavoitteet'.

jj) **Laitteen itse suorittama testi:**

Testi, jonka valvontalaite suorittaa säännöllisesti ja automaattisesti vikojen havaitsemiseksi.

kk) **Ajopiirturikortti:**

Älykortti, joka on tarkoitettu käytettäväksi valvontalaitteen yhteydessä. Ajopiirturikorttien avulla valvontalaite voi tunnistaa kortin haltijan henkilöllisyyden (tai ryhmän, johon hän kuuluu) ja sallia tietojen siirron tai tallennuksen. Ajopiirturikortit voivat olla:

- kuljettajakortteja,
- valvontakortteja,
- korjaamokortteja,
- yrityskortteja;

ll) **Tyyppihyväksyntä:**

Menettely, jolla jäsenvaltio varmistaa, että tutkittava valvontalaite (tai sen osa) tai ajopiirturikortti täyttää tämän asetuksen vaatimukset.

mm) **Rengaskoko:**

Neuvoston direktiivin 92/23/ETY ⁽²⁾ mukainen renkaiden (ulkorenkaiden) koon määrite.

nn) **Ajoneuvon tunnistus:**

Ajoneuvon yksilöivä tunnus: ajoneuvon rekisteritunnus siihen liittyvine tietoineen rekisteröintijäsenvaltiosta ja valmistenumero ⁽³⁾.

oo) **Ajoneuvoyksikkö:**

Valvontalaite ilman liiketunnistinta ja sen liitântäkaapeleita. Ajoneuvoyksikkö voi koostua joko yhdestä laitteesta tai useista eri puolilla ajoneuvoa olevista laitteista edellyttäen, että ne täyttävät tämän asetuksen tietoturva vaatimukset.

⁽¹⁾ Neuvoston suositus 95/144/EY, annettu 7 päivänä huhtikuuta 1995, yleisistä tietotekniikan turvallisuuden arviointiperusteista (EYVL L 93, 26.4.1995, s. 27).

⁽²⁾ EYVL L 129, 14.5.1992, s. 95.

⁽³⁾ Neuvoston direktiivi 76/114/ETY, (EYVL L 24, 30.1.1976, s. 1).

pp) **Valvontalaitteen viikko tietojenkäsittelytarkoituksessa:**

Ajanjakso maanantaista klo 00.00 UTC-aikaa sunnuntaihin klo 24.00 UTC-aikaa.

qq) **Korjaamokortti:**

Jäsenvaltion viranomaisten kyseisen jäsenvaltion hyväksymille valvontalaitteiden valmistajalle, asentajalle, ajoneuvojen valmistajalle tai korjaamolle myöntämä ajopiirturikortti.

Korjaamokortti yksilöi kortin haltijan, ja sen avulla voidaan testata ja kalibroida valvontalaitteita ja/tai kopioida niiden tietoja.

II VALVONTALAITTEEN YLEISET OMINAISUUDET JA TOIMINNOT

000 Ajoneuvossa, johon on asennettu tämän liitteen määräysten mukainen valvontalaite, on oltava nopeus- ja matkamittari. Nämä toiminnot voivat kuulua osana valvontalaitteeseen.

1. **Yleiset ominaisuudet**

Valvontalaitteen tarkoitus on kirjata, tallentaa, näyttää, tulostaa paperille ja muulla tavoin tulostaa kuljettajan toimintaan liittyviä tietoja.

001 Valvontalaite koostuu kaapeleista, liiketunnistimesta ja ajoneuvoyksiköstä.

002 Ajoneuvoyksikön osat ovat keskusyksikkö, datamuisti, tosiaikainen kello, kaksi älykortin liitäntälaitetta (kuljettajalle ja apukuljettajalle), tulostin, näyttö, näkyvä varoitin, kalibrointi-/kopiointiliitin sekä laitteet, joilla käyttäjä voi syöttää tietoja.

Valvontalaite voidaan liittää muihin laitteisiin lisäliittimien avulla.

003 Mikään valvontalaitteeseen lisätty tai liitetty toiminto, laite tai laitteisto, riippumatta siitä, onko sillä hyväksyntä tai ei, ei saa häiritä tai kyetä häiritsemään valvontalaitteen asianmukaista ja turvallista toimintaa tai olla ristiriidassa tämän asetuksen määräysten kanssa.

Valvontalaitteen käyttäjät antavat laitteelle tunnistetietonsa ajopiirturikorttien avulla.

004 Valvontalaite antaa valikoidut tietojen ja toimintojen käyttöoikeudet käyttäjätyyppin ja/tai käyttäjän henkilöllisyyden perusteella.

Valvontalaite kirjaa ja tallentaa tietoja datamuistiinsa ja ajopiirturikortteille.

Tämä tapahtuu Euroopan parlamentin ja neuvoston 24 lokakuuta 1995 antaman, yksilöiden suojelua henkilötietojen käsittelyssä ja näiden tietojen vapaata liikkuvuutta koskevan direktiivin 95/46/EY mukaisesti ⁽¹⁾.

2. **Toiminnot**

005 Valvontalaitteen on huolehdittava seuraavista toiminnoista:

- korttien paikoilleen asetuksen ja poistamisen valvonta,
- nopeuden ja matkan mittaus,
- ajanmittaus,
- kuljettajan toiminnan valvonta,
- ajoneuvon miehityksen valvonta,
- kuljettajan käsin syöttämät tiedot:
 - tiedot paikasta, jossa päivän työaika alkaa ja/tai päättyy,
 - kuljettajan toimintaa koskevien tietojen syöttö käsin,
 - erityisolosuhteita koskevien tietojen syöttö,

⁽¹⁾ EYVL L 281, 23.11.1995, s. 31.

- yritysten tekemien lukitusten hallinta,
- tarkastustoimien hallinta,
- tapauksien ja/tai vikojen havaitseminen,
- sisäänrakennetut ja laitteen itse suorittamat testit,
- tietojen haku datamuistista,
- tietojen kirjaaminen ja tallentaminen datamuistiin,
- tietojen haku ajopiirturikorteilta,
- tietojen kirjaaminen ja tallentaminen ajopiirturikortteille,
- tietojen näyttö,
- tulostus,
- varoitukset,
- tietojen kopiointi ulkoisille tietovälineille,
- tietojen tulostaminen muille ulkoisille välineille,
- kalibrointi,
- ajan asetus.

3. Toimintatilat

006 Valvontalaitteella on oltava neljä toimintatilaa:

- normaalitila,
- tarkastustila,
- kalibrointitila,
- yritystila.

007 Valvontalaitteen on siirryttävä seuraaviin toimintatiloihin liitälaitteisiin asetettujen voimassa olevien ajopiirturikorttien mukaisesti:

Toimintatila		Kuljettajan korttiaukko				
		Ei korttia	Kuljettajakortti	Valvontakortti	Korjaamokortti	Yrityskortti
Apukuljettajan korttiaukko	Ei korttia	Normaali	Normaali	Tarkastus	Kalibrointi	Yritys
	Kuljettajakortti	Normaali	Normaali	Tarkastus	Kalibrointi	Yritys
	Valvontakortti	Tarkastus	Tarkastus	Tarkastus (*)	Normaali	Normaali
	Korjaamokortti	Kalibrointi	Kalibrointi	Normaali	Kalibrointi (*)	Normaali
	Yrityskortti	Yritys	Yritys	Normaali	Normaali	Yritys (*)

008 (*) Näissä tapauksissa valvontalaitteen on käytettävä ainoastaan kuljettajan korttiaukkoon asetettua ajopiirturikorttia.

- 009 Valvontalaite ei saa hyväksyä siihen asetettuja kortteja, jotka eivät ole voimassa, mutta vanhentuneella kortilla olevien tietojen näyttämisen, tulostamisen tai kopioinnin on oltava mahdollista.
- 010 Kaikkien kohdassa II.2 lueteltujen toimintojen on oltava käytettävissä kaikissa toimintatiloissa seuraavin poikkeuksin:
- kalibrintoiminto on käytettävissä vain kalibrintilassa,
 - ajan asetustoiminnon käytettävyys muussa kuin kalibrintilassa on rajoitettu,
 - toiminto, jolla kuljettaja voi syöttää tietoja käsin, on käytettävissä vain normaali- ja kalibrintilassa,
 - yritysten tekemien lukitusten hallintatoiminto on käytettävissä vain yritystilassa,
 - tarkastustoimien hallintatoiminto on käytettävissä vain tarkastustilassa,
 - kopiointitoiminto ei ole käytettävissä normaalitilassa (paitsi vaatimuksessa 150 kuvatuissa tapauksissa).
- 011 Valvontalaite voi tulostaa kaikkia tietoja näyttöön, tulostimeen tai ulkoihin liitälaitteisiin seuraavin poikkeuksin:
- normaalitilassa sellaiset henkilötiedot (sukunimi ja etunimi (-nimet)), jotka eivät vastaa laitteeseen asetettua ajopiirturikorttia, tulostetaan tyhjinä, ja sellaiset korttinumerot, jotka eivät vastaa laitteeseen asetettua ajopiirturikorttia, tulostetaan osittain tyhjinä (jokainen poikkeava merkki – vasemmalta oikealle – tulostetaan tyhjänä),
 - yritystilassa voidaan kuljettajaan liittyviä tietoja (vaatimukset 081, 084 ja 087) tulostaa vain jaksoilta, joita toinen yritys (joka yksilöidään yrityskortin numeron 13 ensimmäisen numeron avulla) ei ole lukinnut,
 - kun valvontalaitteeseen ei ole asetettu mitään korttia, kuljettajaan liittyvien tietojen tulostaminen on mahdollista vain kuluvan ja kahdeksan edellisen kalenterivuorokauden osalta.

4. Tietoturva

Järjestelmän tietoturvan tavoitteena on suojata datamuistia siten, että se ehkäisee tietojen luvattoman käytön ja muuttamisen sekä havaitsee näiden yritykset, suojaa liiketunnistimen ja ajoneuvoyksikön välillä siirrettävien tietojen eheyttä ja muuttamattomuutta, suojaa valvontalaitteen ja ajopiirturikorttien välillä siirrettävien tietojen eheyttä ja muuttamattomuutta sekä varmistaa kopioitavien tietojen eheyden ja muuttamattomuuden.

- 012 Järjestelmän tietoturvan takaamiseksi valvontalaitteen on täytettävä tietoturva-vaatimukset, jotka on määritelty liiketunnistimen ja ajoneuvoyksikön yleisissä tietoturvatavoitteissa (lisäys 10).

III VALVONTALAITTEIDEN RAKENNETTA JA TOIMINTOJA KOSKEVAT VAATTIMUKSET

1. Korttien paikoilleen asetuksen ja poistamisen valvonta

- 013 Valvontalaitteen on valvottava korttien liitälaitteita, jotta se havaitsee korttien paikoilleen asetuksen ja poistamisen.
- 014 Korttia sisään asettaessa valvontalaitteen on tunnistettava, onko sisään asetettu kortti voimassa oleva ajopiirturikortti, ja jos on, tunnistaa sen tyyppi.
- 015 Valvontalaitteen on oltava suunniteltu siten, että ajopiirturikortit lukittuvat paikoilleen, kun ne on asetettu oikein korttien liitälaitteisiin.
- 016 Ajopiirturikorttien paikoilleen lukituksen avaus saa toimia vain ajoneuvon ollessa pysähtyneenä ja vasta silloin, kun kaikki asianmukaiset tiedot on tallennettu korteille. Korttien paikoilleen lukituksen avautuminen saa tapahtua vain avajan nimenomaisesta toimenpiteestä.

2. Nopeuden ja matkan mittaus

- 017 Tämän toiminnon on jatkuvasti mitattava matkamittarin lukemaa ja kyettävä antamaan lukema, joka vastaa ajoneuvon kulkemaa kokonaismatkaa.
- 018 Tämän toiminnon on jatkuvasti mitattava ajoneuvon nopeutta ja kyettävä antamaan nopeuslukema.

- 019 Nopeudenmittaustoiminnon on myös annettava tieto siitä, onko ajoneuvo liikkeessä vai pysähtyneenä. Ajoneuvon katsotaan olevan liikkeessä, kun toiminto havaitsee liiketunnistimelta useamman kuin 1 impulssin sekunnissa vähintään viiden sekunnin ajan; muussa tapauksessa ajoneuvon katsotaan olevan pysähtyneenä.

Tämän asetuksen mukaisella valvontalaitteella varustettuihin ajoneuvoihin asennettujen laitteiden, jotka osoittavat nopeutta (nopeusmittari) ja kokonaismatkaa (matkamittari), on täytettävä tässä liitteessä (kohdat III.2.1 ja III.2.2) annetut virherajoja koskevat vaatimukset.

2.1 Kuljetun matkan mittaus

- 020 Kuljettu matka voidaan mitata joko:

- eteen- ja taaksepäin kuljettujen matkojen summana, tai
- siten, että se sisältää ainoastaan eteenpäin kuljetun matkan.

- 021 Valvontalaitteen on mitattava matkaa välillä 0–9 999 999,9 km.

- 022 Mitatun matkan on oltava seuraavissa virherajoissa (koskee vähintään 1 000 metrin pituisia matkoja):

- ± 1 % ennen asennusta,
- ± 2 % asennettuna ja määräaikaistarkastusten aikana,
- ± 4 % normaalikäytössä.

- 023 Mitatun matkan lukematarkkuuden on oltava 0,1 km tai parempi.

2.2 Nopeuden mittaus

- 024 Valvontalaitteen on mitattava nopeutta välillä 0–220 km/t.

- 025 Jotta varmistetaan osoitetun nopeuden enimmäisvirheeksi ± 6 km/t normaalikäytössä ja kun otetaan huomioon:

- sisääntulosignaalin vaihtelusta (renkaiden eroista, ...) aiheutuva virhe suuruudeltaan ± 2 km/t,
- asennuksen tai määräaikaistarkastusten yhteydessä tehtyjen mittausten virhe suuruudeltaan ± 1 km/t,

valvontalaitteen on nopeusalueella 20–180 km/t ja ajoneuvon ominaiskertoimen ollessa välillä 4 000–25 000 imp/km kyettävä mittaamaan nopeus tarkkuudella ± 1 km/t (ajettaessa tasaista nopeutta).

Huomaus: Tiedontallennuksen lukematarkkuus aiheuttaa valvontalaitteen tallentamaan nopeuslukemaan lisävirheen suuruudeltaan $\pm 0,5$ km/t.

- 025a Nopeuden mittauksen on tapahduttava oikein ja normaaleissa virherajoissa kahden sekunnin kuluessa siitä, kun nopeuden muutos on päättynyt, kun nopeuden muutosnopeus on enintään 2 m/s^2 .

- 026 Nopeuden mittauksen lukematarkkuuden on oltava 1 km/t tai parempi.

3. Ajanmittaus

- 027 Ajanmittaustoiminnon on mitattava jatkuvasti UTC-päivämäärä ja -aika ja annettava ne digitaalimuodossa.

- 028 UTC-päivämäärää ja -aikaa on käytettävä kaikkiin valvontalaitteen päiväyksiin (tallenteet, tulosteet, tietojen siirto, näyttö, ...).

- 029 Paikallisen ajan näyttämiseksi on näytettävän ajan ero UTC-aikaan nähdén oltava aseteltavissa puolen tunnin välein.

- 030 Kellon käyntitarkkuuden on tyyppihyväksyntää vastaavissa olosuhteissa oltava rajoissa ± 2 sekuntia/päivä.

- 031 Mitatun ajan lukematarkkuuden on oltava 1 sekunti tai parempi.

- 032 Ulkoisen virtalähteen kytkeminen pois lyhyemmäksi kuin 12 kuukauden ajaksi ei saa vaikuttaa ajanmittaukseen tyyppihyväksyntää vastaavissa olosuhteissa.

4. Kuljettajan toiminnan valvonta

- 033 Tämän toiminnon on jatkuvasti ja erikseen seurattava yhden kuljettajan ja yhden apukuljettajan toimintaa.
- 034 Kuljettajan toimintaa on DRIVING (ajo), WORK (työ), AVAILABILITY (varallaolo) tai BREAK/REST (tauko/lepo).
- 035 Kuljettajan ja/tai apukuljettajan on kyettävä käsin valitsemaan WORK, AVAILABILITY tai BREAK/REST.
- 036 Kun ajoneuvo on liikkeessä, laitteen on automaattisesti valittava kuljettajalle DRIVING ja apukuljettajalle AVAILABILITY.
- 037 Kun ajoneuvo pysähtyy, laitteen on automaattisesti valittava kuljettajalle WORK.
- 038 Ensimmäinen toiminnan muutos, joka tapahtuu 120 sekunnin kuluessa siitä, kun ajoneuvon pysäyttäminen aiheutti WORK-toiminnan automaattisen valinnan, katsotaan tapahtuneeksi sillä hetkellä, kun ajoneuvo pysähtyi (ja sen vuoksi tämä toiminta mahdollisesti peruuttaa valinnan WORK).
- 039 Tämän toiminnon on tulostettava toiminnan muutokset tallennustoiminnoille yhden minuutin tarkkuudella.
- 040 Jos tietyn kalenteriminuutin aikana on ollut DRIVING-toimintaa, katsotaan koko minuutti kuluneeksi DRIVING-toiminnassa.
- 041 Jos DRIVING-toimintaa on ollut sekä tiettyä kalenteriminuuttia välittömästi edeltävän minuutin että sitä välittömästi seuraavan minuutin aikana, katsotaan koko minuutti kuluneeksi DRIVING-toiminnassa.
- 042 Jos tiettyä kalenteriminuuttia ei edellä olevan nojalla katsota kuluneeksi DRIVING-toiminnassa, katsotaan koko minuutin kuluneen siinä toiminnassa, joka edustaa pisintä yhtäjaksoista toimintaa kyseisen minuutin aikana (tai viimeisintä pisimmistä jaksoista, jos yhtä pitkiä pisimpiä jaksoja on useampia).
- 043 Tämän toiminnon on myös jatkuvasti valvottava keskeytymätöntä ajoaikaa ja kuljettajan yhteenlaskettua taukoaikaa.

5. Ajoneuvon miehityksen valvonta

- 044 Tämä toiminto valvoo jatkuvasti ja automaattisesti ajoneuvon miehitystä.
- 045 Valvontalaitteen on automaattisesti valittava asetus CREW (miehistö), kun siihen on asetettu kaksi voimassa olevaa kuljettajakorttia; muissa tapauksissa sen on valittava asetus SINGLE (yksin).

6. Kuljettajan käsin syöttämät tiedot

6.1 Tiedot paikasta, jossa päivän työaika alkaa ja/tai päättyy

- 046 Tämän toiminnon avulla on voitava syöttää tiedot paikoista, joissa kuljettajan ja/tai apukuljettajan päivän työaika alkaa ja/tai päättyy.
- 047 Paikat määritellään valtion ja tarvittaessa myös alueen tarkkuudella.
- 048 Kun kuljettajakortti (tai korjaamokortti) poistetaan, valvontalaitteen on kehotettava (apu)kuljettajaa syöttämään 'tiedot paikasta, jossa päivän työaika päättyy'.
- 049 Valvontalaitteen on sallittava se, ettei tätä kehotusta noudateta.
- 050 Päivän työajan alkamis- ja/tai päättymispaikkoja koskevien tietojen syöttämisen on oltava mahdollista ilman korttia tai muulloinkin kuin korttia paikoilleen asettaessa tai poistettaessa.

6.2 Kuljettajan toimintaan liittyvien tietojen syöttö käsin

- 050a Asettaessa paikoilleen kuljettajakorttia (tai korjaamokorttia), ja ainoastaan tällöin, valvontalaitteen on:
- kerrottava kortin haltijalle päivämäärä ja aika, jolloin tämä edellisen kerran poisti korttinsa, ja
 - kysyttävä kortin haltijalta, onko nyt tapahtuva kortin paikoilleen asetus merkinä kuluvan päivän työajan jatkamisesta.

Valvontalaitteen on sallittava se, ettei kortin haltija vastaa kysymykseen, tai se, että hän vastaa myöntävästi tai kieltävästi:

- jos kortin haltija ei vastaa kysymykseen, valvontalaitteen on kehotettava kortin haltijaa syöttämään tiedot, jotka koskevat 'päivän työajan alkamispaikkaa'. Valvontalaitteen on sallittava se, ettei tätä kehotusta noudateta. Jos paikkaa koskevat tiedot syötetään, laitteen on tallennettava ne datamuistiin ja ajopiirturikortille ja liitettävä ne tietoon ajasta, jolloin kortti asetettiin paikoilleen,
- jos annetaan kieltävä tai myöntävä vastaus, valvontalaitteen on kehotettava kortin haltijaa syöttämään käsin toimintaa koskevat tiedot, mukaan lukien toiminnan alkamis- ja päättymisajat, ja käyttämään vain toimintatyyppiä WORK, AVAILABILITY tai BREAK/REST, jotka koskevat pelkästään aikaväliä kortin poistosta tähän paikoilleen asettamiseen ilman, että syötettyjen toimintatietojen ajoissa on päällekkäisyyttä. Tämä on tehtävä seuraavasti:
 - kun kortin haltija vastaa kysymykseen myöntävästi, valvontalaitteen on kehotettava kortin haltijaa syöttämään toimintatiedot käsin aikajärjestyksessä, kortin poistosta tähän paikoilleen asettamiseen. Syöttämisen on päättyvä, kun käsin syötetyn toimintatiedon päättymisaika on sama kuin aika, jolloin kortti asetettiin paikoilleen,
 - kun kortin haltija vastaa kysymykseen kieltävästi, valvontalaitteen on:
 - kehotettava kortin haltijaa syöttämään toimintatiedot käsin aikajärjestyksessä kortin poistohetkestä siihen hetkeen, kun kyseessä olevan päivän työaika päättyi (tai kun kyseiseen ajoneuvoon liittyvä toiminta päättyi, jos päivän työaika jatkui normaalin tuntikirjanpidon puitteissa). Tämän vuoksi valvontalaitteen on kysyttävä kortin haltijalta, oliko viimeksi tallennetun toiminnan päättymisaika sama kuin edellisen työajan päättymisaika, ennen kuin se antaa kortin haltijan syöttää käsin kutakin toimintaa koskevan tiedon (ks. seuraava huomautus),

Huomautus: Jos kortin haltija ei kerro laitteelle, milloin edellinen työaika päättyi, ja syöttää käsin tiedon toiminnasta, jonka päättymisaika on sama kuin aika, jolloin kortti asetettiin paikoilleen, valvontalaitteen on:

- oletettava, että päivän työaika päättyi, kun ensimmäinen REST-jakso (tai edelleen tuntematon UNKNOWN-jakso) kortin poistamisen jälkeen alkoi tai, jos lepojaksota ei ole syötetty (eikä mikään jakso enää ole tuntematon UNKNOWN-jakso), kun kortti poistettiin,
- oletettava, että aloitusaika (ks. jäljempänä) on sama kuin aika, jolloin kortti asetettiin paikoilleen,
- jatkettava kuten jäljempänä on selostettu,
- seuraavaksi, jos kyseisen työajan päättymisaika on eri kuin kortin poistamisaika tai jos päivän työajan päättymisaikaa ei tuolloin ole syötetty, kehotettava kortin haltijaa 'vahvistamaan tai syöttämään päivän työajan päättymisaikaa' (valvontalaitteen on sallittava se, ettei tätä kehotusta noudateta). Jos paikka syötetään, se on tallennettava ainoastaan ajopiirturikortille ja vain siinä tapauksessa, että se eroaa korttia poistettaessa syötetystä paikasta (jos sellainen syötettiin), ja mukana on oltava tieto ajasta, jolloin työaika päättyi,
- seuraavaksi kehotettava kortin haltijaa 'syöttämään päivän työajan alkamisaika' (tai kyseiseen ajoneuvoon liittyvän toiminnan alkamisaika, jos kortin haltija on aikaisemmin tämän työajan kuluessa työskennellyt normaalin tuntikirjanpidon puitteissa) sekä kehotettava kortin haltijaa syöttämään 'päivän työajan alkamispaikka' (valvontalaitteen on sallittava se, ettei tätä kehotusta noudateta). Jos alkamispaikka syötetään, se on tallennettava ajopiirturikortille ja mukana on oltava tieto alkamisajasta. Jos mainittu alkamisaika on sama kuin aika, jolloin kortti asetettiin paikoilleen, alkamispaikka on myös tallennettava datamuistiin,
- seuraavaksi, jos mainittu alkamisaika on eri kuin aika, jolloin kortti asetettiin paikoilleen, kehotettava kortin haltijaa syöttämään toimintatiedot käsin aikajärjestyksessä mainitusta alkamisajasta siihen hetkeen, jolloin kortti asetettiin paikoilleen. Syöttämisen on päättyävä, kun käsin syötetyn toimintatiedon päättymisaika on sama kuin aika, jolloin kortti asetettiin paikoilleen,
- seuraavaksi valvontalaitteen on sallittava se, että kortin haltija muokkaa käsin syötettyjä toimintatietoja, kunnes kortin haltija vahvistaa ne valitsemalla tietyn komennon, minkä jälkeen laitteen on estettävä kaikki muokkaaminen,
- jos alkuperäiseen kysymykseen vastataan ilman, että sen jälkeen syötetään toimintatietoja, valvontalaitteen on tulkittava tilanne samaksi kuin jos kortin haltija ei olisi vastannut kysymykseen.

Koko tapahtuman aikana valvontalaitteen on odotettava tietojen syöttöä enintään seuraavien viiveiden ajan:

- kunnes on kulunut 1 minuutti viimeisestä laitteen ja käyttäjän välisestä vuorovaikutuksesta (näkyvä ja mahdollisesti kuuluva varoitusmerkki annetaan 30 sekunnin kuluttua), tai
- kunnes kortti poistetaan tai toinen kuljettajakortti (tai korjaamokortti) asetetaan paikoilleen, tai
- kunnes ajoneuvo lähtee liikkeelle,

jolloin valvontalaitteen on vahvistettava kaikki siihen mennessä syötetyt tiedot.

6.3 Erityisolosuhteisiin liittyvien tietojen syöttö

050b Valvontalaitteen on sallittava se, että kuljettaja syöttää tosiaikaisesti seuraavia erityisolosuhteita koskevat tiedot:

- OUT OF SCOPE (asetuksen piiriin kuulumaton) (alkaminen, päättyminen)
- FERRY/TRAIN CROSSING (lautta-/junamatka)

FERRY/TRAIN CROSSING -olosuhteita ei voi esiintyä, jos OUT OF SCOPE -olosuhteet ovat voimassa.

Valvontalaitteen on automaattisesti lopetettava OUT OF SCOPE -olosuhteiden voimassaolo, jos kuljettajakortti asetetaan paikoilleen tai poistetaan.

7. Yritysten tekemien lukitusten hallinta

- 051 Tämän toiminnon avulla on voitava hallita yrityksen tekemiä lukituksia, jotta vain sillä olisi mahdollisuus käyttää tietoja yritystilassa.
- 052 Yrityksen tekemät lukitukset sisältävät alkamispäivän ja -ajan (lukitseminen) ja päättymispäivän ja -ajan (lukituksen avaaminen), johon liittyy yrityksen tunnistus yrityskortin numeron perusteella (lukittaessa).
- 053 Lukituksia voi kytkeä 'päälle' tai 'pois' vain toisaikaisesti.
- 054 Lukituksen pois kytkemisen on oltava mahdollista vain yritykselle, jonka lukitus on 'päällä' (mikä tunnistetaan yrityskortin 13 ensimmäisen numeron perusteella), tai
- 055 lukituksen pois kytkemisen on tapahduttava automaattisesti, jos jokin toinen yritys tekee lukituksen.
- 055a Tapauksessa, jossa yritys tekee lukituksen ja aikaisempi lukitus on saman yrityksen, oletetaan, että aikaisempaa lukitusta ei ole kytketty 'pois', vaan se on yhä 'päällä'.

8. Tarkastustoimien hallinta

- 056 Tämän toiminnon on valvottava DISPLAYING (näyttö)-, PRINTING (tulostus)-, VU (ajoneuvoyksikkö)- sekä DOWNLOADING (kortin tietojen kopiointi) -toimenpiteitä laitteen ollessa tarkastustilassa.
- 057 Tämän toiminnon on myös valvottava OVER SPEEDING CONTROL (ylinopeuden valvonta) -toimenpiteitä laitteen ollessa tarkastustilassa. Ylinopeuden valvonta katsotaan tapahtuneeksi, kun ylinopeudesta kertova tuloste on lähetetty tulostimelle tai näytölle laitteen ollessa tarkastustilassa tai kun tapauksiin ja vikoihin liittyvät tiedot on kopioitu ajoneuvoyksikön datamuistista.

9. Tapauksien ja/tai vikojen havaitseminen

- 058 Tämän toiminnon on havaittava seuraavat tapaukset ja/tai viat:

9.1 'Kortti ei voimassa' -tapaus

- 059 Tämä tapaus syntyy, kun paikoilleen asetetaan jokin kortti, joka ei ole voimassa, ja/tai kun paikoilleen asetetun kortin voimassaoloaika umpeutuu.

9.2 'Korttiristiriitä'-tapaus

- 060 Tämä tapaus syntyy, kun jokin seuraavassa taulukossa kirjaimella X merkityistä kahden voimassa olevan kortin yhdistelmistä on asetettu paikoilleen:

Korttiristiriitä		Kuljettajan korttiauikko				
		Ei korttia	Kuljettajakortti	Valvontakortti	Korjaamokortti	Yrityskortti
Apukuljettajan korttiauikko	Ei korttia					
	Kuljettajakortti				X	
	Valvontakortti			X	X	X
	Korjaamokortti		X	X	X	X
	Yrityskortti			X	X	X

9.3 'Aikojen päällekkäisyys' -tapaus

- 061 Tämä tapaus syntyy, kun kortilta luettu viimeisin kuljettajakortin pois ottamisen päivämäärä/aika on myöhempi kuin se valvontalaitteen päivämäärä/aika, jolloin kortti asetetaan paikoilleen.

9.4 'Ajo ilman asianmukaista korttia' -tapaus

- 062 Tämä tapaus syntyy, kun jokin seuraavassa taulukossa kirjaimella X merkityistä ajopiirturikorttiyhdistelmistä on asetettu paikoilleen ja kuljettajan toiminta muuttuu DRIVING-toiminnaksi tai laitteen toimintatila muuttuu kuljettajan toiminnan ollessa tyyppiä DRIVING:

Ajo ilman asianmukaista korttia		Kuljettajan korttiauikko				
		Ei korttia (tai kortti ei voimassa)	Kuljettajakortti	Valvontakortti	Korjaamokortti	Yrityskortti
Apukuljettajan korttiauikko	Ei korttia (tai kortti ei voimassa)	X		X		X
	Kuljettajakortti	X		X	X	X
	Valvontakortti	X	X	X	X	X
	Korjaamokortti	X	X	X		X
	Yrityskortti	X	X	X	X	X

9.5 'Kortin paikoilleen asettaminen ajettaessa' -tapaus

- 063 Tämä tapaus syntyy, kun ajopiirturikortti asetetaan johonkin korttiaukkoon kuljettajan toiminnan ollessa DRIVING.

9.6 'Edellistä kortin käyttöjaksoa ei lopetettu oikein' -tapaus

- 064 Tämä tapaus syntyy, kun valvontalaite havaitsee korttia paikoilleen asetettaessa, että kohdan III.1 määräyksistä huolimatta kortin edellistä käyttöjaksoa ei ole lopetettu oikein (kortti on otettu pois ennen kuin kaikki asianmukaiset tiedot on tallennettu sille). Tämä tapaus koskee vain kuljettaja- ja korjaamokortteja.

9.7 'Ylinopeus'-tapaus

- 065 Tämä tapaus syntyy aina, kun ajetaan ylinopeutta.

9.8 'Keskeytynyt virransyöttö' -tapaus

- 066 Tämä tapaus syntyy, kun laite on muussa kuin kalibroitilassa ja liiketunnistimen tai ajoneuvoyksikön virransyöttö keskeytyy yli 200 millisekunnin ajaksi. Laitteen valmistajan on määriteltävä keskeytymisen kynnyisarvo. Jännitteen aleneminen ajoneuvoa käynnistettäessä ei saa aiheuttaa tätä tapausta.

9.9 'Virhe liikedatassa' -tapaus

- 067 Tämä tapaus syntyy, kun liiketunnistimen ja ajoneuvoyksikön välinen normaali datavirta keskeytyy ja/tai kun liiketunnistimen ja ajoneuvoyksikön välisen tiedonsiirron eheydessä tai autenttisuudessa ilmenee virhe.

9.10 'Tietoturvan murtoyritys' -tapaus

- 068 Tämä tapaus syntyy, kun ilmenee jokin muu tapaus, joka vaikuttaa liiketunnistimen ja/tai ajoneuvoyksikön yleisissä tietoturvatavoitteissa määriteltyyn tietoturvaan laitteen ollessa muussa kuin kalibroitilassa.

9.11 'Kortti'-vikatapahtuma

- 069 Tämä vikatapahtuma syntyy, kun ajopiirturikorttiin tulee vika käytön aikana.

9.12 'Valvontalaite'-vikatapahtuma

- 070 Tämä vikatapahtuma syntyy, kun jokin seuraavista vioista ilmenee laitteen ollessa muussa kuin kalibroitilassa:

- vika ajoneuvoyksikön sisällä
- vika tulostimessa
- vika näytössä
- tietojen kopiointiin liittyvä vika
- vika tunnistimessa

10. Sisäänrakennetut ja laitteen itse suorittamat testit

- 071 Valvontalaitteen on itse havaittava viat itse suorittamiensa ja sisäänrakennettujen testien avulla seuraavan taulukon mukaisesti:

Testattava osakokoonpano	Laitteen itse suorittama testi	Sisäänrakennettu testi
Ohjelmisto		Eheys
Datamuisti	Käyttö	Käyttö, datan eheys
Kortin liitäntälaitte	Käyttö	Käyttö
Näppäimistö		Tarkastus käsin
Tulostin	(riippuu valmistajasta)	Koetuloste
Näyttö		Silmämääräinen tarkastus
Tietojen kopiointi (suoritetaan vain kopiointin yhteydessä)	Virheetön toiminta	
Tunnistin	Virheetön toiminta	Virheetön toiminta

11. Tietojen haku datamuistista

- 072 Valvontalaitteen on kyettävä lukemaan kaikkea dataa, jota on tallennettu sen datamuistiin.

12. Tietojen kirjaaminen ja tallentaminen datamuistiin

Tässä kohdassa:

- 365 vuorokaudella tarkoitetaan 365:tä keskimääräistä kuljettajan toimintaa sisältävää kalenterivuorokautta. Keskimääräisen päivittäisen toiminnan ajoneuvossa määritellään sisältävän vähintään kuusi kuljettajaa tai apukuljettajaa, kuusi kortin paikoilleen asettamis- ja poistotapahtumaa sekä 256 muutosta toiminnan tilassa. Näin ollen '365 vuorokautta' sisältää vähintään 2 190 (apu)kuljettajaa, 2 190 kortin paikoilleen asettamis- ja poistotapahtumaa sekä 93 440 muutosta toiminnan tilassa.
- ajat kirjataan yhden minuutin tarkkuudella, ellei toisin määritellä.
- matkamittarin lukemat kirjataan yhden kilometrin tarkkuudella.
- nopeudet kirjataan tarkkuudella 1 km/t.

073 Ulkoisen virransyötön katkeaminen lyhyemmäksi kuin 12 kuukauden ajaksi ei saa vaikuttaa datamuistiin tallennettuun dataan tyyppihyväksyntää vastaavissa olosuhteissa.

074 Valvontalaitteen on kyettävä epäsuorasti tai suoraan kirjaamaan ja tallentamaan datamuistiinsa seuraavat tiedot:

12.1 Laitteen tunnistetiedot

12.1.1 Ajoneuvoyksikön tunnistetiedot

075 Valvontalaitteen on kyettävä tallentamaan datamuistiinsa seuraavat ajoneuvoyksikön tunnistetiedot:

- valmistajan nimi,
- valmistajan osoite,
- osanumero,
- sarjanumero,
- ohjelmistoversion numero,
- ohjelmaversion asennuspäivämäärä,
- laitteen valmistusvuosi,
- hyväksyntänumero.

076 Ajoneuvoyksikön valmistaja kirjaa ja tallentaa yksikön tunnistetiedot yhdellä kertaa, lukuun ottamatta ohjelmistoon liittyviä tietoja ja hyväksyntänumeroa, joita voidaan muuttaa ohjelmistoa päivitettäessä.

12.1.2 Liiketunnistimen tunnistetiedot

077 Liiketunnistimen on kyettävä tallentamaan muistiinsa seuraavat tunnistetiedot:

- valmistajan nimi,
- osanumero,
- sarjanumero,
- hyväksyntänumero,
- tunnistimeen sulautetun tietoturvakomponentin tunniste (esim. sirun/proessorin osanumero),
- käyttöjärjestelmän tunniste (esim. ohjelmistoversion numero).

- 078 Liiketunnistimen valmistaja kirjaa ja tallentaa liiketunnistimen tunnistetiedot liiketunnistimeen yhdellä kertaa.
- 079 Ajoneuvoyksikön on kyettävä kirjaamaan ja tallentamaan datamuistiinsa seuraavat siihen liitetyn liiketunnistimen tunnistetiedot:
- sarjanumero,
 - hyväksyntänumero,
 - päivämäärä, jolloin tunnistin ensi kerran liitettiin ajoneuvoyksikköön.

12.2 *Tietoturvan osatekijät*

- 080 Valvontalaitteen on kyettävä tallentamaan seuraavat tietoturvan osatekijät:
- eurooppalainen julkinen avain,
 - jäsenvaltion myöntämä todistus,
 - laitteelle myönnetty todistus,
 - laitteen yksityinen avain.

Ajoneuvoyksikön valmistaja tallentaa tietoturvan osatekijät valvontalaitteeseen.

12.3 *Kuljettajakortin paikoilleen asetukseen ja poistamiseen liittyvät tiedot*

- 081 Aina kun kuljettaja- tai korjaamokortti asetetaan paikoilleen laitteeseen tai poistetaan siitä, valvontalaitteen on tallennettava ja säilytettävä datamuistissaan:
- kortin haltijan sukunimi ja etunimi (-nimet) siinä muodossa kuin ne on tallennettu kortille,
 - kortin numero, kortin myöntänyt jäsenvaltio sekä viimeinen voimassaolopäivä siinä muodossa kuin ne on tallennettu kortille,
 - päivämäärä ja aika, jolloin kortti asetettiin paikoilleen,
 - ajoneuvon matkamittarin lukema hetkellä, jolloin kortti asetettiin paikoilleen,
 - korttiaukko, johon kortti on asetettu,
 - päivämäärä ja aika, jolloin kortti poistettiin,
 - ajoneuvon matkamittarin lukema hetkellä, jolloin kortti poistettiin,
 - seuraavat tiedot ajoneuvosta, jota kuljettaja käytti ennen tätä, siinä muodossa kuin ne on tallennettu kortille:
 - rekisteritunnus ja jäsenvaltio, jossa ajoneuvo on rekisteröity,
 - päivämäärä ja aika, jolloin kortti poistettiin,
 - tunnus, josta ilmenee, onko kuljettaja korttia paikoilleen asettaessaan syöttänyt toimintatietoja käsin.
- 082 Datamuistin on kyettävä tallentamaan näitä tietoja vähintään 365 vuorokauden ajalta.
- 083 Kun tiedontallennuskapasiteetti loppuu, uusimpien tietojen on korvattava vanhimmat tiedot.

12.4 *Kuljettajan toimintaan liittyvät tiedot*

084 Aina kun kuljettajan ja/tai apukuljettajan toiminnan tyyppi muuttuu ja/tai ajoneuvon miehitys muuttuu ja/tai kuljettaja- tai korjaamokortti asetetaan paikoilleen tai poistetaan, valvontalaitteen on tallennettava ja säilytettävä datamuistissaan:

- ajoneuvon miehitys (CREW, SINGLE),
- korttiaukko (DRIVER, CO-DRIVER),
- kunkin korttiaukon tila (INSERTED (kortti asetettu), NOT INSERTED (korttia ei asetettu)) (ks. huomautus),
- toiminta (DRIVING, AVAILABILITY, WORK, BREAK/REST),
- päivämäärä ja aika, jolloin muutos tapahtui.

Huomautus: INSERTED tarkoittaa, että korttiaukkoon on asetettu voimassa oleva kuljettaja- tai korjaamokortti. NOT INSERTED tarkoittaa, että tilanne on päinvastainen, toisin sanoen korttiaukkoon ei ole asetettu voimassa olevaa kuljettaja- tai korjaamokorttia (esim. korttiaukkoon on asetettu yrityskortti tai siinä ei ole lainkaan korttia).

Huomautus: Kuljettajan käsin syöttämät toimintatiedot eivät tallennu datamuistiin.

085 Datamuistin on kyettävä tallentamaan kuljettajan toimintaan liittyviä tietoja vähintään 365 vuorokauden ajalta.

086 Kun tiedontallennuskapasiteetti loppuu, uusimpien tietojen on korvattava vanhimmat tiedot.

12.5 *Tiedot paikasta, jossa päivän työaika alkaa ja/tai päättyy*

087 Aina kun (apu)kuljettaja syöttää päivän työajan alkamis- ja/tai päättymispaikkaa koskevat tiedot, valvontalaitteen on tallennettava ja säilytettävä datamuistissaan:

- (apu)kuljettajan kortin numero ja kortin myöntänyt jäsenvaltio, jos tarpeen,
- päivämäärä ja aika, jolloin tiedot syötettiin (tai syötettyihin tietoihin liittyvä päivämäärä ja aika, jos tietojen syöttäminen tapahtui tietojen käsin syöttämistä koskevan menettelyn mukaisesti),
- syötetyn tiedon tyyppi (alkamis- tai päättymistieto, olosuhteet, joissa tieto on syötetty),
- valtio ja alue, jota syötetty tieto koskee,
- ajoneuvon matkamittarin lukema.

088 Datamuistin on kyettävä tallentamaan päivän työajan alkamis- ja/tai päättymispaikkaan liittyviä tietoja vähintään 365 vuorokauden ajalta (olettaen, että yksi kuljettaja syöttää kaksi tietuetta vuorokaudessa).

089 Kun tiedontallennuskapasiteetti loppuu, uusimpien tietojen on korvattava vanhimmat tiedot.

12.6 *Matkamittarin tiedot*

090 Valvontalaitteen on tallennettava datamuistiinsa ajoneuvon matkamittarin lukema ja sitä vastaava päivämäärä keskiyöllä jokaisena kalenterivuorokautena.

091 Datamuistin on kyettävä tallentamaan keskiyöllä otettuja matkamittarin lukemia vähintään 365 vuorokauden ajalta.

092 Kun tiedontallennuskapasiteetti loppuu, uusimpien tietojen on korvattava vanhimmat tiedot.

12.7 *Yksityiskohtaiset nopeustiedot*

093 Valvontalaitteen on tallennettava ja säilytettävä datamuistissaan ajoneuvon hetkellinen nopeus ja sitä vastaava päivämäärä ja aika kerran sekunnissa vähintään viimeisen 24 sellaisen tunnin ajalta, jolloin ajoneuvo on ollut liikkeessä.

12.8 *Tapauksia koskevat tiedot*

Tässä alakohdassa käsiteltäviin asioihin liittyvä aika on kirjattava yhden sekunnin tarkkuudella.

094 Valvontalaitteen on tallennettava ja säilytettävä datamuistissaan seuraavat tiedot kustakin havaitusta tapauksesta seuraavien tallennussääntöjen mukaisesti:

Tapaus	Tallennussäännöt	Kustakin tapauksesta kirjattavat tiedot
Korttiristiriita	— 10 viimeisintä tapausta	<ul style="list-style-type: none"> — tapauksen alkamispäivämäärä ja -aika, — tapauksen päättymispäivämäärä ja -aika, — kunkin ristiriidan aiheuttaneen kortin tyyppi, numero ja kortin myöntänyt jäsenvaltio
Ajo ilman asianmukaista korttia	<ul style="list-style-type: none"> — pisimpään kestänyt tapaus kultakin niistä 10 viimeisimmästä päivästä, jolloin tapauksia sattui, — viisi pisimpään kestänyttä tapausta viimeisten 365 vuorokauden ajalta 	<ul style="list-style-type: none"> — tapauksen alkamispäivämäärä ja -aika, — tapauksen päättymispäivämäärä ja -aika, — tapauksen alkaessa ja/tai päättyessä paikoilleen asetetun kortin tyyppi, numero ja kortin myöntänyt jäsenvaltio, — kyseisenä päivänä sattuneiden vastaavien tapausten lukumäärä
Kortin paikoilleen asettaminen ajon aikana	— viimeinen tapaus kultakin niistä 10 viimeisimmästä päivästä, jolloin tapauksia sattui	<ul style="list-style-type: none"> — tapauksen päivämäärä ja aika, — kortin tyyppi, numero ja kortin myöntänyt jäsenvaltio, — kyseisenä päivänä sattuneiden vastaavien tapausten lukumäärä
Edellistä kortin käyttöjaksoa ei lopetettu oikein	— 10 viimeisintä tapausta	<ul style="list-style-type: none"> — päivämäärä ja aika, jolloin kortti asetettiin paikoilleen, — kortin tyyppi, numero ja kortin myöntänyt jäsenvaltio, — viimeisimmän käyttöjakson tiedot sellaisina kuin ne on luettavissa kortilta: <ul style="list-style-type: none"> — päivämäärä ja aika, jolloin kortti asetettiin paikoilleen, — rekisteritunnus ja jäsenvaltio, jossa ajoneuvo on rekisteröity
Ylinopeus ⁽¹⁾	<ul style="list-style-type: none"> — räikein tapaus kultakin niistä 10 viimeisimmästä päivästä, jolloin tapauksia sattui (eli tapaus, johon liittyy korkein keskinopeus), — viisi räikeintä tapausta viimeisten 365 vuorokauden ajalta, — ensimmäinen tapaus, joka sattui viimeksi suoritettun kalibroinnin jälkeen 	<ul style="list-style-type: none"> — tapauksen alkamispäivämäärä ja -aika, — tapauksen päättymispäivämäärä ja -aika, — suurin tapauksen kestäessä mitattu nopeus, — tapauksen kestäessä mitattujen nopeuslukemien aritmeettinen keskiarvo, — kuljettajan kortin tyyppi, numero ja kortin myöntänyt jäsenvaltio (soveltuvin osin), — kyseisenä päivänä sattuneiden vastaavien tapausten lukumäärä

Tapaus	Tallennussäännöt	Kustakin tapauksesta kirjattavat tiedot
Keskeytynyt virransyöttö ⁽²⁾	<ul style="list-style-type: none"> — pisimpään kestänyt tapaus kultakin niistä 10 viimeisimmästä päivästä, jolloin tapauksia sattui, — viisi pisimpään kestänyttä tapausta viimeisten 365 vuorokauden ajalta 	<ul style="list-style-type: none"> — tapauksen alkamispäivämäärä ja -aika, — tapauksen päättymispäivämäärä ja -aika, — tapauksen alkaessa ja/tai päättyessä paikoilleen asetettujen korttien tyyppi, numero ja ne myöntänyt jäsenvaltio, — kyseisenä päivänä sattuneiden vastaavien tapausten lukumäärä
Virhe liikedatassa	<ul style="list-style-type: none"> — pisimpään kestänyt tapaus kultakin niistä 10 viimeisimmästä päivästä, jolloin tapauksia sattui, — viisi pisimpään kestänyttä tapausta viimeisten 365 vuorokauden ajalta 	<ul style="list-style-type: none"> — tapauksen alkamispäivämäärä ja -aika, — tapauksen päättymispäivämäärä ja -aika, — tapauksen alkaessa ja/tai päättyessä paikoilleen asetettujen korttien tyyppi, numero ja ne myöntänyt jäsenvaltio, — kyseisenä päivänä sattuneiden vastaavien tapausten lukumäärä
Tietoturvan murtoyritys	<ul style="list-style-type: none"> — 10 viimeisintä kutakin tyyppiä edustavaa tapausta 	<ul style="list-style-type: none"> — tapauksen alkamispäivämäärä ja -aika, — tapauksen päättymispäivämäärä ja -aika (jos tieto on oleellinen), — tapauksen alkaessa ja/tai päättyessä paikoilleen asetettujen korttien tyyppi, numero ja ne myöntänyt jäsenvaltio, — tapauksen tyyppi

095

⁽¹⁾ Valvontalaitteen on myös tallennettava ja säilytettävä datamuistissaan:

- viimeisimmän OVER SPEEDING CONTROL -toimenpiteen päivämäärä ja aika,
- ensimmäisen tätä OVER SPEEDING CONTROL -toimenpidettä seuraavan ylinopeustapauksen päivämäärä ja aika,
- viimeisimmän OVER SPEEDING CONTROL -toimenpiteen jälkeen sattuneiden ylinopeustapauksien lukumäärä.

⁽²⁾ Nämä tiedot voidaan tallentaa vasta, kun virransyöttö on kytketty uudelleen; ajat voidaan kirjata minuutin tarkkuudella.

12.9 Vikoihin liittyvät tiedot

Tässä alakohdassa käsiteltäviin asioihin liittyvä aika on kirjattava yhden sekunnin tarkkuudella.

096

Valvontalaitteen on yritettävä tallentaa ja säilyttää datamuistissaan seuraavat, kutakin havaittua vikaa koskevat tiedot seuraavien tallennussääntöjen mukaisesti:

Vikatapahtumat	Tallennussäännöt	Kustakin viasta kirjattavat tiedot
Korttivika	<ul style="list-style-type: none"> — 10 viimeisintä kuljettajakortin vikatapahtumaa 	<ul style="list-style-type: none"> — päivämäärä ja aika, jolloin vikatapahtuma alkoi, — päivämäärä ja aika, jolloin vikatapahtuma päättyi, — kortin tyyppi, numero ja kortin myöntänyt jäsenvaltio
Valvontalaitteivat	<ul style="list-style-type: none"> — 10 viimeisintä kutakin tyyppiä edustavaa vikatapahtumaa, — ensimmäinen vikatapahtuma, joka sattui viimeksi suoritettuna kalibroinnin jälkeen 	<ul style="list-style-type: none"> — päivämäärä ja aika, jolloin vikatapahtuma alkoi, — päivämäärä ja aika, jolloin vikatapahtuma päättyi, — vian tyyppi, — vikatapahtuman alkaessa ja/tai päättyessä paikoilleen asetettujen korttien tyyppi, numero ja ne myöntänyt jäsenvaltio

12.10 Kalibrointiin liittyvät tiedot

- 097 Valvontalaitteen on tallennettava ja säilytettävä datamuistissaan tiedot, jotka liittyvät:
- aktivointihetkellä tunnettuihin kalibrointiparametreihin,
 - laitteen ensimmäiseen kalibrointiin sen aktivoinnin jälkeen,
 - sen ensimmäiseen kalibrointiin nykyisessä ajoneuvossa (joka tunnustetaan rekisteritunnuksensa perusteella),
 - sen viiteen viimeiseen kalibrointiin (jos saman kalenterivuorokauden aikana suoritetaan useita kalibrointeja, ainoastaan viimeinen niistä tallennetaan).
- 098 Kaikista näistä kalibroinneista on tallennettava seuraavat tiedot:
- kalibroinnin tarkoitus (aktivointi, ensiasennus, asennus, määräaikaistarkastus)
 - kalibroinnin suorittaneen korjaamon nimi ja osoite,
 - korjaamokortin numero, kortin myöntänyt jäsenvaltio ja kortin viimeinen voimassaolopäivä,
 - ajoneuvon tunnistetiedot,
 - päivitetty tai vahvistettu parametrit: w, k, l, rengaskoko, nopeudenrajoittimen asetukset, matkamittari (vanhat ja uudet lukemat), päivämäärä ja aika (vanhat ja uudet lukemat).
- 099 Liiketunnistimen on tallennettava ja säilytettävä muistissaan seuraavat liiketunnistimen asennustiedot:
- sen ensimmäinen liittäminen ajoneuvoyksikköön (päivämäärä, aika, ajoneuvoyksikön hyväksyntänumero, ajoneuvoyksikön sarjanumero),
 - sen viimeisin liittäminen ajoneuvoyksikköön (päivämäärä, aika, ajoneuvoyksikön hyväksyntänumero, ajoneuvoyksikön sarjanumero).

12.11 Ajan asetukseen liittyvät tiedot

- 100 Valvontalaitteen on tallennettava ja säilytettävä datamuistissaan tiedot, jotka liittyvät:
- viimeisimpään ajan asetukseen,
 - niihin viimeisimmän kalibroinnin jälkeen tehtyihin viiteen ajan asetukseen, joissa aikaa on muutettu eniten ja jotka on tehty kalibrointitilassa tavanomaisen kalibroinnin (määritelmä f) ulkopuolella.
- 101 Kaikista näistä ajan asetuksista on tallennettava seuraavat tiedot:
- päivämäärä ja aika, vanhat lukemat,
 - päivämäärä ja aika, uudet lukemat,
 - ajan asetuksen suorittaneen korjaamon nimi ja osoite,
 - korjaamokortin numero, kortin myöntänyt jäsenvaltio ja kortin viimeinen voimassaolopäivä.

12.12 Tarkastustoiimiin liittyvät tiedot

- 102 Valvontalaitteen on tallennettava ja säilytettävä datamuistissaan seuraavat tiedot, jotka liittyvät 20 viimeisimpään tarkastustoimeen:
- päivämäärä ja aika, jolloin tarkastus suoritettiin,
 - valvontakortin numero ja kortin myöntänyt jäsenvaltio,
 - tarkastuksen tyyppi (tietojen näyttö ja/tai tulostus ja/tai ajoneuvoyksikön tietojen kopiointi ja/tai kortin tietojen kopiointi).

103 Kun tietoja kopioidaan, myös tiedot ensimmäisestä ja viimeisestä päivästä, joita kopiointi koskee, on kirjattava.

12.13 Yritysten tekemiin lukituksiin liittyvät tiedot

104 Valvontalaitteen on tallennettava ja säilytettävä datamuistissaan seuraavat tiedot, jotka liittyvät 20 viimeisimpään yrityksen tekemään lukitukseen:

- päivämäärä ja aika, jolloin lukitus tehtiin,
- päivämäärä ja aika, jolloin lukitus avattiin,
- yrityskortin numero ja kortin myöntänyt jäsenvaltio,
- yrityksen nimi ja osoite.

12.14 Tietojen kopiointiin liittyvät tiedot

105 Valvontalaitteen on tallennettava ja säilytettävä datamuistissaan seuraavat tiedot, jotka liittyvät datamuistin viimeisimpään kopiointiin ulkoiselle tietovälineelle laitteen ollessa yritys- tai kalibrointitilassa:

- päivämäärä ja aika, jolloin kopiointi suoritettiin,
- yritys- tai korjaamokortin numero ja kortin myöntänyt jäsenvaltio,
- yrityksen tai korjaamon nimi.

12.15 Erityisolosuhteisiin liittyvät tiedot

105a Valvontalaitteen on tallennettava datamuistiinsa seuraavat tiedot, jotka liittyvät erityisolosuhteisiin:

- syötetyn tiedon päivämäärä ja aika,
- erityisolosuhteiden tyyppi.

105b Datamuistin on kyettävä tallentamaan erityisolosuhteisiin liittyviä tietoja vähintään 365 vuorokauden ajalta (olettaen, että päivittäin alkaa ja päättyy keskimäärin yksi erityisolosuhtetilanne). Kun tiedontallennuskapasiteetti loppuu, uusimpien tietojen on korvattava vanhimmat tiedot.

13. Tietojen haku ajopiirturikorteilta

106 Valvontalaitteen on kyettävä tarvittaessa lukemaan ajopiirturikorteilta tiedot, joita tarvitaan, jotta voidaan:

- tunnistaa kortin tyyppi, kortin haltija, aiemmin käytetty ajoneuvo, päivämäärä ja aika, jolloin kortti viimeksi poistettiin, sekä tuolloin valittu toiminnan tyyppi,
- tarkastaa, että viimeisin kortin käyttöjakso lopetettiin oikein,
- laskea kuljettajan keskeytymätön ajoaika, yhteenlaskettu tauko-aika sekä edellisen ja kuluvan viikon yhteenlasketut ajoajat,
- tulostaa tarvittavia tulosteita, jotka liittyvät kuljettajakortille tallennettuihin tietoihin,
- kopioida kuljettajakortin tietoja ulkoiselle tietovälineelle.

107 Jos tietojen lukemisessa tapahtuu virhe, valvontalaitteen on yritettävä enintään kolme kertaa uudelleen käyttää samaa lukukomentoa, ja mikäli tietojen lukeminen ei vielä onnistu, laitteen on katsottava, että kortti on viallinen eikä se ole voimassa.

14. Tietojen kirjaaminen ja tallentaminen ajopiirturikorteille

108 Valvontalaitteen on kirjattava kortin tätä käyttöjaksoa koskevat tiedot kuljettaja- tai korjaamokortille heti, kun se on asetettu laitteeseen.

- 109 Valvontalaitteen on päivitettävä voimassa olevat kuljettaja-, kokeilu- ja/tai valvontakortit kaikilla niillä tarvittavilla tiedoilla, jotka liittyvät aikaan, jolloin kortti on asetettuna laitteeseen, sekä tiedoilla, jotka liittyvät kortin haltijaan. Näille kortteille tallennettavat tiedot on määritelty luvussa IV.
- 109a Valvontalaitteen on päivitettävä kuljettajan toimintaa ja olinpaikkaa koskevat tiedot (kuten luvun IV kohdissa 5.2.5 ja 5.2.6 on määritelty), jotka on tallennettu voimassa oleville kuljettaja- ja/tai korjaamokortteille, kortin haltijan käsin syötämällä toimintaa ja olinpaikkaa koskevilla tiedoilla.
- 110 Ajopiirturikorttien tietojen päivityksen on tapahduttava siten, että tarvittaessa ja tiedontallennuskapasiteetti huomioon ottaen uusimmat tiedot korvaavat vanhimmat tiedot.
- 111 Jos tietojen kirjoittamisessa kortille tapahtuu virhe, valvontalaitteen on yritettävä enintään kolme kertaa uudelleen käyttää samaa kirjoituskomentoa, ja mikäli tietojen kirjoittaminen ei vielääkään onnistu, laitteen on katsottava, että kortti on viallinen eikä se ole voimassa.
- 112 Ennen kuin valvontalaitteeseen sallii kuljettajakortin poistamisen ja sen jälkeen, kun kaikki oleelliset tiedot on tallennettu kortille, valvontalaitteen on saatettava nyt päättyvää kortin käyttöjaksoa koskevat tiedot ajan tasalle.

15. Tietojen näyttö

- 113 Näytön on oltava vähintään 20 merkin laajuinen.
- 114 Merkkien on oltava vähintään 5 mm korkeita ja 3,5 mm leveitä.
- 114a Näytön on tuettava ISO 8859 -standardin osissa 1 ja 7 määriteltyjä Latin1- ja Greek-merkistöjä, kuten lisäyksen 1 luvussa 4 'Merkistöt' on määritelty. Näytössä voidaan käyttää yksinkertaistettuja merkkikuvioita (esim. merkit, joissa on korkomerkkejä, voidaan näyttää ilman niitä, tai pienet kirjaimet voidaan näyttää isoina kirjaimina).
- 115 Näytössä on oltava asianmukainen ja häikäisemätön valaistus.
- 116 Näytön on oltava nähtävissä avaamatta valvontalaitetta.
- 117 Valvontalaitteen on kyettävä näyttämään:
- oletusarvoiset tiedot,
 - varoituksiin liittyvät tiedot,
 - valikkojen käyttöön liittyvät tiedot,
 - muut käyttäjän pyytämät tiedot.
- Valvontalaitteeseen saa näyttää muitakin tietoja, edellyttäen, että ne ovat selvästi erotettavissa edellä mainituista tiedoista.
- 118 Valvontalaitteen näytössä on käytettävä lisäyksessä 3 lueteltuja kuvakkeita tai niiden yhdistelmiä. Näytössä voidaan lisäksi käyttää muita kuvakkeita tai niiden yhdistelmiä, mikäli ne ovat selvästi erotettavissa edellä mainituista kuvakkeista tai niiden yhdistelmistä.
- 119 Näytön on aina oltava ON (päällä) -tilassa ajoneuvon ollessa liikkeessä.
- 120 Valvontalaitteessa saa olla käsikäyttöinen tai automaattinen mahdollisuus kytkeä näyttö OFF (pois) -tilaan silloin, kun ajoneuvo ei ole liikkeessä.
- Näytön esitysmuoto on määritelty lisäyksessä 5.

15.1 Oletusarvoinen näyttö

- 121 Kun ei ole tarvetta näyttää muita tietoja, valvontalaitteen on oletusarvoisesti näytettävä seuraavat tiedot:
- paikallinen aika (UTC-ajan ja kuljettajan asettaman aikaeron perusteella),
 - laitteen toimintatila,
 - kuljettajan ja apukuljettajan sen hetkisen toiminnan tyyppi,

- kuljettajaan liittyvät tiedot:
 - jos kuljettajan sen hetkinen toiminta on tyyppiä DRIVING, näytetään kuljettajan sen hetkinen keskeytymätön ajoaika ja sen hetkinen yhteenlaskettu tauko-aika,
 - jos kuljettajan sen hetkinen toiminta ei ole tyyppiä DRIVING, näytetään kyseisen toiminnan sen hetkinen kesto (alkaen hetkestä, jolloin se valittiin) ja kuljettajan sen hetkinen yhteenlaskettu tauko-aika,
 - apukuljettajaan liittyvät tiedot:
 - apukuljettajan toiminnan sen hetkinen kesto (alkaen hetkestä, jolloin se valittiin).
- 122 Kuhunkin kuljettajaan liittyvien tietojen näytön on oltava selkeä, pelkistetty ja yksiselitteinen. Jos kuljettajaan ja apukuljettajaan liittyviä tietoja ei voida näyttää samanaikaisesti, valvontalaitteen on oletusarvoisesti näytettävä kuljettajaan liittyvät tiedot ja sallittava se, että käyttäjä itse tuo näyttöön apukuljettajaan liittyvät tiedot.
- 123 Jos laitteen toimintatila ei voida oletusarvoisesti näyttää näytön leveyden asettamien rajoitusten vuoksi, on valvontalaitteen näytettävä uusi toimintatila hetken ajan tilan vaihtuessa.
- 124 Valvontalaitteen on näytettävä kortin haltijan nimi hetken ajan korttia paikoilleen asetettaessa.
- 124a Kun OUT OF SCOPE -olosuhteet ovat voimassa, näytössä on oletusarvoisesti oltava asianomainen kuvake, joka osoittaa, että kyseiset olosuhteet ovat voimassa (kuljettajan sen hetkisen toiminnan tyyppiä ei tarvitse näyttää samaan aikaan).

15.2 Varoitusten näyttö

- 125 Valvontalaitteen on näytettävä varoitukset ensisijaisesti käyttäen lisäyksen 3 kuvakkeita täydennettynä tarvittaessa numerokodein välitettävillä lisätiedoilla. Varoituksen selväkielinen kuvaus kuljettajan valitsemalla kielellä voidaan myös lisätä toimintoon.

15.3 Valikkojen käyttö

- 126 Valvontalaitteessa on oltava asianmukaisen valikkorakenteen avulla käytettävät tarvittavat komennot.

15.4 Muut näytöt

- 127 Haluttaessa on voitava valita seuraavien tietojen näyttö:
- UTC-päivämäärä ja -aika,
 - laitteen toimintatila (ellei se sisälly oletusarvoiseen näyttöön),
 - kuljettajan keskeytymätön ajoaika ja yhteenlaskettu tauko-aika,
 - apukuljettajan keskeytymätön ajoaika ja yhteenlaskettu tauko-aika,
 - kuljettajan edellisen ja kuluvan viikon yhteenlasketut ajoajat,
 - apukuljettajan edellisen ja kuluvan viikon yhteenlasketut ajoajat,
 - kuuden eri vakiotulosteen sisältö samassa muodossa kuin itse tulosteet.
- 128 Tulosteen sisällön näyttämisen on tapahduttava jaksoittaisesti, rivi kerrallaan. Jos näytön leveys on alle 24 merkkiä, käyttäjän on saatava tiedot täydellisinä käyttäen sopivaa keinoa (tiedon näyttäminen useammalla rivillä, rivien vierittäminen...). Käsin tehtäviä merkintöjä varten varattuja tulosteiden rivejä ei tarvitse näyttää.

16. Tulostaminen

- 129 Valvontalaitteen on kyettävä tulostamaan datamuistissaan ja/tai ajopiirturikorteilla olevia tietoja seuraavien tulosteiden muodossa:
- kuljettajan toiminta kortin tietojen mukaan päivittäin tulostettuna,
 - kuljettajan toiminta ajoneuvoyksikön tietojen mukaan päivittäin tulostettuna,

- tapaukset ja viat kortin tietojen mukaan tulostettuna,
- tapaukset ja viat ajoneuvoyksikön tietojen mukaan tulostettuna,
- teknisten tietojen tuloste,
- ylinopeustuloste.

Näiden tulosteiden ulkoasu ja sisältö on määritelty lisäyksessä 4.

Tulosteiden lopussa voidaan antaa lisätietoja.

Valvontalaite voi tuottaa myös muita tulosteita, jos ne ovat selvästi erotettavissa kuudesta edellä mainitusta tulosteesta.

- 130 Tulosteiden 'kuljettajan toiminta kortin tietojen mukaan päivittäin tulostettuna' ja 'tapaukset ja viat kortin tietojen mukaan tulostettuna' on oltava saatavissa vain, kun valvontalaitteeseen on asetettu kuljettaja- tai korjaamokortti. Valvontalaitteen on päivitettävä kyseiselle kortille tallennetut tiedot ennen tulostusta.
- 131 Tulosteiden 'kuljettajan toiminta kortin tietojen mukaan päivittäin tulostettuna' ja 'tapaukset ja viat kortin tietojen mukaan tulostettuna' tulostamiseksi valvontalaitteen on:
- joko automaattisesti valittava kuljettajakortti tai korjaamokortti, jos vain toinen näistä on asetettu laitteeseen,
 - tai annettava käyttäjän käyttöön komento, jolla tämä voi valita kortin, jolta tiedot luetaan, tai kortin, joka on asetettu kuljettajan korttiaukkoon, jos laitteeseen on asetettu kaksi korttia.
- 132 Tulostimen on kyettävä tulostamaan 24 merkkiä riville.
- 133 Merkkien on oltava vähintään 2,1 mm korkeita ja 1,5 mm leveitä.
- 133a Tulostimen on tuettava ISO 8859 -standardin osissa 1 ja 7 määriteltyjä Latin 1- ja Greek-merkistöjä, kuten lisäyksen 1 luvussa 4 'Merkistöt' on määritelty.
- 134 Tulostimien on oltava suunniteltu siten, että ne kykenevät tuottamaan edellä mainitut tulosteet riittävän selvinä, jottei niitä luettaessa synny väärinkäsityksiä.
- 135 Tulosteiden koon ja niiden sisältämien tietojen on säilyttävä muuttumattomina normaaleissa kosteus- (10–90 %) ja lämpötilaolosuhteissa.
- 136 Valvontalaitteessa käytettävä tulostuspaperi on varustettava asianmukaisin tyyppihyväksyntämerkinnöin sekä merkinnöin siitä, minkä tyyppisessä (tyyppisissä) valvontalaitteessa (-laitteissa) sitä saadaan käyttää. Tulosteiden on säilyttävä selvästi luettavina ja tunnistettavina senkin jälkeen, kun niitä on säilytetty vähintään vuoden ajan valaistuksen, kosteuden ja lämpötilan osalta normaaleissa olosuhteissa.
- 137 Näihin asiakirjoihin on myös voitava tehdä käsin kirjoitettuja merkintöjä kuten kuljettajan allekirjoitus.
- 138 Valvontalaitteen on hallittava tilanteet, joissa tulostuspaperi loppuu, siten, että uuden paperin lisäämisen jälkeen laite joko aloittaa tulostuksen alusta tai jatkaa tulostusta antamalla yksiselitteisen viitteen ennen paperin loppumista tulostettuun osaan.
- 17. Varoitukset**
- 139 Valvontalaitteen on varoitettava kuljettajaa, jos se havaitsee tapauksen ja/tai vian.
- 140 Virransyötön keskeytymistapausta koskeva varoitus voidaan antaa virransyötön uudelleenkytkemisen jälkeen.
- 141 Valvontalaitteen on varoitettava kuljettajaa 15 minuuttia ennen 4 tunnin 30 minuutin keskeytymättömän ajoajan ylitystä sekä ylityksen tapahtumishetkellä.
- 142 Varoitusten on oltava näkyviä. Näkyvien varoitusten lisäksi voidaan antaa kuultavia varoituksia.

- 143 Käyttäjän on kyettävä selvästi tunnistamaan näkyvät varoitukset, niiden on oltava kuljettajan näkökentässä ja selvästi luettavissa sekä päivällä että yöllä.
- 144 Näkyviä varoituksia voidaan lisätä valvontalaitteeseen ja/tai järjestää erilleen siitä.
- 145 Jälkimmäisessä tapauksessa varoituksessa on oltava merkki 'T' ja varoituksen on oltava väriltään keltainen tai oranssi.
- 146 Varoitusten on kestävä vähintään 30 sekuntia, ellei käyttäjä kuittaa niitä painamalla jotakin valvontalaitteen näppäintä. Tämä pikakuittaus ei tyhjennä varoituksen syyn kertovaa näyttöä, johon viitataan seuraavassa kappaleessa.
- 147 Varoituksen syyn on näyttävä valvontalaitteen näytössä, kunnes käyttäjä kuittaa sen tietyllä valvontalaitteen näppäimellä tai komennolla.
- 148 Muita varoituksia voidaan antaa, jos ne eivät aiheuta kuljettajille sekaannusta edellä mainittujen varoitusten suhteen.

18. Tietojen kopioiminen ulkoisille tietovälineille

- 149 Valvontalaitteen on kyettävä tarvittaessa kopioimaan tietoja datamuististaan tai kuljettajakortilta ulkoisille tallennusvälineille kalibrointi-/kopiointiliittimen kautta. Valvontalaitteen on päivitettävä kyseiselle kortille tallennetut tiedot ennen tulostusta.
- 150 Lisäksi valvontalaitteessa voi olla lisäominaisuus, jonka avulla se voi missä hyvänsä toimintatilassa kopioida tietoja jonkin muun liittimen kautta yritykselle, jonka tunnistetiedot on varmennettu tämän väylän kautta. Tällaisessa tapauksessa kopioinnille pätevät yritystilaa vastaavat käyttöoikeudet.
- 151 Kopiointi ei saa muuttaa tai pyyhkiä tallennettuja tietoja.

Kalibrointi-/kopiointiliittimen sähköiset liityntätiedot on määritelty lisäyksessä 6.

Kopiointiprotokollat on määritelty lisäyksessä 7.

19. Tietojen tulostaminen muille ulkoisille välineille

- 152 Jos valvontalaitteessa ei ole nopeuden ja/tai matkan näyttötoimintoja, laitteen on annettava lähtösignaali(-t), jonka (joiden) avulla voidaan näyttää ajoneuvon nopeus (nopeusmittari) ja/tai sen kulkema kokonaismatka (matkamittari).
- 153 Ajoneuvoyksikön on myös kyettävä tulostamaan seuraavat tiedot käyttäen asianmukaista tarkoitukseen varattua sarjaliitännästä, joka on riippumaton valinnaisesta CAN-väyläliitännästä (ISO 11898 -standardi, joka koskee maantieajoneuvoja, digitaalisen tiedon siirtoa ja CAN-verkkoja tiedon siirtämiseksi suurella nopeudella), jotta muut ajoneuvon asennetut elektroniset yksiköt voivat käsitellä niitä:

- kuluva UTC-päivämäärä ja -aika,
- ajoneuvon nopeus,
- ajoneuvon kulkema kokonaismatka (matkamittari),
- kuljettajan ja apukuljettajan sen hetkinen toiminta,
- tieto siitä, onko kuljettajan ja apukuljettajan korttiaukkoon asetettu ajopiirturikorttia, sekä (tarvittaessa) näiden korttien tunnistetiedot (kortin numero ja kortin myöntänyt jäsenvaltio).

Näiden vähimmäisvaatimusten lisäksi voidaan tulostaa myös muita tietoja.

Kun ajoneuvon syytysvirtakytkin on ON-asennossa, laitteen on tulostettava näitä tietoja jatkuvasti sarjaliitännästä. Kun ajoneuvon syytysvirtakytkin on OFF-asennossa, ainakin kuljettajan ja/tai apukuljettajan toiminnan tilan muuttumisen ja/tai ajopiirturikortin paikalleen asettamisen tai poistamisen on saatava aikaan vastaavien tietojen tulostuminen sarjaliitännästä. Jos tietojen tulostumista on lykätty siksi aikaa, kun ajoneuvon syytysvirtakytkin on OFF-asennossa, tietojen on oltava käytettävissä, kun ajoneuvon syytysvirtakytkin on jälleen ON-asennossa.

20. Kalibrointi

- 154 Kalibrointitoiminnon avulla on voitava:
- automaattisesti liittää liiketunnistin ajoneuvoyksikköön,
 - digitaalisesti sovittaa valvontalaitteen vakio (k) ajoneuvon ominaiskertoimeen (w) (ajoneuvoihin, joissa on kaksi tai useampia vetopyörästä välityssuhteita, on asennettava katkaisin, jonka avulla nämä erilaiset välityssuhteet saadaan automaattisesti vastaamaan sitä välityssuhdetta, jota käyttäen valvontalaite on sovitettu ajoneuvoon),
 - asettaa (ilman rajoituksia) kuluva aika,
 - asettaa matkamittarin kuluva lukema,
 - päivittää datamuistiin tallennetut liiketunnistimen tunnistetiedot,
 - päivittää tai vahvistaa muita valvontalaitteen tiedossa olevia parametreja, joita ovat: ajoneuvon tunnistetiedot, w-kerroin, l-mitta, rengaskoko ja nopeudenrajoittimen asetukset, jos sellainen on.
- 155 Liiketunnistimen ajoneuvoyksikköön liittämiseen on sisällyttävä ainakin:
- liiketunnistimeen tallennettujen liiketunnistimen asennustietojen päivitys (tarvittaessa),
 - tarvittavien liiketunnistimen tunnistetietojen kopiointi tunnistimelta ajoneuvoyksikön datamuistiin.
- 156 Kalibrointitoiminnon avulla on kyettävä automaattisesti syöttämään tarvittavat tiedot kalibrointi-/kopiointiliittimen kautta lisäyksessä 8 määriteltyä kalibrointiprotokollaa käyttäen. Kalibrointitoiminnon avulla voidaan syöttää myös muita tarvittavia tietoja muiden liittimien kautta.

21. Ajan asetus

- 157 Ajan asetustoiminnon avulla on kyettävä asettamaan kuluva aika enintään yhden minuutin välein ja vähintään seitsemän päivän väliajoin.
- 158 Ajan asetustoiminnon avulla on kyettävä asettamaan kuluva aika ilman rajoituksia laitteen ollessa kalibrointitilassa.

22. Laitteen toimintaominaisuudet

- 159 Ajoneuvoyksikön on säilyttävä täysin toimintakuntoisena lämpötila-alueella -20 °C – 70 °C ja liiketunnistimen lämpötila-alueella -40 °C – 135 °C . Datamuistin tietojen on säilyttävä -40 °C lämpötilaan asti.
- 160 Valvontalaitteen on säilyttävä täysin toimintakuntoisena kosteuden ollessa 10–90 %.
- 161 Valvontalaitteen on oltava suojattu ylijännitettä, väärää napaisuutta ja oikosulkuja vastaan.
- 162 Valvontalaitteen on oltava sähkömagneettista yhteensopivuutta koskevan neuvoston direktiivin 72/245/ETY⁽¹⁾ mukauttamisesta tekniikan kehitykseen annetun komission direktiivin 95/54/EY⁽²⁾ mukainen, sekä suojattu staattisen sähkön aiheuttamilta purkauksilta ja jännitepiikeiltä.

23. Materiaalit

- 163 Kaikkien valvontalaitteen osien on oltava valmistettuja materiaaleista, joilla on riittävä kestävyys ja mekaaninen lujuus sekä muuttumattomat sähköiset ja magneettiset ominaisuudet.
- 164 Normaalien käyttöolosuhteiden vuoksi kaikki laitteen sisäpuoliset osat on suojattava kosteudelta ja pölyltä.
- 165 Ajoneuvoyksikön on täytettävä IEC 529 -standardin mukaiset suojausluokan IP 40 vaatimukset ja liiketunnistimen on täytettävä IEC 529 -standardin mukaiset suojausluokan IP 64 vaatimukset.

⁽¹⁾ EYVL L 152, 6.7.1972, s. 15.

⁽²⁾ EYVL L 266, 8.11.1995, s. 1.

- 166 Valvontalaitteen on täytettävä siihen soveltuviin ergonomiseen muotoiluun liittyvien määräysten vaatimukset.
- 167 Valvontalaite on suojattava mahdollisilta vahingoilta.

24. Merkinnät

- 168 Jos valvontalaite näyttää ajoneuvon matkamittarilukeman ja nopeuden, on sen näytössä oltava seuraavat merkinnät:
- matkan mittayksikkö, jota osoittaa km-lyhenne matkaa osoittavan lukeman lähellä,
 - merkintä 'km/h' nopeutta osoittavan lukeman lähellä.
- Valvontalaite voidaan myös kytkeä osoittamaan nopeutta mailleina tunnissa, jolloin nopeuden mittayksikkö on näytetty lyhenteellä 'mph'.
- 169 Jokaiseen valvontalaitteen erilliseen osaan on kiinnitettävä tunnustekilpi, josta ilmenevät seuraavat tiedot:
- laitteen valmistajan nimi ja osoite,
 - valmistajan osanumero sekä laitteen valmistusvuosi,
 - laitteen sarjanumero,
 - laitteen tyyppihyväksyntätunnus.
- 170 Jos tila ei riitä kaikkien edellä mainittujen tietojen näyttämiseen, tunnustekilvestä on ilmettävä ainakin valmistajan nimi tai liiketunnus sekä laitteen osanumero.

IV AJOPIIRTURIKORTTIEN RAKENNETTA JA TOIMINTOJA KOSKEVAT VAATIMUKSET

1. Näkyvissä olevat tiedot

Etupuolella on:

- 171 kortin tyyppin mukaan sana 'kuljettajakortti' tai 'valvontakortti' tai 'korjaamokortti' tai 'yrityskortti' painettuna suurikokoisin kirjaimin kortin myöntävän jäsenvaltion virallisella kielellä tai kielillä;
- 172 sama sana yhteisön muilla virallisilla kielillä painettuna siten, että ne muodostavat kortin taustan:

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

- 173 kortin myöntävän jäsenvaltion nimi (vapaaehtoinen);

174 kortin myöntävän jäsenvaltion kansainvälinen tunnus negatiivina sinisessä suorakulmiossa ja kahdentoista keltaisen tähden ympäröimänä. Jäsenvaltioiden kansainväliset tunnukset ovat seuraavat:

B	Belgia
DK	Tanska
D	Saksa
GR	Kreikka
E	Espanja
F	Ranska
IRL	Irlanti
I	Italia
L	Luxemburg
NL	Alankomaat
A	Itävalta
P	Portugali
FIN	Suomi
S	Ruotsi
UK	Yhdistynyt kuningaskunta

175 myönnettyä korttia koskevat seuraavasti numeroidut tiedot:

	Kuljettajakortti	Valvontakortti	Yritys- tai korjaamokortti
1.	kuljettajan sukunimi	Valvontaelimen nimi	yrityksen tai korjaamon nimi
2.	kuljettajan etunimi (etunimet)	Valvojan sukunimi (jos nimetty)	kortin haltijan sukunimi (jos nimetty)
3.	kuljettajan syntymäaika	Valvojan etunimi (etunimet) (jos nimetty)	kortin haltijan etunimi (etunimet) (jos nimetty)
4.(a)	kortin ensimmäinen voimassaolopäivä		
(b)	kortin viimeinen voimassaolopäivä (jos sellaista on)		
(c)	kortin myöntävä viranomainen (voidaan painaa kortin kääntöpuolelle)		
(d)	hallinnollinen numero, joka on muu kuin kohdassa 5 ilmoitettu numero (vapaaehtoinen)		
5.(a)	ajokortin numero (kuljettajakortin myöntämispäivänä)		
5.(b)	kortin numero		
6.	kuljettajan valokuva	Valvojan valokuva (vapaaehtoinen)	—
7.	kuljettajan allekirjoitus	haltijan allekirjoitus (vapaaehtoinen)	
8.	haltijan vakainainen asuinpaikka tai postiosoite (vapaaehtoinen)	Valvontaelimen postiosoite	yrityksen tai korjaamon postiosoite





176 päivämäärät on kirjoitettava käyttäen muotoa 'pp/kk/vvvv' tai 'pp.kk.vvvv' (päivä, kuukausi, vuosi).

Kääntöpuolella on:

177 kortin etupuolella olevien numeroitujen kohtien selitykset;

178 haltijan nimenomaisella kirjallisella suostumuksella lisättyjä, muita kuin korttia koskevia hallinnollisia tietoja; tämänkaltaisten tietojen lisääminen ei millään tavoin vaikuta mallin käyttämiseen ajopiirturikorttina.

YHTEISÖN MALLIN MUKAISET AJOPIIRTURIKORTIT

<i>ETUPUOLI</i>	<i>KÄÄNTÖPUOLI</i>
<div style="text-align: center;"></div> <p>KULJETTAJAKORTTI JÄSENVALTIO TARJETA DEL CONDUCTOR FÖRERFÖRT 1. FÖRERFÖRT 2. FAHREKARTE 3. KAPTA 1 ET 07 4a. 4b. DRIVER CARD 4c. CARTE DE CONDUCTEUR (4d.) CARTA TIOMANAI 5a. CARTA DEL CONDUCENTE 5b. BESTUURDESKAART 7. CARTÃO DE CONDUTOR (8.) KULJETTAJAKORTTI FÖRARKORT</p>	<p>1. Sukunimi 2. Etunimi (etunimet) 3. Syntymäaika 4a. Kortin ensimmäinen voimassaolopäivä 4b. Kortin hallinnollinen viimeinen voimassaolopäivä 4c. Kortin myöntävä viranomainen (4d.) Kansallinen hallinnollinen numero 5a. Ajokortin numero 5b. Kortin numero 6. Valokuva 7. Allekirjoitus (8) Osoite</p> <p style="text-align: center;"><i>Kortti pyydetään palauttamaan osoitteeseen:</i></p> <div style="border: 1px solid black; padding: 2px; text-align: center;">VIRANOMAISEN NIMI JA OSOITE</div>
<div style="text-align: center;"></div> <p>VALVONTAKORTTI JÄSENVALTIO 1. TARJETA DE CONTROL (2.) KONTROLLKORT (3.) KONTROLLKARTE 4a. 4b.) KAPTA 1 ET 07 4c. CONTROL CARD (4d.) CARTE DE CONTROLLEUR 5b. CARTA STURTHA (7.) CARTA DI CONTROLLO 8. CONTROLLEKAART CARTÃO DE CONTROLLO VALVONTAKORTTI KONTROLLKORT</p>	<p>1. Valvontaelin 2. Sukunimi 3. Etunimi (etunimet) 4a. Kortin ensimmäinen voimassaolopäivä (4b.) Kortin hallinnollinen viimeinen voimassaolopäivä 4c. Kortin myöntävä viranomainen (4d.) Kansallinen hallinnollinen numero 5b. Kortin numero 6. Valokuva 7. Allekirjoitus (8) Osoite</p> <p style="text-align: center;"><i>Kortti pyydetään palauttamaan osoitteeseen:</i></p> <div style="border: 1px solid black; padding: 2px; text-align: center;">VIRANOMAISEN NIMI JA OSOITE</div>
<div style="text-align: center;"></div> <p>KORJAAMOKORTTI JÄSENVALTIO 1. TARJETA DEL CENTRO DE ENSAIO (2.) VÆRKSTEDSKORT (3.) WERKSTÄTTKARTE 4a. 4b.) KAPTA 1 ET 07 4c. WORKSHOP CARD (4d.) CARTE D'ATELIER 5b. CARTA CEARDLAINNE (7.) CARTA DELL'OFFICINA 8. WERKPLAATSKAART CARTÃO DO CENTRO DE ENSAIO TESTAUSASEMAKORTTI VÆRKSTADSKORT</p>	<p>1. Korjaamon nimi 2. Sukunimi 3. Etunimi (etunimet) 4a. Kortin ensimmäinen voimassaolopäivä 4b. Kortin hallinnollinen viimeinen voimassaolopäivä 4c. Kortin myöntävä viranomainen (4d.) Kansallinen hallinnollinen numero 5b. Kortin numero 7. Allekirjoitus (8) Osoite</p> <p style="text-align: center;"><i>Kortti pyydetään palauttamaan osoitteeseen:</i></p> <div style="border: 1px solid black; padding: 2px; text-align: center;">VIRANOMAISEN NIMI JA OSOITE</div>
<div style="text-align: center;"></div> <p>YRITYSKORTTI JÄSENVALTIO 1. TARJETA DE LA EMPRESA (2.) VIRKSOMHEDSKORT (3.) UNTERNEHMENSKARTE 4a. 4b.) KAPTA 1 ET 07 4c. COMPANY CARD (4d.) CARTE D'ENTREPRISE 5b. CARTA DELL'AZIENDA (7.) BEDRIJFSKAART 8. CARTÃO DE EMPRESA YRITYSKORTTI FÖRETAGSKORT</p>	<p>1. Yrityksen nimi 2. Sukunimi 3. Etunimi (etunimet) 4a. Kortin ensimmäinen voimassaolopäivä 4b. Kortin hallinnollinen viimeinen voimassaolopäivä 4c. Kortin myöntävä viranomainen (4d.) Kansallinen hallinnollinen numero 5b. Kortin numero 7. Allekirjoitus (8) Osoite</p> <p style="text-align: center;"><i>Kortti pyydetään palauttamaan osoitteeseen:</i></p> <div style="border: 1px solid black; padding: 2px; text-align: center;">VIRANOMAISEN NIMI JA OSOITE</div>

179 Ajopiirturikortit on painettava käyttäen seuraavia hallitsevia taustavärejä:

- kuljettajakortti: valkoinen,
- valvontakortti: sininen,
- korjaamokortti: punainen,
- yrityskortti: keltainen.

180 Ajopiirturikorteilla on oltava ainakin seuraavat ominaisuudet, jotka suojaavat sitä väärentämiseltä ja vilpilliseltä käytöltä:

- turvakuviointi, jossa on ohut aaltomainen viivakuvioiden ja iirisävyjen,
- valokuvan kohdalla on taustan turvakuvioinnin ja valokuvan mentävä osittain päällekkäin,
- ainakin yksi kaksiväristä mikrokirjoitusta sisältävä rivi.

- 181 Jäsenvaltiot voivat komissiota kuultuaan lisätä korttiin värejä tai merkintöjä, kuten kansallisia tunnuksia ja turvallisuutta lisääviä ominaisuuksia, tämän kuitenkaan rajoittamatta tämän liitteen muita määräyksiä.

2. Tietoturva

Järjestelmän turvallisuuden tavoitteena on suojata korttien ja valvontalaitteen välillä siirrettävien tietojen eheys ja autenttisuus, suojata korteilta kopioitavien tietojen eheys ja autenttisuus, sallia valvontalaitteiden siirtää vain tiettyjä tietoja korteille, tehdä korteille tallennetun tiedon väärentäminen mahdottomaksi, estää vilpallinen käsittely sekä havaita kaikki sen tapaiset yritykset.

- 182 Järjestelmän turvallisuuden saavuttamiseksi ajopiirturikorttien on täytettävä tietoturva-vaatimukset, jotka on määritelty lisäyksessä 10 'Yleiset tietoturvatavoitteet'.

- 183 Ajopiirturikorttien on oltava luettavissa muilla laitteilla, kuten henkilökohtaisilla tietokoneilla.

3. Standardit

- 184 Ajopiirturikorttien on oltava seuraavien standardien mukaisia:

- ISO/IEC 7810 Identification cards — Physical characteristics (henkilökortit/toimikortit — fyysiset ominaisuudet),
- ISO/IEC 7816 Identification cards — Integrated circuits with contacts (henkilökortit/toimikortit — liittimillä varustetut integroidut piirit):
 - osa 1: Physical characteristics (fyysiset ominaisuudet),
 - osa 2: Dimensions and location of the contacts (mitat ja liittimien paikat),
 - osa 3: Electronic signals and transmission protocols (sähköiset signaalit ja siirtoprotokollat),
 - osa 4: Inter-industry commands for interchange (yleiset siirtokomennot),
 - osa 8: Security related inter-industry commands (yleiset turvakomennot),
- ISO/IEC 10373 Identification cards — Test methods (henkilökortit/toimikortit — testausmenetelmät),

4. Ympäristöön liittyvät ja sähkötekniset eritelmät

- 185 Ajopiirturikorttien on kyettävä toimimaan moitteettomasti kaikissa yhteisön alueella tavattavissa ilmasto-olosuhteissa sekä vähintään lämpötila-alueella -25 °C – $+70\text{ °C}$, jolloin satunnaiset lämpötilahuiput voivat olla jopa $+85\text{ °C}$, missä satunnainen tarkoittaa enintään neljän tunnin jaksoja kerrallaan enintään sata kertaa kortin käyttöä aikana.

- 186 Ajopiirturikorttien on voitava toimia moitteettomasti kosteuden ollessa 10–90 %.

- 187 Ajopiirturikorttien on voitava toimia moitteettomasti viiden vuoden ajan, jos niitä käytetään ympäristöön liittyvien ja sähkötekniikan eritelmien rajoissa.

- 188 Käytön aikana ajopiirturikortin on oltava sähkömagneettisesta yhteensopivuudesta annetun direktiivin 95/54/EY mukainen sekä suojattu staattisen sähkö aiheuttamilta purkauksilta.

5. Tietojen tallennus

Tässä kohdassa käsiteltävien asioiden osalta,

- ajat kirjataan yhden minuutin tarkkuudella, ellei toisin ole määrätty,
- matkamittarin lukemat kirjataan yhden kilometrin tarkkuudella,
- nopeudet kirjataan tarkkuudella 1 km/t.

Tietojen tallennuksen vaatimukset täyttävät ajopiirturikorttien toiminnot, komennot ja loogiset rakenteet on määritelty lisäyksessä 2.

- 189 Tässä kohdassa määritellään erilaisia sovellustiedostoja koskevat tiedontallennuskapasiteetin vähimmäisvaatimukset. Ajopiirturikorttien on kyettävä antamaan valvontalaitteelle tieto näiden tiedostojen vaatimasta todellisesta tallennuskapasiteetista.

Muut ajopiirturikorteille mahdollisesti tallennettavat, muihin kortilla mahdollisesti oleviin sovelluksiin liittyvät tiedot on tallennettava direktiivin 95/46/EY mukaisesti.

5.1 **Kortin tunniste- ja turvatiedot**

5.1.1 *Sovellusten tunnistetiedot*

- 190 Ajopiirturikorttien on kyettävä tallentamaan seuraavat sovellusten tunnistetiedot:

- ajopiirturisovelluksen tunniste,
- ajopiirturikortin tunnisteen tyyppi.

5.1.2 *Mikrosirujen tunnistetiedot*

- 191 Ajopiirturikorttien on kyettävä tallentamaan seuraavat integroitujen piirien tunnistetiedot:

- integroidun piirin sarjanumero,
- integroidun piirin valmistajan viitetiedot.

5.1.3 *Srukorttien tunnistetiedot*

- 192 Ajopiirturikorttien on kyettävä tallentamaan seuraavat älykorttien tunnistetiedot:

- kortin sarjanumero (mukaan lukijan valmistajan viitetiedot),
- kortin tyyppihyväksyntänumero,
- kortin yksilöivä tunniste,
- kortin laminoijan tunniste,
- integroidun piirin tunniste.

5.1.4 *Tietoturvan osatekijät*

- 193 Ajopiirturikorttien on kyettävä tallentamaan seuraavat tietoturvan osatekijöihin liittyvät tiedot:

- eurooppalainen julkinen avain,
- jäsenvaltion myöntämä todistus,
- kortille myönnetty todistus,
- kortin yksityinen avain.

5.2 **Kuljettajakortti**

5.2.1 *Kortin tunnistetiedot*

- 194 Kuljettajakortin on kyettävä tallentamaan seuraavat kortin tunnistetiedot:

- kortin numero,
- kortin myöntänyt jäsenvaltio, myöntäneen viranomaisen nimi, myöntämispäivä,
- kortin ensimmäinen voimassaolopäivä, kortin viimeinen voimassaolopäivä.

5.2.2 Kortin haltijan tunnistetiedot

195 Kuljettajakortin on kyettävä tallentamaan seuraavat kortin haltijan tunnistetiedot:

- haltijan sukunimi,
- haltijan etunimi (etunimet),
- syntymäaika,
- haltijan ensisijaisesti käyttämä kieli.

5.2.3 Ajokorttiin liittyvät tiedot

196 Kuljettajakortin on kyettävä tallentamaan seuraavat ajokorttiin liittyvät tiedot:

- kortin myöntänyt jäsenvaltio, myöntäneen viranomaisen nimi,
- ajokortin numero (myöntämispäivänä).

5.2.4 Käytössä olleisiin ajoneuvoihin liittyvät tiedot

197 Kuljettajakortin on kyettävä tallentamaan seuraavat tiedot erikseen jokaista sellaista kalenterivuorokautta kohti, jolloin korttia on käytetty, ja erikseen jokaista tietyn ajoneuvon kyseisenä päivänä tapahtunutta käyttöjaksoa kohti (käyttöjaksoon sisältyvät kaikki peräkkäin tapahtuneet työjaksot kortin paikoilleen asettamisesta sen poistoon kyseisessä ajoneuvossa, kortin kannalta tarkasteltuna):

- päivämäärä ja aika, jolloin ajoneuvoa ensi kerran käytettiin (eli hetki, jolloin kortti ensimmäisen kerran asetettiin paikoilleen kyseisen ajoneuvon käyttöjakson aikana, tai klo 00.00, jos ajoneuvon käyttö tuolloin oli jatkuvaa),
- ajoneuvon matkamittarin lukema tuona ajanhetkenä,
- päivämäärä ja aika, jolloin ajoneuvoa viimeisen kerran käytettiin (eli hetki, jolloin kortti viimeisen kerran poistettiin kyseisen ajoneuvon käyttöjakson aikana, tai klo 23.59, jos ajoneuvon käyttö tuolloin oli jatkuvaa),
- ajoneuvon matkamittarin lukema tuona ajanhetkenä,
- ajoneuvon rekisteritunnus ja jäsenvaltio, jossa ajoneuvo on rekisteröity.

198 Kuljettajakortin on kyettävä tallentamaan vähintään 84 tällaista tietuetta.

5.2.5 Kuljettajan toimintaan liittyvät tiedot

199 Kuljettajakortin on kyettävä tallentamaan seuraavat tiedot erikseen jokaista sellaista kalenterivuorokautta kohti, jolloin korttia on käytetty tai joille kuljettaja on syöttänyt tietoja käsin:

- päivämäärä,
- käyttövuorokausien juokseva järjestysnumero (jota suurennetaan yhdellä jokaisena sellaisena kalenterivuorokautena, jolloin korttia käytetään),
- kuljettajan kyseisen vuorokauden aikana kulkema kokonaismatka,
- kuljettajatilanne klo 00.00,
- seuraavat tiedot aina, kun kuljettajan toiminnan tila muuttuu ja/tai ajoneuvon miehitys muuttuu ja/tai kuljettajakortti asetetaan paikoilleen tai poistetaan:
 - ajoneuvon miehityksen tila (CREW, SINGLE),
 - käytetty korttipaikka (DRIVER, CO-DRIVER),
 - kortin tila (INSERTED, NOT INSERTED),
 - toiminta (DRIVING, AVAILABILITY, WORK, BREAK/REST),
 - aika, jolloin muutos tapahtui.

200 Kuljettajakortin muistin on kyettävä tallentamaan kuljettajan toimintaan liittyviä tietoja vähintään 28 vuorokauden ajalta (kuljettajan keskimääräisen toiminnan määritellään sisältävän 93 toiminnan tilan muutosta vuorokaudessa).

201 Vaatimusten 197 ja 199 kohdalla luetellut tiedot on tallennettava siten, että toimintaa koskevat tiedot voidaan hakea siinä järjestyksessä, jossa nämä toiminnot ovat tapahtuneet, vaikka aikatiedoissa olisikin päällekkäisyyttä.

5.2.6 Tiedot paikasta, jossa päivän työaika alkaa ja/tai päättyy

202 Kuljettajakortin on kyettävä tallentamaan seuraavat kuljettajan syöttämät tiedot paikasta, jossa päivän työaika alkaa ja/tai päättyy:

- päivämäärä ja aika, jolloin tiedot syötettiin (tai syötettyihin tietoihin liittyvä päivämäärä ja aika, jos tietojen syöttäminen tapahtui tietojen käsin syöttämistä koskevan menettelyn mukaisesti),
- syötetyn tiedon tyyppi (alkamis- tai päättymistieto, olosuhteet, joissa tieto on syötetty),
- valtio ja alue, jota syötetty tieto koskee,
- ajoneuvon matkamittarin lukema.

203 Kuljettajakortin muistin on kyettävä tallentamaan vähintään 42 paria tällaisia tietueita.

5.2.7 Tapauksiin liittyvät tiedot

Tässä alakohdassa käsiteltäviin asioihin liittyvä aika on kirjattava yhden sekunnin tarkkuudella.

204 Kuljettajakortin on kyettävä tallentamaan tiedot, jotka liittyvät seuraaviin tapauksiin, jotka valvontalaite on havainnut kortin ollessa paikoilleen asetettuna:

- aikojen päällekkäisyys (jos tapaus on tämän kortin aiheuttama),
- kortin paikoilleen asettaminen ajettaessa (jos tämä kortti on tapauksen kohteena),
- edellistä kortin käyttöjaksoa ei lopetettu oikein (jos tämä kortti on tapauksen kohteena),
- keskeytynyt virransyöttö,
- virhe liikedatassa,
- tietoturvan murtoyritykset.

205 Kuljettajakortin on kyettävä tallentamaan seuraavat näihin tapauksiin liittyvät tiedot:

- tapauksen tunnuskoodi,
- päivämäärä ja aika, jolloin tapaus alkoi (tai päivämäärä ja aika, jolloin kortti asetettiin paikoilleen, jos tapaus oli tuolloin jo alkanut),
- päivämäärä ja aika, jolloin tapaus päättyi (tai päivämäärä ja aika, jolloin kortti poistettiin, jos tapaus oli tuolloin vielä käynnissä),
- tapaukseen liittyvän ajoneuvon rekisteritunnus ja jäsenvaltio, jossa ajoneuvo on rekisteröity.

Huomautus: 'aikojen päällekkäisyys' -tapauksen osalta:

- tapauksen alkamispäivämäärän ja -ajan on vastattava sitä päivämäärää ja aikaa, jolloin kortti poistettiin edellisestä ajoneuvosta,
- tapauksen päättymispäivämäärän ja -ajan on vastattava sitä päivämäärää ja aikaa, jolloin kortti asetettiin paikoilleen nyt käytössä olevaan ajoneuvoon,
- ajoneuvoon liittyvien tietojen on vastattava nyt käytössä olevaa, tapauksen aiheuttanutta ajoneuvoa.

Huomautus: 'edellistä kortin käyttöjaksoa ei lopetettu oikein' -tapauksen osalta:

- tapauksen alkamispäivämäärän ja -ajan on vastattava sitä päivämäärää ja aikaa, jolloin kortti asetettiin paikoilleen sen käyttöjakson aluksi, jota ei lopetettu oikein,
- tapauksen päättymispäivämäärän ja -ajan on vastattava sitä päivämäärää ja aikaa, jolloin kortti asetettiin paikoilleen sen käyttöjakson aluksi, jonka aikana tapaus havaittiin (kuluva käyttöjakso),
- ajoneuvoon liittyvien tietojen on vastattava sitä ajoneuvoa, jota käytettäessä kortin käyttöjaksoa ei lopetettu oikein.

206 Kuljettajakortin on kyettävä tallentamaan kuuteen viimeisimpään kutakin tapaustyyppiä edustavaan tapaukseen liittyvät tiedot (eli 36 tapauksen tiedot).

5.2.8 *Vikoihin liittyvät tiedot*

Tässä alakohdassa käsiteltäviin asioihin liittyvä aika on kirjattava yhden sekunnin tarkkuudella.

207 Kuljettajakortin on kyettävä tallentamaan tiedot, jotka liittyvät seuraaviin vikoihin, jotka valvontalaite on havainnut kortin ollessa paikoilleen asetettuna:

- korttivika (jos tämä kortti on tapauksen kohteena),
- valvontalaitteen vika.

208 Kuljettajakortin on kyettävä tallentamaan seuraavat näihin vikoihin liittyvät tiedot:

- vian tunnuskoodi,
- päivämäärä ja aika, jolloin vikatapahtuma alkoi (tai päivämäärä ja aika, jolloin kortti asetettiin paikoilleen, jos vikatapahtuma oli tuolloin jo alkanut),
- päivämäärä ja aika, jolloin vikatapahtuma päättyi (tai päivämäärä ja aika, jolloin kortti poistettiin, jos vikatapahtuma oli tuolloin vielä käynnissä),
- vikatapahtumaan liittyvän ajoneuvon rekisteritunnus ja jäsenvaltio, jossa ajoneuvo on rekisteröity.

209 Kuljettajakortin on kyettävä tallentamaan kahteentoista viimeisimpään kutakin vikatyyppiä edustavaan vikatapahtumaan liittyvät tiedot (eli 24 vikatapahtuman tiedot).

5.2.9 *Tarkastustoimiin liittyvät tiedot*

210 Kuljettajakortin on kyettävä tallentamaan seuraavat tarkastustoimiin liittyvät tiedot:

- tarkastuksen päivämäärä ja aika,
- tarkastuskortin numero ja kortin myöntänyt jäsenvaltio,
- tarkastuksen tyyppi (tietojen näyttö ja/tai tulostus ja/tai ajoneuvoyksikön tietojen kopiointi ja/tai kortin tietojen kopiointi (ks. huomautus)),
- jakso, jota koskevat tiedot kopioitiin, kun kyseessä on tietojen kopiointi,
- tarkastettavan ajoneuvon rekisteritunnus ja jäsenvaltio, jossa ajoneuvo on rekisteröity.

Huomautus: tietoturva vaatimusten vuoksi tietojen kopiointi kirjataan vain, jos se on suoritettu valvontalaitteen kautta.

211 Kuljettajakortin on kyettävä tallentamaan yksi tällainen tietue.

5.2.10 *Kortin käyttöjaksoon liittyvät tiedot*

212 Kuljettajakortin on kyettävä tallentamaan tiedot, jotka liittyvät ajoneuvoon, jota käytettäessä kuluva käyttöjakso alkoi:

- päivämäärä ja aika, jolloin käyttöjakso alkoi (eli kortti asetettiin paikoilleen) yhden sekunnin tarkkuudella,
- ajoneuvon rekisteritunnus, ja jäsenvaltio, jossa ajoneuvo on rekisteröity.

5.2.11 *Erityisolosuhteisiin liittyvät tiedot*

212a Kuljettajakortin on kyettävä tallentamaan seuraavat erityisolosuhteisiin liittyvät tiedot, jotka on syötetty kortin ollessa paikoilleen asetettuna (mihin hyvänsä korttiaukkoon):

- päivämäärä ja aika, jolloin tieto syötettiin,
- erityisolosuhteiden tyyppi.

- 212b Kuljettajakortin on kyettävä tallentamaan 56 tällaista tietuetta.
- 5.3 Korjaamokortti**
- 5.3.1 *Tietoturvan osatekijät*
- 213 Korjaamokortin on kyettävä tallentamaan henkilökohtainen tunnusluku (PIN-koodi).
- 214 Korjaamokortin on kyettävä tallentamaan ne salakirjoitusavaimet, joita tarvitaan liittämään liiketunnistimet ajoneuvoyksikköihin.
- 5.3.2 *Kortin tunnistetiedot*
- 215 Korjaamokortin on kyettävä tallentamaan seuraavat kortin tunnistetiedot:
- kortin numero,
 - kortin myöntänyt jäsenvaltio, myöntäneen viranomaisen nimi, myöntämispäivä,
 - kortin ensimmäinen voimassaolopäivä, kortin viimeinen voimassaolopäivä.
- 5.3.3 *Kortin haltijan tunnistetiedot*
- 216 Korjaamokortin on kyettävä tallentamaan seuraavat kortin haltijan tunnistetiedot:
- korjaamon nimi,
 - korjaamon osoite,
 - haltijan sukunimi,
 - haltijan etunimi (etunimet),
 - haltijan ensisijaisesti käyttämä kieli.
- 5.3.4 *Käytössä olleisiin ajoneuvoihin liittyvät tiedot*
- 217 Korjaamokortin on kyettävä tallentamaan käytössä olleisiin ajoneuvoihin liittyvät tiedot samalla tavoin kuin kuljettajakortin.
- 218 Korjaamokortin on kyettävä tallentamaan vähintään neljä tällaista tietuetta.
- 5.3.5 *Kuljettajan toimintaan liittyvät tiedot*
- 219 Korjaamokortin on kyettävä tallentamaan kuljettajan toimintaan liittyvät tiedot samalla tavoin kuin kuljettajakortin.
- 220 Korjaamokortin on kyettävä tallentamaan vähintään yhden kuljettajan keskimääräistä toimintaa vastaavan päivän tiedot.
- 5.3.6 *Päivän työajan alkamiseen ja/tai päättymiseen liittyvät tiedot*
- 221 Korjaamokortin on kyettävä tallentamaan päivän työajan alkamiseen ja/tai päättymiseen liittyvät tiedot samalla tavoin kuin kuljettajakortin.
- 222 Korjaamokortin on kyettävä tallentamaan vähintään kolme paria tällaisia tietueita.
- 5.3.7 *Tapauksiin ja vikoihin liittyvät tiedot*
- 223 Korjaamokortin on kyettävä tallentamaan tapauksiin ja vikoihin liittyvät tiedot samalla tavoin kuin kuljettajakortin.
- 224 Korjaamokortin on kyettävä tallentamaan tiedot, jotka koskevat kolmea viimeisintä kutakin tapaustyyppiä edustavaa tapausta (eli 18 tapausta) ja kuutta viimeisintä kutakin vikatyyppiä edustavaa vikatapahtumaa (eli 12 vikatapahtumaa).
- 5.3.8 *Tarkastustoimiin liittyvät tiedot*
- 225 Korjaamokortin on kyettävä tallentamaan tarkastustoimiin liittyvät tiedot samalla tavoin kuin kuljettajakortin.

5.3.9 Kalibrointiin ja ajan asetukseen liittyvät tiedot

- 226 Korjaamokortin on kyettävä tallentamaan tiedot, jotka liittyvät kalibrointeihin ja/tai ajan asetuksiin, jotka on suoritettu kortin ollessa asetettuna valvontalaitteeseen.
- 227 Kunkin kalibrointiin liittyvän tietueen on kyettävä tallentamaan seuraavat tiedot:
- kalibroinnin tarkoitus (ensiasennus, asennus, määräaikaistarkastus),
 - ajoneuvon tunnistetiedot,
 - päivitetty tai vahvistetut parametrit (w, k, l, rengaskoko, nopeudenrajoittimen asetukset, matkamittari (uudet ja vanhat lukemat), päivämäärä ja aika (uudet ja vanhat lukemat)),
 - valvontalaitteen tunnistetiedot (ajoneuvoyksikön osanumero, ajoneuvoyksikön sarjanumero, liiketunnistimen sarjanumero).
- 228 Korjaamokortin on kyettävä tallentamaan vähintään 88 tällaista tietuetta.
- 229 Korjaamokortin on pidettävä muistissa sen avulla suoritettujen kalibrointien kokonaislukumäärä.
- 230 Korjaamokortin on pidettävä muistissa sen avulla suoritettujen kalibrointien lukumäärä kortin tietojen viimeksi tapahtuneen kopioinnin jälkeen.

5.3.10 Erityisolosuhteisiin liittyvät tiedot

- 230a Korjaamokortin on kyettävä tallentamaan erityisolosuhteisiin liittyvät tiedot samalla tavoin kuin kuljettajakortin. Korjaamokortin on kyettävä tallentamaan kaksi tällaista tietuetta.

5.4 Valvontakortti

5.4.1 Kortin tunnistetiedot

- 231 Valvontakortin on kyettävä tallentamaan seuraavat kortin tunnistetiedot:
- kortin numero,
 - kortin myöntänyt jäsenvaltio, myöntäneen viranomaisen nimi, myöntämispäivä,
 - kortin ensimmäinen voimassaolopäivä, kortin viimeinen voimassaolopäivä (jos sellainen on)

5.4.2 Kortin haltijan tunnistetiedot

- 232 Valvontakortin on kyettävä tallentamaan seuraavat kortin haltijan tunnistetiedot:
- tarkastuselimen nimi,
 - tarkastuselimen osoite,
 - haltijan sukunimi,
 - haltijan etunimi (etunimet),
 - haltijan ensisijaisesti käyttämä kieli.

5.4.3 Tarkastustoimiin liittyvät tiedot

- 233 Valvontakortin on kyettävä tallentamaan seuraavat tarkastustoimiin liittyvät tiedot:
- tarkastuksen päivämäärä ja aika,
 - tarkastuksen tyyppi (tietojen näyttö ja/tai tulostus ja/tai ajoneuvoyksikön tietojen kopiointi ja/tai kortin tietojen kopiointi),

- jakso, jota koskevat tiedot kopioitiin (jos niitä kopioitiin),
 - tarkastettavan ajoneuvon rekisteritunnus ja jäsenvaltion viranomainen, joka on rekisteröinyt tarkastettavan ajoneuvon,
 - tarkastettavan kuljettajakortin numero ja kortin myöntänyt jäsenvaltio.
- 234 Valvontakortin on kyettävä tallentamaan vähintään 230 tällaista tietuetta.
- 5.5 Yrityskortti**
- 5.5.1 *Kortin tunnistetiedot*
- 235 Yrityskortin on kyettävä tallentamaan seuraavat kortin tunnistetiedot:
- kortin numero,
 - kortin myöntänyt jäsenvaltio, myöntäneen viranomaisen nimi, myöntämispäivä,
 - kortin ensimmäinen voimassaolopäivä, kortin viimeinen voimassaolopäivä (jos sellainen on).
- 5.5.2 *Kortin haltijan tunnistetiedot*
- 236 Yrityskortin on kyettävä tallentamaan seuraavat kortin haltijan tunnistetiedot:
- yrityksen nimi,
 - yrityksen osoite.
- 5.5.3 *Yrityksen toimenpiteitä koskevat tiedot*
- 237 Yrityskortin on kyettävä tallentamaan seuraavat yrityksen toimenpiteitä koskevat tiedot:
- päivämäärä ja aika, jolloin toimenpide suoritettiin,
 - toimenpiteen tyyppi (ajoneuvoyksikön lukitseminen ja/tai lukituksen avaaminen ja/tai ajoneuvoyksikön tietojen kopiointi ja/tai kortin tietojen kopiointi),
 - jakso, jota koskevat tiedot kopioitiin (jos niitä kopioitiin),
 - kyseisen ajoneuvon rekisteritunnus ja jäsenvaltion viranomainen, joka on rekisteröinyt kyseisen ajoneuvon,
 - kortin numero ja kortin myöntänyt jäsenvaltio (jos kortin tietoja kopioitiin).
- 238 Yrityskortin on kyettävä tallentamaan vähintään 230 tällaista tietuetta.

V VALVONTALAITTEEN ASENNUS

1. Asennus

- 239 Uudet valvontalaitteet on toimitettava asentajille tai ajoneuvovalmistajille aktivoimattomana ja siten, että kaikille III luvun kohdassa 20 luetelluille kalibrointiparametreille on asetettu asianmukaiset ja käyvät oletusarvot. Tapauksissa, joissa mikään oletusarvo ei ole asianmukainen, kirjaimin ilmaistavien parametrien arvo on asetettava kysymysmerkeistä muodostuviksi merkkijonoiksi ja numeeristen parametrien arvo nollassi.
- 240 Valvontalaite on ennen sen aktivointia pystyttävä kalibroimaan, vaikka laite ei olisikaan kalibrointitilassa.
- 241 Valvontalaite ei saa ennen aktivoimistaan kirjata tai tallentaa tietoja, jotka on kuvattu III luvun kohdissa 12.3–12.9 ja 12.12–12.14 (mainitut kohdat mukaan lukien).
- 242 Asennuksen aikana ajoneuvovalmistajien on asetettava valmiiksi kaikki tiedossa olevat parametrit.

- 243 Ajoneuvovalmistajien tai asentajien on aktivoitava asennettu valvontalaite ennen kuin ajoneuvo siirretään pois toimitiloista, joissa asennus suoritettiin.
- 244 Valvontalaitteen aktivoinnin on käynnistytävä automaattisesti, kun sen jompaan kumpaan korttiliitälaitteeseen ensimmäisen kerran asetetaan korjaamokortti.
- 245 Mikäli liiketunnistimen ja ajoneuvoyksikön toisiinsa liittäminen vaatii erityisiä toimintoja, niiden on tapahduttava automaattisesti ennen aktivointia tai sen aikana.
- 246 Aktivoinnin tapahduttua valvontalaitteen toimintojen ja tietojen käyttöoikeuksien on oltava täysin käytettävissä.
- 247 Valvontalaitteen tietojen kirjaamis- ja tallennustoimintojen on laitteen aktivoinnin jälkeen oltava täysin toimintakuntoiset.
- 248 Asennuksen jälkeen laite on kalibroitava. Ajoneuvon rekisteritunnus syötetään ensimmäisen kalibroinnin yhteydessä, kahden viikon kuluessa asennuksesta tai viimeistään silloin, kun rekisteritunnus on myönnetty.
- 248a Valvontalaite on sijoitettava ajoneuvoon siten, että kuljettaja kykenee käyttämään tarvittavia toimintoja istuimeltaan käsin.

2. Asennuskilpi

- 249 Sen jälkeen, kun valvontalaite on tarkastettu asennuksen yhteydessä, on sen päälle, sisälle tai viereen helppopääsyiseen paikkaan kiinnitettävä selvästi näkyvä asennuskilpi. Jokaisen hyväksytyt asentajan tai korjaamon suorittaman tarkastuksen jälkeen on edellisen paikalle kiinnitettävä uusi kilpi.
- 250 Kilvestä on käytävä ilmi ainakin seuraavat tiedot:
- hyväksytyt asentajan tai korjaamon nimi, osoite tai toiminimi,
 - ajoneuvon ominaiskerroin muodossa 'w = ... imp/km',
 - valvontalaitteen vakio muodossa 'k = ... imp/km',
 - pyörien renkaiden tehollinen ympärysmitta muodossa 'l = ... mm',
 - rengaskoko,
 - päivämäärä, jolloin ajoneuvon ominaiskerroin ja pyörien renkaiden tehollinen ympärysmitta on mitattu,
 - ajoneuvon valmistenumero.

3. Sinetöinti

- 251 Seuraavat osat on sinetöitävä:
- jokainen liitântä, joka irrotessaan aiheuttaisi muutoksia, joita on mahdoton havaita, tai tietojen tuhoutumista, jota on mahdoton havaita;
 - asennuskilpi, jollei sitä ole kiinnitetty siten, ettei sitä voi poistaa siinä olevien merkintöjen tuhoutumatta.
- 252 Edellä mainitut sinetit voidaan poistaa:
- hätätapauksessa,
 - nopeudenrajoittimen tai muun liikenneturvallisuuksia parantavan laitteen asentamiseksi, säätämiseksi tai korjaamiseksi edellyttäen, että valvontalaitteen toiminta jatkuu luotettavasti ja moitteettomasti ja että hyväksytty asentaja tai korjaamo sinetöi sen uudelleen (VI luvun mukaisesti) välittömästi nopeudenrajoittimen tai muun liikenneturvallisuuksia parantavan laitteen asentamisen jälkeen tai seitsemän päivän kuluessa muissa tapauksissa.

- 253 Aina kun sinetit poistetaan, toimivaltaiselle viranomaiselle on laadittava ja toimitettava kirjallinen ilmoitus, jossa esitetään toimenpiteen syyt.

VI TARKASTUKSET, MÄÄRÄAIKAISTARKASTUKSET JA KORJAUKSET

Niitä olosuhteita koskevat vaatimukset, joissa sinetit saadaan poistaa ja joihin viitataan asetuksen (ETY) N:o 3821/85 12 artiklan 5 kohdassa, sellaisena kuin se on viimeksi muutettuna asetuksella (EY) N:o 2135/98, on määritelty tämän liitteen V luvun kohdassa 3.

1. Asentajien tai testausasemien hyväksyminen

Jäsenvaltiot hyväksyvät, tarkastavat säännöllisesti ja laillistavat elimet, jotka saavat suorittaa:

- asennuksia,
- tarkistuksia,
- tarkastuksia,
- korjauksia.

Tämän asetuksen 12 artiklan 1 kohdan mukaisesti korjaamokortteja myönnetään vain asentajille ja/tai testausasemille, jotka on hyväksytty suorittamaan valvontalaitteen aktivointi ja/tai kalibrointi tämän liitteen mukaisesti ja (paitsi milloin tästä poikkeamiseen on perusteltu syy):

- jotka eivät ole oikeutettuja yrityskorttiin;
- ja joiden muut työtehtävät eivät vaaranna lisäyksessä 10 määriteltyä järjestelmän kokonaistietoturva.

2. Uusien tai korjattujen laitteiden tarkastaminen

- 254 Jokaisen uuden tai korjatun laitteen moitteeton toiminta ja sen lukemien ja tallennusten tarkkuus suhteessa III luvun kohdissa 2.1 ja 2.2 annettuihin rajoihin on tarkastettava V luvun kohdan 3 mukaisen sinetöinnin ja kalibroinnin avulla.

3. Asennuksen tarkastus

- 255 Ajoneuvon asentamisen jälkeen koko laitteiston (valvontalaite mukaan lukien) on oltava III luvun kohdissa 2.1 ja 2.2 esitettyjen enimmäisvirherajoihin liittyvien määräysten mukainen.

4. Määräaikaistarkastukset

- 256 Ajoneuvoihin asennettujen laitteiden määräaikaistarkastukset on suoritettava laitteiden korjaamisen jälkeen tai ajoneuvon ominaiskertoimen tai pyörän renkaiden tehollisen ympärysmittan muutoksen jälkeen tai silloin, jos laitteen UTC-aika poikkeaa oikeasta enemmän kuin 20 minuuttia tai kun ajoneuvon rekisteritunnus on muuttunut, tai vähintään kerran kahden vuoden (24 kuukauden) kuluessa edellisestä tarkastuksesta.

- 257 Näissä tarkastuksissa on tarkastettava ainakin:

- että valvontalaite, mukaan lukien tiedon säilytys ajopiirturikortilla, toimii moitteettomasti,
- että III luvun kohdissa 2.1 ja 2.2 esitettyjä enimmäisvirherajoihin liittyviä määräyksiä noudatetaan,
- että valvontalaitteessa on tyyppihyväksyntämerkintä,
- että asennuskilpi on kiinnitettynä,
- että laitteen ja muiden laitteiston osien sinetit ovat koskemattomat,
- rengaskoko ja pyörien renkaiden todellinen ympärysmitta.

258 Kalibrointi on suoritettava osana näitä tarkastuksia.

5. Virheiden mittaaminen

259 Virheiden mittaaminen asennuksen yhteydessä tai käytön aikana on suoritettava seuraavissa olosuhteissa, joiden on katsottava olevan standardinmukaiset testausolosuhteet:

- ajoneuvo kuormaamattomana ja normaalissa ajokunnossa,
- rengaspaine valmistajan ohjeiden mukainen,
- renkaiden kuluminen kansallisen lainsäädännön sallimissa rajoissa,
- ajoneuvon liikkuminen:
 - ajoneuvon on kuljettava oman moottorinsa teholla suoraan tasaisella alustalla nopeudella 50 ± 5 km/t. Mittausmatkan on oltava ainakin 1 000 m.
- testaus voidaan suorittaa myös muilla menetelmillä, kuten tarkoitukseen soveltuva testipenkissä, edellyttäen, että siten saavutetaan vastaava tarkkuus.

6. Korjaukset

260 Testausasemien on kyettävä kopioimaan tietoja valvontalaitteesta tarkoituksenaan toimittaa tiedot takaisin kuljetusyhtiölle.

261 Hyväksytyjen testausasemien on annettava kuljetusyhtiöille todistus tietojen kopioinnin mahdottomuudesta tapauksissa, joissa valvontalaite ei salli aiemmin tallennettujen tietojen kopioimista tällaisen testausaseman suorittaman korjauksen jälkeenkään. Tällaiset korjaukset säilyttävät jäljennöksen antamistaan todistuksista vähintään vuoden ajan.

VII KORTTIEN MYÖNTÄMINEN

Jäsenvaltioiden käyttöön ottamien korttien myöntämiseen liittyvien menettelyjen on oltava seuraavien säännösten mukaisia:

- 262 Ensimmäisen hakijalle myönnetyn ajopiirturikortin haltijakohtaisen sarjanumeron (jos sellainen on), korvausnumeron ja uusintanumeron on oltava asetettu nolllaksi (0).
- 263 Kaikkien tietylle valvontaelimelle tai tietylle korjaamolle tai tietylle kuljetusyhtiölle myönnettyjen muiden kuin henkilökohtaisten ajopiirturikorttien numeroissa on oltava samat 13 ensimmäistä merkkiä ja niillä on oltava eri järjestysnumero.
- 264 Entisen ajopiirturikortin tilalle annetulla ajopiirturikortilla on oltava sama numero kuin kortilla, jonka se korvaa, lukuun ottamatta korvausnumeroa, jota suurennetaan yhdellä (järjestyksessä 0, ..., 9, A, ..., Z).
- 265 Entisen ajopiirturikortin tilalle annetulla ajopiirturikortilla on oltava sama viimeinen voimassaolopäivä kuin kortilla, jonka se korvaa.
- 266 Uusittavan ajopiirturikortin tilalle annetulla ajopiirturikortilla on oltava sama numero kuin kortilla, jonka se korvaa, lukuun ottamatta korvausnumeroa, joka on asetettava nolllaksi (0), ja uusintanumeroa, jota suurennetaan yhdellä (järjestyksessä 0, ..., 9, A, ..., Z).
- 267 Ajopiirturikortin vaihtamisessa hallinnollisten tietojen muuttamiseksi noudatetaan kortin uusimista koskevia sääntöjä, jos vaihtaminen tapahtuu samassa jäsenvaltiossa, ja kortin ensi kertaa myöntämistä koskevia sääntöjä, jos vaihtaminen tapahtuu jossakin muussa jäsenvaltiossa.
- 268 Muiden kuin henkilökohtaisten korjaamo- tai valvontakorttien kohtaan 'kortin haltijan sukunimi' on merkittävä korjauksen tai valvontaelimen nimi.

VIII VALVONTALAITTEIDEN JA AJOPIIRTURIKORTTIEN TYYPIHYVÄKSYNTÄ

1. Yleisiä asioita

Tässä luvussa valvontalaitteella tarkoitetaan valvontalaitetta tai sen osia. Kaapeli(t), jo(i)lla liiketunnistin yhdistetään ajoneuvoyksikköön, ei(vät) tarvitse tyyppihyväksyntää. Valvontalaitteen käyttämä paperi katsotaan valvontalaitteen osaksi.

- 269 Valvontalaite on tyyppihyväksytettävä täydellisenä kaikkien siihen kiinteästi liitettyjen lisälaitteiden kanssa.
- 270 Valvontalaitteiden ja ajopiirturikorttien tyyppihyväksyntään on sisällyttävä tietoturvaan liittyviä testejä, toimintaan liittyviä testejä ja yhteentoimivuuteen liittyviä testejä. Kunkin testityypin hyväksytyt tulokset esitetään asianmukaisessa todistuksessa.
- 271 Jäsenvaltioiden tyyppihyväksyntäviranomaiset eivät myönnä tyyppihyväksyntää tämän asetuksen 5 artiklan mukaisesti, ellei heillä ole käytettävissään sen valvontalaitteen tai ajopiirturikortin:
- tietoturvatodistusta,
 - toiminnallisuustodistusta
 - sekä yhteentoimivuustodistusta,
- jolle tyyppihyväksyntää anotaan.
- 272 Kaikista laitteiden ohjelmistojen tai varusteiden taikka niiden valmistuksessa käytettävien materiaalien muutoksista on ennen niiden käyttöönottoa ilmoitettava tyyppihyväksynnän myöntäneelle viranomaiselle. Tämän viranomaisen on joko vahvistettava valmistajalle, että tyyppihyväksyntä ulotetaan käsittämään nämä muutokset, tai vaadittava asianomaisten toiminnallisuus-, tietoturva- ja/tai yhteentoimivuustodistusten ajan tasalle saattamista tai vahvistamista.
- 273 Toimenpiteet, joilla päivitetään käytössä olevien valvontalaitteiden ohjelmistoja, on hyväksytettävä sillä viranomaisella, joka on myöntänyt valvontalaitteen tyyppihyväksynnän. Ohjelmiston päivitys ei saa muuttaa tai pyyhkiä pois mitään valvontalaitteeseen tallennettuja kuljettajan toimintaa koskevia tietoja. Ohjelmistoja voidaan päivittää vain laitteen valmistajan vastuulla.

2. Tietoturvatodistus

- 274 Tietoturvatodistus annetaan tämän liitteen lisäyksen 10 määräysten mukaisesti.

3. Toiminnallisuustodistus

- 275 Jokaisen tyyppihyväksyntää hakevan on annettava jäsenvaltion tyyppihyväksyntäviranomaisen käyttöön kaikki aineisto ja asiakirjat, jotka kyseinen viranomainen katsoo tarpeelliseksi.
- 276 Toiminnallisuustodistus annetaan valmistajalle vasta, kun vähintään kaikista lisäyksessä 9 määritellyistä testeistä on saatu hyväksyttävä tulos.
- 277 Toiminnallisuustodistuksen antaa tyyppihyväksyntäviranomainen. Todistukseen on sen saajan nimen ja mallin tunnistetietojen lisäksi sisällyttävä yksityiskohtainen luettelo suoritetuista testeistä ja saaduista tuloksista.

4. Yhteentoimivuustodistus

- 278 Yhteentoimivuustestit suoritetaan yhdessä laboratoriossa Euroopan komission valtuuttamana ja vastuulla.
- 279 Laboratorion on kirjattava valmistajien esittämät yhteentoimivuutta koskevat testauspyynnöt siinä aikajärjestyksessä, kun ne saapuvat.
- 280 Pyyntö kirjataan virallisesti vain, jos laboratoriolle on käytettävissään:
- kaikki kyseisten yhteentoimivuustestien suorittamisessa tarvittava aineisto ja asiakirjat,
 - vastaava tietoturvatodistus,
 - vastaava toiminnallisuustodistus.
- Pyyntö kirjataan kirjainpäivämäärä on ilmoitettava valmistajalle.

- 281 Laboratorio ei suorita yhteentoimivuustestejä valvontalaitteille tai ajopiirturikorteille, joille ei ole myönnetty tietoturvatodistusta ja toiminnallisuustodistusta.

- 282 Valmistajan, joka pyytää yhteentoimivuustestien suorittamista, on sitouduttava antamaan laboratorion vastata näistä testeistä sekä kaikesta aineistosta ja asiakirjoista, jotka valmistaja on testien suorittamiseksi antanut laboratorion käyttöön.

- 283 Yhteentoimivuustestit on suoritettava tämän liitteen lisäyksen 9 kohdan 5 mukaisesti kaikkien niiden valvontalaite- tai ajopiirturikorjattyyppien kanssa:
- joiden tyyppihyväksyntä on vielä voimassa tai,
 - joiden tyyppihyväksyntää on haettu ja joilla on voimassa oleva yhteentoimivuustodistus.
- 284 Laboratorio antaa valmistajalle yhteentoimivuustodistuksen vasta, kun kaikista yhteentoimivuustesteistä on saatu hyväksyttävät tulokset.
- 285 Jos yhteentoimivuustestit eivät anna hyväksyttäviä tuloksia yhden tai useamman valvontalaitteen tai ajopiirturikortin osalta vaatimuksen 283 mukaisesti, yhteentoimivuustodistusta ei anneta, ennen kuin sitä pyytänyt valmistaja on tehnyt tarvittavat muutokset ja saanut yhteentoimivuustesteissä hyväksyttävät tulokset. Laboratorion on määritettävä ongelman syy tähän yhteentoimivuusongelmaan liittyvien valmistajien avulla ja pyrittävä auttamaan todistusta pyytäneitä valmistajaa teknisen ratkaisun löytämisessä. Kun valmistaja tekee tuotteeseensa muutoksia, hänen itsensä on varmistettava asiaankuuluvilta viranomaisilta, että tietoturva- ja toiminnallisuustodistukset ovat vielä voimassa.
- 286 Yhteentoimivuustodistus on voimassa kuusi kuukautta. Se peruutetaan tämän ajan kuluttua, ellei valmistaja ole saanut vastaavaa tyyppihyväksyntätodistusta. Valmistaja toimittaa yhteentoimivuustodistuksen sille jäsenvaltion tyyppihyväksyntäviranomaiselle, joka on antanut toiminnallisuustodistuksen.
- 287 Mitään tekijää, joka saattaa aiheuttaa yhteentoimivuusongelman, ei saa käyttää voiton tavoitteluun tai määrävän aseman hankkimiseen.

5. Tyyppihyväksyntätodistus

- 288 Jäsenvaltion tyyppihyväksyntäviranomaisen saa antaa tyyppihyväksyntätodistuksen heti, kun sillä on käytettävissään vaadittavat kolme todistusta.
- 289 Tyyppihyväksyntäviranomaisen on toimitettava jäljennös tyyppihyväksyntätodistuksesta laboratoriolle, joka vastasi yhteensopivuustesteistä silloin, kun todistus annettiin valmistajalle.
- 290 Yhteentoimivuustestejä suorittamaan valtuutetun testauslaboratorion on ylläpidettävä julkista WWW-sivustoa, jolla on ajan tasalla pidettävä luettelo valvontalaite- ja ajopiirturikorttimalleista:
- joita koskeva yhteentoimivuuden testauspyyntö on kirjattu,
 - jotka ovat saaneet yhteentoimivuustodistuksen (myös väliaikaisen),
 - jotka ovat saaneet tyyppihyväksyntätodistuksen.

6. Poikkeusmenettely: ensimmäiset yhteentoimivuustodistukset

- 291 Neljän kuukauden ajan siitä lukien, kun ensimmäiset valvontalaitteet ja ajopiirturikortit (kuljettaja-, korjaamo-, valvontaja-yrityskortit) ovat saaneet yhteentoimivuustodistuksen, kaikki annettavat yhteentoimivuustodistukset (kaikkein ensimmäinen mukaan lukien) ovat väliaikaisia.
- 292 Jos kaikki nämä tuotteet ovat mainitun ajan kuluttua keskenään yhteentoimivia, kaikki vastaavat yhteentoimivuustodistukset muuttuvat lopullisiksi.
- 293 Jos tämän ajan kuluessa havaitaan yhteentoimivuusongelmia, yhteentoimivuustesteistä vastaavan laboratorion on määritettävä ongelmien syyt kaikkien asianosaisten valmistajien avulla sekä kehotettava näitä tekemään vaadittavat muutokset.
- 294 Jos tämän ajan kuluttua vielä esiintyy yhteentoimivuusongelmia, on yhteentoimivuustesteistä vastaavan laboratorion yhteistyössä kaikkien asianosaisten valmistajien ja vastaavat toiminnallisuustodistukset antaneiden tyyppihyväksyntäviranomaisten kanssa määritettävä yhteentoimivuusongelmien syyt ja päätettävä, mitä muutoksia kunkin asianomaisen valmistajan on tehtävä. Teknisten ratkaisujen hakeminen saa kestää enintään kaksi kuukautta, minkä jälkeen, ellei ratkaisua ole löytynyt, komission on yhteentoimivuustesteistä vastaavaa laboratoriota kuultuaan päätettävä, mikä tai mitkä valvontalaitteet ja kortit saavat lopullisen yhteentoimivuustodistuksen ja perusteltava ratkaisunsa.
- 295 Kaikki yhteentoimivuutta koskevat testauspyynnöt, jotka laboratorio on kirjannut ensimmäistä yhteensopivuustodistusta seuraavan neljän kuukauden ajan päättymisen ja vaatimuksessa 294 mainitun komission päätöksen välisenä aikana, on lykättävä siihen asti, kunnes alkuperäiset yhteentoimivuusongelmat on ratkaistu. Sen jälkeen nämä pyynnöt on käsiteltävä siinä aikajärjestyksessä, jossa ne on kirjattu.

Lisäys 1

DATATERMISTÖ

SISÄLLYSLUETTELO

1.	Johdanto	54
1.1	Datatyypin määrittelytapa	54
1.2	Viitetiedot	54
2	Datatyypin määrittelyt	55
2.1	ActivityChangeInfo	55
2.2	Address	56
2.3	BCDString	56
2.4	CalibrationPurpose	56
2.5	CardActivityDailyRecord	57
2.6	CardActivityLengthRange	57
2.7	CardApprovalNumber	57
2.8	CardCertificate	57
2.9	CardChipIdentification	57
2.10	CardConsecutiveIndex	58
2.11	CardControlActivityDataRecord	58
2.12	CardCurrentUse	58
2.13	CardDriverActivity	58
2.14	CardDrivingLicenceInformation	59
2.15	CardEventData	59
2.16	CardEventRecord	59
2.17	CardFaultData	60
2.18	CardFaultRecord	60
2.19	CardIccIdentification	60
2.20	CardIdentification	61
2.21	CardNumber	61
2.22	CardPlaceDailyWorkPeriod	61
2.23	CardPrivateKey	62
2.24	CardPublicKey	62
2.25	CardRenewalIndex	62
2.26	CardReplacementIndex	62
2.27	CardSlotNumber	62
2.28	CardSlotsStatus	62
2.29	CardStructureVersion	63

2.30	CardVehicleRecord	63
2.31	CardVehiclesUsed	63
2.32	Certificate	64
2.33	CertificateContent	64
2.34	CertificateHolderAuthorisation	64
2.35	CertificateRequestID	65
2.36	CertificationAuthorityKID	65
2.37	CompanyActivityData	65
2.38	CompanyActivityType	66
2.39	CompanyCardApplicationIdentification	66
2.40	CompanyCardHolderIdentification	66
2.41	ControlCardApplicationIdentification	67
2.42	ControlCardControlActivityData	67
2.43	ControlCardHolderIdentification	67
2.44	ControlType	68
2.45	CurrentDateTime	68
2.46	DailyPresenceCounter	68
2.47	Datef	69
2.48	Distance	69
2.49	DriverCardApplicationIdentification	69
2.50	DriverCardHolderIdentification	69
2.51	EntryTypeDailyWorkPeriod	70
2.52	EquipmentType	70
2.53	EuropeanPublicKey	70
2.54	EventFaultType	70
2.55	EventFaultRecordPurpose	71
2.56	ExtendedSerialNumber	72
2.57	FullCardNumber	72
2.58	HighResOdometer	72
2.59	HighResTripDistance	72
2.60	HolderName	72
2.61	K-ConstantOfRecordingEquipment	73
2.62	KeyIdentifier	73
2.63	L-TyreCircumference	73
2.64	Language	73
2.65	LastCardDownload	73
2.66	ManualInputFlag	73
2.67	ManufacturerCode	74

2.68	MemberStateCertificate	74
2.69	MemberStatePublicKey	75
2.70	Name	75
2.71	NationAlpha	75
2.72	NationNumeric	76
2.73	NoOfCalibrationRecords	77
2.74	NoOfCalibrationSinceDownload	77
2.75	NoOfCardPlaceRecords	77
2.76	NoOfCardVehicleRecords	77
2.77	NoOfCompanyActivityRecords	77
2.78	NoOfControlActivityRecords	78
2.79	NoOfEventsPerType	78
2.80	NoOfFaultsPerType	78
2.81	OdometerValueMidnight	78
2.82	OdometerShort	78
2.83	OverspeedNumber	78
2.84	PlaceRecord	78
2.85	PreviousVehicleInfo	79
2.86	PublicKey	79
2.87	RegionAlpha	79
2.88	RegionNumeric	79
2.89	RSAPublicModulus	80
2.90	RSAPublicPrivateExponent	80
2.91	RSAPublicExponent	80
2.92	SensorApprovalNumber	80
2.93	SensorIdentification	80
2.94	SensorInstallation	81
2.95	SensorInstallationSecData	81
2.96	SensorOSIdentifier	81
2.97	SensorPaired	81
2.98	SensorPairingDate	82
2.99	SensorSerialNumber	82
2.100	SensorSCIdentifier	82
2.101	Signature	82
2.102	SimilarEventsNumber	82
2.103	SpecificConditionType	82
2.104	SpecificConditionRecord	82
2.105	Speed	83

2.106	SpeedAuthorised	83
2.107	SpeedAverage	83
2.108	SpeedMax	83
2.109	TDesSessionKey	83
2.110	TimeReal	83
2.111	TyreSize	83
2.112	VehicleIdentificationNumber	84
2.113	VehicleRegistrationIdentification	84
2.114	VehicleRegistrationNumber	84
2.115	VuActivityDailyData	84
2.116	VuApprovalNumber	84
2.117	VuCalibrationData	84
2.118	VuCalibrationRecord	85
2.119	VuCardIWDData	85
2.120	VuCardIWRRecord	86
2.121	VuCertificate	86
2.122	VuCompanyLocksData	86
2.123	VuCompanyLocksRecord	87
2.124	VuControlActivityData	87
2.125	VuControlActivityRecord	87
2.126	VuDataBlockCounter	87
2.127	VuDetailedSpeedBlock	87
2.128	VuDetailedSpeedData	88
2.129	VuDownloadablePeriod	88
2.130	VuDownloadActivityData	88
2.131	VuEventData	88
2.132	VuEventRecord	89
2.133	VuFaultData	89
2.134	VuFaultRecord	89
2.135	VuIdentification	90
2.136	VuManufacturerAddress	90
2.137	VuManufacturerName	90
2.138	VuManufacturingDate	90
2.139	VuOverSpeedingControlData	91
2.140	VuOverSpeedingEventData	91
2.141	VuOverSpeedingEventRecord	91
2.142	VuPartNumber	91
2.143	VuPlaceDailyWorkPeriodData	92

2.144	VuPlaceDailyWorkPeriodRecord	92
2.145	VuPrivateKey	92
2.146	VuPublicKey	92
2.147	VuSerialNumber	92
2.148	VuSoftInstallationDate	92
2.149	VuSoftwareIdentification	92
2.150	VuSoftwareVersion	93
2.151	VuSpecificConditionData	93
2.152	VuTimeAdjustmentData	93
2.153	VuTimeAdjustmentRecord	93
2.154	W-VehicleCharacteristicConstant	93
2.155	WorkshopCardApplicationIdentification	94
2.156	WorkshopCardCalibrationData	94
2.157	WorkshopCardCalibrationRecord	94
2.158	WorkshopCardHolderIdentification	95
2.159	WorkshopCardPIN	95
3.	Arvoalueiden määrittelyt	96
3.1	Kuljettajakorttia koskevat määrittelyt:	96
3.2	Korjaamokorttia koskevat määrittelyt:	96
3.3	Yrityskorttia koskevat määrittelyt:	96
3.4	Yrityskorttia koskevat määrittelyt	96
4.	Merkistöt	96
5.	Koodaus	96

1. JOHDANTO

Tässä lisäyksessä määritellään valvontalaitteissa ja ajopiirturikorteissa käytettävän datan muodot, elementit ja rakenteet.

1.1 Datatyyppien määrittelytapa

Tässä lisäyksessä käytetään ASN.1-merkintätavan mukaisia datatyyppien määrittelyjä. Näin erilliset dataelementit ja data-rakenteet voidaan määritellä ilman sidonnaisuutta mihinkään datansiirron vaatimaan muotorakenteeseen (koodaussääntöön), jolloin määrittelyt ovat sovelluksesta ja ympäristöstä riippumattomia.

ASN.1-merkintätavan mukaiset datatyyppien määrittelyt on tehty ISO/IEC 8824-1 -standardin mukaisesti. Tästä seuraa, että:

- mikäli mahdollista, datatypille valittu nimi viittaa sen käyttötarkoitukseen,
- milloin datatyyppi on muiden datatyyppien yhdistelmä, sen nimi on silti yhteen kirjoitettu sarja kirjainmerkkejä, joka alkaa isolla kirjaimella, kuitenkin siten, että isoja kirjaimia on käytetty myös nimen keskellä välittämään tietoa nimen osien merkityksestä,
- yleensä datatyyppien nimet liittyvät niiden datatyyppien nimiin, joista ne on rakennettu, niiden laitteiden nimiin, joissa dataa tallennetaan, ja niihin toimintoihin, joihin data liittyy.

Jos ASN.1-datatyyppi on jo määritelty osana jotain muuta standardia, ja sitä käytetään myös valvontalaitteissa, määritellään kyseinen ASN.1-datatyyppi tässä lisäyksessä.

Jotta useiden erilaisten koodaussääntöjen käyttäminen olisi mahdollista, joillakin tämän lisäyksen ASN.1-datatyypeillä on rajoituksia arvoalueiden osalta. Nämä arvoalueiden rajoitukset on määritelty kohdassa 3.

1.2 Viitetiedot

Tässä lisäyksessä käytetään seuraavia viitteitä:

- | | |
|----------------|--|
| ISO 639 | Code for the representation of names of languages. First Edition: 1988. (Kielten nimien tunnukset Ensimmäinen painos: 1998.) |
| EN 726-3 | Identification cards systems — Telecommunications integrated circuit(s) cards and terminals — Part 3: Application independent card requirements. December 1994. (Henkilökorttijärjestelmät. Tietoliikenteessä käytettävät integroidulla piirillä varustetut kontaktilliset kortit. Osa 3: Sovelluksesta riippumattomien korttien vaatimukset. Joulukuu 1994.) |
| ISO 3779 | Road vehicles — Vehicle identification number (VIN) — Content and structure. Edition 3: 1983. (Tietoliikenteessä käytettävät ajoneuvot. Ajoneuvojen valmistenumero. Sisältö ja rakenne. Kolmas painos: 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. (Tietotekniikka. Henkilökortit. Integroidulla piirillä varustetut kontaktilliset kortit. Osa 5: Numerointijärjestelmä ja rekisteröintimenettelyt sovellustunnuksille. Ensimmäinen painos: 1994, ensimmäinen muutos: 1996.) |
| ISO/IEC 8824-1 | Information technology — Abstract Syntax Notation 1 (ASN.1): Specification of basic notation. Edition 2: 1998. (Tietotekniikka. Abstrakti syntaksin esitysmuoto 1 (ASN.1): Perusesitysmuodon määrittely. Toinen painos: 1998.) |
| ISO/IEC 8825-2 | Information technology — ASN.1 encoding rules: Specification of Packed Encoding Rules (PER). Edition 2: 1998. (Tietotekniikka. ASN.1-koodaussäännöt: pakkaukseen tarkoitettujen koodaussääntöjen (PER) määrittely. Toinen painos: 1998.) |
| ISO/IEC 8859-1 | Information technology — 8 bit single-byte coded graphic character sets — Part 1: Latin alphabet No.1. First edition: 1998. (Tietotekniikka. Yksitavuiset 8-bittiset koodatut graafiset merkit. Osa 1. Latinalaisaakkosto nro 1. Ensimmäinen painos: 1998.) |
| ISO/IEC 8859-7 | Information technology — 8 bit single-byte coded graphic character sets — Part 7: Latin/Greek alphabet. First edition: 1987. (Tietotekniikka. Yksitavuiset 8-bittiset koodatut graafiset merkit. Osa 7. Latinalais-kreikkalaisaakkosto. Ensimmäinen painos: 1987.) |
| ISO 16844-3 | Road vehicles — Tachograph systems — Motion Sensor Interface. WD 3-20/05/99. (Tietoliikenteessä käytettävät ajoneuvot. Ajopiirturijärjestelmät. Liiketunnistimen liitäntälaite.) |

2 DATATYYPPIEN MÄÄRITTELYT

Kaikkien seuraavien datatyyppien oletusarvoinen dataelementin arvo tapauksissa, joissa arvo on tuntematon tai ei sovellettavissa, saadaan täyttämällä dataelementti tavuilla, joiden arvo on 'FFh'.

2.1 ActivityChangeInfo

Tämän datatyypin avulla voidaan kaksitavuista sanaa käyttäen koodata korttiaukon tilanne klo 00.00 ja/tai kuljettajatilanne klo 00.00 ja/tai toiminnan muutoksia ja/tai ajoneuvon miehityksen muutoksia ja/tai kuljettajan tai apukuljettajan kortin tilan muutoksia. Tämä datatyyppi liittyy vaatimuksiin 084, 109a, 199 ja 219.

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

Asetettava arvo — Octet Aligned (tavuittain ryhmitelty): 'scpaattttttttttt'B (16 bittiä)

Datamuistin tallenteille (tai korttiaukon tilanteelle):

's'B	Korttiaukko:
	'0'B: DRIVER (kuljettaja),
	'1'B: CO-DRIVER (apukuljettaja),
'c'B	Ajoneuvon miehitys:
	'0'B: SINGLE (yksin),
	'1'B: CREW (miehistö),
'p'B	Kuljettajakortin (tai korjaamokortin) tila kyseisessä korttiaukossa:
	'0'B: INSERTED (kortti on asetettuna aukkoon),
	'1'B: NOT INSERTED (korttia ei ole asetettu aukkoon (tai se on poistettu)),
'aa'B	Toiminta:
	'00'B: BREAK/REST (tauko/lepo),
	'01'B: AVAILABILITY (varallaolo),
	'10'B: WORK (työ),
	'11'B: DRIVING (ajo),
'ttttttttttt'B	Muutoksen aika: minuutteina klo 00.00 lukien kyseisenä päivänä.

Kuljettajakortin (tai korjaamokortin) tallenteille (ja kuljettajatilanteelle):

's'B	Korttiaukko (ei oleellinen, kun 'p' = 1, paitsi alla olevan huomautuksen tapauksessa):	
	'0'B: DRIVER (kuljettaja),	
	'1'B: CO-DRIVER (apukuljettaja),	
'c'B	Ajoneuvon miehitys (tapaus 'p' = 0) tai toiminnan tilan mukaan (tapaus 'p' = 1):	
	'0'B: SINGLE (yksin),	'0'B: UNKNOWN (tuntematon)
	'1'B: CREW (miehistö),	'1'B: KNOWN (= käsin syötetty)
'p'B	Kortin tila:	
	'0'B: INSERTED, (kortti on asetettuna valvontalaitteeseen),	
	'1'B: NOT INSERTED, (korttia ei ole asetettu laitteeseen (tai se on postettu)),	

'aa'B Toiminta (ei oleellinen, kun 'p' = 1, paitsi alla olevan huomautuksen tapauksessa):

'00'B: BREAK/REST (tauko/lepo),

'01'B: AVAILABILITY (varallaolo),

'10'B: WORK (työ),

'11'B: DRIVING (ajo),

'tttttttttt'B Muutoksen aika: minuutteina klo 00.00 lukien kyseisenä päivänä.

Huomautus, joka koskee tapausta 'kortin poistaminen':

Kun kortti poistetaan:

- 's' on oleellinen ja osoittaa korttiaukon, josta kortti poistetaan,
- 'c' on asetettava arvoon 0,
- 'p' on asetettava arvoon 1,
- 'aa' on asetettava kortin poistamishetkellä valittuna ollutta toimintaa vastaavaksi,

Käsin syöttämisen tuloksena kortille tallennetun tietueen tavujen 'c' ja 'aa' päälle voidaan myöhemmin kirjoittaa uudet tilannetta kuvaavat tiedot.

2.2 Address

Osoite.

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

codePage määrittelee sen ISO/IEC 8859 -standardin osan, jonka mukaisesti osoite on koodattu,

address on ISO/IEC 8859-codePage -koodisivun mukaisesti määritelty osoite.

2.3 BCDString

BCDString-datatyypillä esitetään luvut BCD- eli binaarikoodatussa desimaalimuodossa. Tätä datatyyppiä käytetään esittämään yksi desimaali yhdellä nelibittisellä (puoli)tavulla. BCDString perustuu ISO/IEC 8824-1 -standardin 'CharacterStringType'-määrittelyyn.

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

BCDString-datatyypissä käytetään 'hstring'-merkintätapaa. Vasemmanpuoleisin heksadesimaaliluku on ensimmäisen tavun merkitsevin puolittavu. Muodostettaessa useita tavuja on tarvittaessa lisättävä nollan arvoisia puolittavuja ensimmäisen tavun vasemmanpuoleisesta puolittavusta alkaen.

Sallitut luvut ovat: 0, 1, ... 9.

2.4 CalibrationPurpose

Koodi, joka ilmaisee, miksi joukko kalibrointiparametreja on tallennettu. Tämä datatyyppi liittyy vaatimuksiin 097 ja 098.

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

Asetettava arvo:

'00'H varattu arvo,

'01'H aktivointi: ajoneuvoyksikköä aktivoitaessa tunnettujen kalibrointiparametrien tallennus,

- '02'H ensiasennus: ajoneuvoyksikön ensimmäinen kalibrointi sen aktivoinnin jälkeen,
 '03'H asennus: ajoneuvoyksikön ensimmäinen kalibrointi sen ollessa nykyisessä ajoneuvossa,
 '04'H määräaikaistarkastus.

2.5 CardActivityDailyRecord

Kortille tallennetut tiedot, jotka liittyvät kuljettajan toimintaan tietyn kalenterivuorokauden aikana. Tämä datatyypin liitetty vaatimukseen 199 ja 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 on edellisen päivätietueen kokonaispituus tavuina. Tämän maksimiarvon määrää sen OCTET STRING -tavujonon pituus, johon nämä tiedot tallennetaan. (Ks. CardActivityLengthRange-muuttujan selitystä kohdassa 3). Kun kyseinen tietue on vanhin päivittäinen tietue, on activityPreviousRecordLength-muuttujan arvoksi asetettava 0.

activityRecordLength on tämän tietueen kokonaispituus tavuina. Tämän maksimiarvon määrää sen OCTET STRING -tavujonon pituus, johon nämä tiedot tallennetaan.

activityRecordDate on tietueen päiväys.

activityDailyPresenceCounter on kyseistä päivää vastaava kortin käyttökertalaskurin arvo.

activityDayDistance on kyseisenä päivänä kuljettu kokonaismatka.

activityChangeInfo on kuljettajan ActivityChangeInfo-tiedot kyseiseltä päivältä. Se voi sisältää enintään 1440 tietoa (yksi toiminnan tilan muutos minuuttia kohden). Sisältää aina ActivityChangeInfo-tiedot, jotka ilmoittavat kuljettajatilanteen klo 00.00.

2.6 CardActivityLengthRange

Kuljettaja- tai korjaamokortilla oleva tavumäärä kuljettajan toimintaa koskevien tietojen tallentamiseksi.

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

Asetettava arvo: Ks. kohta 3.

2.7 CardApprovalNumber

Kortin tyyppihyväksyntänumero.

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

Asetettava arvo: Määrittelemätön.

2.8 CardCertificate

Kortin julkisen avaimen varmenne.

```
CardCertificate ::= Certificate
```

2.9 CardChipIdentification

Kortille tallennetut tiedot, jotka liittyvät kortin integroituun piiriin (IC:hen) (vaatimus 191).

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


activityPointerOldestDayRecord on sen tallennuspaikan alun määrittely (tavuina merkkijonon alusta lukien), johon on tallennettu vanhin täydellinen activityDailyRecords-merkkijonoon sisältyvä päivätietue. Osoitinmuuttujan maksimiarvon määrää merkkijonon pituus.

activityPointerNewestRecord on sen tallennuspaikan alun määrittely (tavuina merkkijonon alusta lukien), johon on tallennettu viimeisin täydellinen activityDailyRecords-merkkijonoon sisältyvä päivätietue. Osoitinmuuttujan maksimiarvon määrää merkkijonon pituus.

activityDailyRecords on kuljettajan päivittäiseen toimintaan liittyvien tietojen tallennukseen käytettävissä oleva tila (datarakenne: CardActivityDailyRecord) jokaista sellaista kalenterivuorokautta kohden, jolloin korttia on käytetty.

Asetettava arvo: Tätä tavujonoa täytetään kiertävästi CardActivityDailyRecord-tiedoilla. Ensimmäisellä kerralla tallennus aloitetaan jonon ensimmäisestä tavusta. Kaikki uudet tietueet lisätään edellisen perään. Kun tavujono on täynnä, tallennusta jatketaan jonon ensimmäisestä tavusta välittämättä dataelementin sisälle syntyvästä katkoksesta. Ennen kuin tavujonoon lisätään uusia toimintatietoja (laajentamalla käytössä olevaa activityDailyRecord-tilaa tai avaamalla uusi activityDailyRecord-tila), jotka korvaavat vanhempia toimintatietoja, activityPointerOldestDayRecord-osoitin on asetettava vanhimman täydellisen päivittäisen tietueen sijaintia vastaavaksi ja tämän (uuden) vanhimman täydellisen päivittäisen tietueen activityPreviousRecordLength-tieto on asetettava nollassi.

2.14 CardDrivingLicenceInformation

Kuljettajakortille tallennetut tiedot, jotka liittyvät kortin haltijan ajokortin tietoihin (vaatimus 196).

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

drivingLicenceIssuingAuthority on kortin myöntänyt viranomainen.

drivingLicenceIssuingNation on kortin myöntäneen viranomaisen kansallisuus.

drivingLicenceNumber on ajokortin numero.

2.15 CardEventData

Kuljettaja- tai korjaamokortille tallennetut tiedot, jotka liittyvät kortin haltijaa koskeviin tapauksiin (vaatimukset 204 ja 223).

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

CardEventData on sarja cardEventRecords-tietueita, järjestettynä nousevaan järjestykseen EventFaultType-muuttujan arvon mukaan (paitsi tietoturvan murtoyritykset, jotka kerätään tietuesarjan viimeiseen osaan).

cardEventRecords on sarja tietyn tyyppin tapauksiin liittyviä tietueita (tai tietoturvan murtoyrityksiin liittyvä tapausluokka).

2.16 CardEventRecord

Kuljettaja- tai korjaamokortille tallennetut tiedot, liittyvät kortin haltijaa koskeviin tapauksiin (vaatimukset 205 ja 223).

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

eventType on tapauksen tyyppi.

eventBeginTime on päivämäärä ja aika, jolloin tapaus alkoi.

eventEndTime on päivämäärä ja aika, jolloin tapaus päättyi.

eventVehicleRegistration on sen ajoneuvon rekisteritunnus ja rekisteröinyt jäsenvaltio, jossa tapaus sattui.

2.17 CardFaultData

Kuljettaja- tai korjaamokortille tallennetut tiedot, jotka liittyvät kortin haltijaa koskeviin vikatapahtumiin (vaatimukset 207 ja 223).

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

CardFaultData on sarja valvontalaittevikoihin liittyviä tietueita ja sen perässä oleva sarja korttivikoihin liittyviä tietueita.

cardFaultRecords on sarja tiettyihin vikatyyppeihin liittyviä tietueita (valvontalaitte- tai korttivika).

2.18 CardFaultRecord

Kuljettaja- tai korjaamokortille tallennetut tiedot, jotka liittyvät kortin haltijaa koskeviin vikatapahtumiin (vaatimukset 208 ja 223).

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

faultType on vikatapahtuman tyyppi.

faultBeginTime on päivämäärä ja aika, jolloin vikatapahtuma alkoi.

faultEndTime on päivämäärä ja aika, jolloin vikatapahtuma päättyi.

faultVehicleRegistration on sen ajoneuvon rekisteritunnus ja rekisteröinyt jäsenvaltio, jossa vikatapahtuma sattui.

2.19 CardIccIdentification

Kortille tallennetut tiedot, jotka liittyvät integroidun piirin sisältävän kortin (IC-kortin) tunnistukseen (vaatimus 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 on standardissa EN 726-3 määritelty Clockstop-tila.

cardExtendedSerialNumber on IC-kortin sarjanumero ja IC-kortin valmistusviite siten kuin se on määritelty standardissa EN 726-3 ja edelleen määritelty ExtendedSerialNumber-datatyypillä.

cardApprovalNumber on kortin tyyppihyväksyntänumero.

cardPersonaliserID on standardissa EN 726-3 määritelty kortin yksilöintitunnus.

embedderIcAssemblerId on kortin laminoijan/IC:n asentajan tunniste siten kuin se on määritelty standardissa EN 726-3.

icIdentifier on kortilla olevan integroidun piirin ja piirin valmistajan Identifier-tunnus siten kuin se on määritelty standardissa EN 726-3.

2.20 CardIdentification

Kortille tallennetut tiedot, jotka liittyvät kortin tunnistukseen (vaatimukset 194, 215, 231, 235).

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

cardIssuingMemberState on kortin myöntäneen jäsenvaltion tunnus.

cardNumber on kortin numero.

cardIssuingAuthorityName on kortin myöntäneen viranomaisen nimi.

cardIssueDate on päivämäärä, jolloin kortti myönnettiin nykyiselle haltijalleen.

cardValidityBegin on kortin ensimmäinen voimassaolopäivä.

cardExpiryDate on kortin viimeinen voimassaolopäivä.

2.21 CardNumber

Määritelmän g mukainen kortin numero.

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

driverIdentification on tunniste, joka yksilöi kuljettajan jäsenvaltiossa.

ownerIdentification on tunniste, joka yksilöi yrityksen tai korjaamon tai tarkastuksia suorittavan elimen jäsenvaltiossa.

cardConsecutiveIndex on kortin haltijakohtainen sarjanumero.

cardReplacementIndex on kortin korvausnumero.

cardRenewalIndex on kortin uusintanumero.

Tietokokonaisuuden (CHOICE) ensimmäiseen kohtaan (SEQUENCE) voi sisällyttää kuljettajakortin numeron ja toiseen kohtaan (SEQUENCE) korjaamokortin, valvontakortin ja yrityskortin numeron.

2.22 CardPlaceDailyWorkPeriod

Kuljettaja- tai korjaamokortille tallennetut tiedot, jotka liittyvät paikkaan, jossa päivän työaika alkaa ja/tai päättyy (vaatimukset 202 ja 221).

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

placePointerNewestRecord on viimeksi päivitetyn paikkaan liittyvän tiedon järjestysnumero.

Asetettava arvo: Numero, joka vastaa paikkaan liittyvän tietueen järjestysnumeroa, alkaen numerosta '0' ensimmäiselle paikkaan liittyvälle tietueelle datarakenteessa.

placeRecords on sarja tietueita, jotka sisältävät syötettyihin paikkoihin liittyviä tietoja.

2.23 CardPrivateKey

Kortin yksityinen avain.

```
CardPrivateKey ::= RSAKeyPrivateExponent
```

2.24 CardPublicKey

Kortin julkinen avain.

```
CardPublicKey ::= PublicKey
```

2.25 CardRenewalIndex

Kortin uusintanumero (määritelmä i).

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

Asetettava arvo: (ks. tämän liitteen VII luku).

'0' Ensi kerran myönnetty.

Suurennusjärjestys: '0, ..., 9, A, ..., Z'

2.26 CardReplacementIndex

Kortin korvausnumero (määritelmä j).

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

Asetettava arvo: (ks. tämän liitteen VII luku).

'0' Alkuperäinen kortti.

Suurennusjärjestys: '0, ..., 9, A, ..., Z'

2.27 CardSlotNumber

Tunnus, jolla erotetaan toisistaan ajoneuvoyksikön kaksi korttiaukkoa.

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

Asetettava arvo: Ei lisämäärittelyä.

2.28 CardSlotsStatus

Tunnus, joka osoittaa ajoneuvoyksikön kahteen korttiaukkoon asetettujen korttien tyyppin.

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

Asetettava arvo — Octet Aligned (tavuittain ryhmitelty): 'ccccddd'B:

'cccc'B apukuljettajan korttiaukkoon asetetun kortin tunnistus,

'ddd'B kuljettajan korttiaukkoon asetetun kortin tunnistus,

jossa käytetään seuraavia tunnuksia:

'0000'B aukossa ei ole korttia,

'0001'B aukossa on kuljettajakortti,

'0010'B aukossa on korjaamokortti,

'0011'B aukossa on valvontakortti,

'0100'B aukossa on yrityskortti.

2.29 CardStructureVersion

Tunnus, joka osoittaa ajopiirturikortille annetun datarakenteen versionumeron.

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

Asetettava arvo: 'aabb'H:

'aa'H rakenteen muutoksen järjestysnumero,

'bb'H eniten merkitsevän tavun mukaiselle datarakennaversiolle määriteltyjen dataelementtien käyttöä koskevan muutoksen järjestysnumero.

2.30 CardVehicleRecord

Kuljettaja- tai korjaamokortille tallennetut tiedot, jotka liittyvät ajoneuvon käyttöjaksoon kalenterivuorokauden aikana (vaatimukset 197 ja 217).

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

vehicleOdometerBegin on ajoneuvon matkamittarin lukema ajoneuvon käyttöjakson alussa.

vehicleOdometerEnd on ajoneuvon matkamittarin lukema ajoneuvon käyttöjakson lopussa.

vehicleFirstUse vehicleFirstUse on päivämäärä ja aika, jolloin ajoneuvon käyttöjakso alkoi.

vehicleLastUse on päivämäärä ja aika, jolloin ajoneuvon käyttöjakso päättyi.

vehicleRegistration on ajoneuvon rekisteritunnus ja ajoneuvon rekisteröinyt jäsenvaltio.

vuDataBlockCounter on VuDataBlockCounter-laskurin arvo, kun kortti poistetaan viimeisen kerran ajoneuvon käyttöjakson aikana.

2.31 CardVehiclesUsed

Kuljettaja- tai korjaamokortille tallennetut tiedot, jotka liittyvät kortin haltijan käyttämiin ajoneuvoihin (vaatimukset 197 ja 217).

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

vehiclePointerNewestRecord on viimeksi päivitetyn ajoneuvon liittyvän tietueen järjestysnumero.

Asetettava arvo: Numero, joka vastaa ajoneuvon liittyvän tietueen järjestysnumeroa, alkaen numerosta '0' ensimmäiselle ajoneuvon liittyvälle tietueelle datarakenteessa.

cardVehicleRecords on sarja tietueita, jotka sisältävät haltijan käyttämiin ajoneuvoihin liittyviä tietoja.

2.32 Certificate

Varmenneviranomaisen antama julkisen avaimen varmenne.

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

Asetettava arvo: Digitaalinen allekirjoitus, joka sisältää CertificateContent-tietueen sisällön osittaisen palautuksen lisäyksen 11 (Yhteiset turvamekanismit) mukaisesti: allekirjoitus (128 tavua) || julkisen avaimen jakojäännös (58 tavua) || varmenteen antaneen viranomaisen viite (8 tavua).

2.33 CertificateContent

Julkisen avaimen varmenteen (selväkielinen) sisältö lisäyksen 11 (Yhteiset turvamekanismit) mukaisesti.

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

certificateProfileIdentifier on vastaavan varmenteen versio.

Asetettava arvo: '01h' tälle versiolle.

CertificationAuthorityReference yksilöi varmenneviranomaisen, joka on antanut tämän varmenteen, sekä antaa kyseisen viranomaisen julkisen avaimen viitetiedot.

certificateHolderAuthorisation yksilöi varmenteen haltijan oikeudet.

certificateEndOfValidity on varmenteen viimeinen hallinnollinen voimassaolopäivä.

certificateHolderReference yksilöi varmenteen haltijan sekä antaa hänen julkisen avaimensa viitetiedot.

publicKey on tämän varmenteen avulla varmennettu julkinen avain.

2.34 CertificateHolderAuthorisation

Varmenteen haltijan oikeuksien tunniste.

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

tachographApplicationID on piirturisovelluksen tunniste.

Asetettava arvo: 'FFh' '54h' '41h' '43h' '48h' '4Fh'. Tämä sovellustunniste on ISO/IEC 7816-5 -standardin mukainen varattu rekisteröimätön sovellustunniste.

equipmentType on sen laitetyyppin tunniste, jonka yhteydessä varmennetta käytetään.

Asetettava arvo: EquipmentType-datatyyppin mukaan. Nolla, jos kyseessä on jäsenvaltion oma varmenne.

2.35 CertificateRequestID

Varmennepyynnön täysin yksilöivä tunniste. Tunnistetta voidaan käyttää myös ajoneuvoyksikön julkisen avaimen tunnisteena, mikäli sen ajoneuvoyksikön sarjanumero, johon avain on tarkoitettu, ei ole tiedossa silloin, kun varmenne luodaan.

```
CertificateRequestID ::= SEQUENCE {
    requestSerialNumber          INTEGER(0..232-1)
    requestMonthYear             BCDString(SIZE(2))
    crIdentifier                 OCTET STRING(SIZE(1))
    manufacturerCode            ManufacturerCode
}
```

requestSerialNumber on varmennepyynnön sarjanumero, joka täysin yksilöi valmistajan ja alla määritellyn kuukauden.

requestMonthYear on sen kuukauden ja vuoden tunniste, jolloin varmennepyyntö tehtiin.

Asetettava arvo: Binaarikoodatussa desimaalimuodossa (BCD) esitetty kuukausi (kaksi numeroa) ja vuosi (kaksi viimeistä numeroa).

crIdentifier: on tunniste, jolla varmennepyyntö erotetaan laajennetusta sarjanumerosta.

Asetettava arvo: 'FFh'.

manufacturerCode: on varmennetta pyytävän valmistajan numerotunniste.

2.36 CertificationAuthorityKID

Varmenneviranomaisen (jäsenvaltion tai eurooppalainen varmenneviranomaisen) julkisen avaimen tunniste.

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

nationNumeric on varmenneviranomaisen maan numerotunnus.

nationAlpha on varmenneviranomaisen maan kirjaintunnus.

keySerialNumber on sarjanumero, jonka avulla tunnistetaan varmenneviranomaisen eri avaimet siinä tapauksessa, että avain vaihtuu.

additionalInfo on kaksitavuinen kenttä lisäkoodeja varten (varmenneviranomaisen mukaan).

caIdentifier on tunnus, jolla varmenneviranomaisen avaimen tunniste erotetaan muista avaimen tunnisteista.

Asetettava arvo: '01h'.

2.37 CompanyActivityData

Yrityskortille tallennetut tiedot, jotka liittyvät kortilla suoritettuihin toimiin (vaatimus 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 on viimeksi päivitetyn companyActivityRecord-tietueen järjestysnumero.

Asetettava arvo: Numero, joka vastaa yrityksen toimiiin liittyvän tietueen järjestysnumeroa, alkaen numerosta '0' ensimmäiselle yrityksen toimiiin liittyvälle tietueelle datarakenteessa.

companyActivityRecords on sarja tietueita, joka sisältää kaikki yrityksen toimiiin liittyvät tiedot.

companyActivityRecord on yhteen yrityksen toimeen liittyviä tietoja sisältävä tietue.

companyActivityType on yrityksen toimen tyyppi.

companyActivityTime on yrityksen toimen päivämäärä ja aika.

cardNumberInformation on sen kortin numero ja myöntänyt viranomainen, jonka tiedot kopioitiin, jos tällainen kopiointi suoritettiin.

vehicleRegistrationInformation on sen ajoneuvon rekisteritunnus ja rekisteröinyt viranomainen, jossa lukitus tehtiin tai avattiin.

downloadPeriodBegin y **downloadPeriodEnd** ovat sen ajanjakson alku ja loppu, jota vastaavat tiedot kopioitiin ajoneuvoyksiköstä, jos tällainen kopiointi suoritettiin.

2.38 CompanyActivityType

Tunnus, joka osoittaa yrityksen toimen tyyppin yrityskorttia käytettäessä.

```

CompanyActivityType ::= INTEGER {
    card downloading                (1),
    VU downloading                  (2),
    VU lock-in                       (3),
    VU lock-out                      (4)
}

```

2.39 CompanyCardApplicationIdentification

Yrityskortille tallennetut tiedot, jotka liittyvät kortilla olevan sovelluksen tunnistamiseen (vaatimus 190).

```

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

```

typeOfTachographCardId määrittelee kortilla käytetyn tunnisteen tyyppin.

cardStructureVersion määrittelee kortilla käytetyn datarakenteen version.

noOfCompanyActivityRecords on kortille tallennettavissa olevien yrityksen toimiiin liittyvien tietueiden määrä.

2.40 CompanyCardHolderIdentification

Yrityskortille tallennetut tiedot, jotka liittyvät kortin haltijan tunnistukseen (vaatimus 236).

```

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

```

companyName on kortin haltijayrityksen nimi.

companyAddress on kortin haltijayrityksen osoite.

cardHolderPreferredLanguage on kortin haltijan ensisijaisesti käyttämä kieli.

2.41 ControlCardApplicationIdentification

Valvontakortille tallennetut tiedot, jotka liittyvät kortilla olevan sovelluksen tunnistamiseen (vaatimus 190).

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

typeOfTachographCardId määrittelee kortilla käytetyn tunnisteen tyyppin.

cardStructureVersion määrittelee kortilla käytetyn datarakenteen version.

noOfControlActivityRecords on kortille tallennettavissa olevien tarkastustoimiin liittyvien tietueiden määrä.

2.42 ControlCardControlActivityData

Valvontakortille tallennetut tiedot, jotka liittyvät korttia käyttäen suoritettuihin tarkastustoimiin (vaatimus 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 on viimeksi päivitetyn companyActivityRecord-tietueen järjestysnumero.

Asetettava arvo: Numero, joka vastaa tarkastustoimiin liittyvän tietueen järjestysnumeroa, alkaen numerosta '0' ensimmäiselle tarkastustoimiin liittyvälle tietueelle datarakenteessa.

controlActivityRecords on sarja tietueita, jotka sisältävät kaikki tarkastustoimiin liittyvät tiedot.

controlActivityRecord on yhteen tarkastustoimeen liittyviä tietoja sisältävä tietue.

controlType on tarkastustoimen tyyppi.

controlTime on tarkastustoimen päivämäärä ja aika.

controlledCardNumber on sen kortin numero ja myöntänyt viranomainen, johon tarkastustoimi kohdistui.

controlledVehicleRegistration on sen ajoneuvon rekisteritunnus ja rekisteröinyt viranomainen, jossa tarkastus tapahtui.

controlDownloadPeriodBegin ja **controlDownloadPeriodEnd** ovat sen ajanjakson alku ja loppu, jota koskevat tiedot mahdollisesti kopioitiin.

2.43 ControlCardHolderIdentification

Valvontakortille tallennetut tiedot, jotka liittyvät kortin haltijan tunnistukseen (vaatimus 232).

```

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

```

controlBodyName on sen tarkastuselimen nimi, johon kortin haltija kuuluu.

controlBodyAddress on sen tarkastuselimen osoite, johon kortin haltija kuuluu.

cardHolderName on kortin haltijan nimi ja etunimi (etunimet).

cardHolderPreferredLanguage on kortin haltijan ensisijaisesti käyttämä kieli.

2.44 ControlType

Tunnus, joka osoittaa tarkastuksen aikana suoritettut toimet. Tämä datatyyppi liittyy vaatimuksiin 102, 210 ja 225.

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

Asetettava arvo — Octet aligned (tavuittain ryhmitelty): 'c'p'd'xxxx'B (8 bits)

'c'B kortin tietojen kopiointi:

'0'B: kortin tietoja ei kopioitu tämän tarkastustoimen aikana,

'1'B: kortin tietoja kopioitiin tämän tarkastustoimen aikana

'v'B ajoneuvoyksikön tietojen kopiointi:

'0'B: ajoneuvoyksikön tietoja ei kopioitu tämän tarkastustoimen aikana,

'1'B: ajoneuvoyksikön tietoja kopioitiin tämän tarkastustoimen aikana

'p'B printing:

'0'B: tietoja ei tulostettu tämän tarkastustoimen aikana,

'1'B: tietoja tulostettiin tämän tarkastustoimen aikana

'd'B display:

'0'B: näyttöä ei käytetty tämän tarkastustoimen aikana,

'1'B: näyttöä käytettiin tämän tarkastustoimen aikana

'xxxx'B ei käytössä.

2.45 CurrentDateTime

Valvontalaitteessa meneillään oleva päivämäärä ja aika.

```
CurrentDateTime ::= TimeReal
```

Asetettava arvo: Ei lisämäärittelyjä.

2.46 DailyPresenceCounter

Kuljettaja- tai korjaamokortille tallennettu laskuri, jonka arvoa suurennetaan yhdellä jokaisena sellaisena kalenterivuorokautena, jolloin kortti on ollut asetettuna ajoneuvoyksikköön. Tämä datatyyppi liittyy vaatimuksiin 199 ja 219.

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

Asetettava arvo: Juokseva numero, jonka maksimiarvo on 9999 ja joka sen jälkeen alkaa jälleen nolasta. Korttia ensi kerran myönnettäessä numero asetetaan nolaksi.

2.47 Datef

Päivämäärä ilmaistuna helposti tulostettavassa numeerisessa muodossa.

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

Asetettava arvo:

```
YYYY      vuosi
mm        kuukausi
dd        päivä
```

'00000000'H merkitsee nimenomaan, ettei päivämäärätietoa ole.

2.48 Distance

Kuljettu matka (ajoneuvon kahden matkamittarilukeman laskettu ero kilometreinä).

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

Asetettava arvo: Etumerkitön binaariluku. Arvo kilometreinä alueella 0-9 999 km.

2.49 DriverCardApplicationIdentification

Kuljettajakortille tallennetut tiedot, jotka liittyvät kortilla olevan sovelluksen tunnistamiseen (vaatimus 190).

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

typeOfTachographCardId määrittelee kortilla käytetyn tunnisteiden tyypin.

cardStructureVersion määrittelee kortilla käytetyn datarakenteen version.

noOfEventsPerType on niiden tapauksien määrä tapaustyyppiä kohden, jotka voidaan tallentaa kortille.

noOfFaultsPerType on niiden vikatapahtumien määrä vikatyyppiä kohden, jotka voidaan tallentaa kortille.

activityStructureLength osoittaa niiden tavujen määrän, jotka ovat käytettävissä kuljettajan toimintaan liittyvien tietojen tallennukseen.

noOfCardVehicleRecords on niiden ajoneuvon liittyviä tietoja sisältävien tietueiden määrä, jotka voidaan tallentaa kortille.

noOfCardPlaceRecords on niiden paikkoihin liittyviä tietoja sisältävien tietueiden määrä, jotka voidaan tallentaa kortille.

2.50 DriverCardHolderIdentification

Kuljettajakortille tallennetut tiedot, jotka liittyvät kortin haltijan tunnistukseen (vaatimus 195).

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

cardHolderName on kuljettajakortin haltijan nimi ja etunimi (etunimet).

cardHolderBirthDate on kuljettajakortin haltijan syntymäaika.

cardHolderPreferredLanguage on kuljettajakortin haltijan ensisijaisesti käyttämä kieli.

2.51 EntryTypeDailyWorkPeriod

Tunnus, jolla tehdään ero päivän työajan alkamis- ja päättymispaikkaa koskevien syötettyjen tietojen alkamis- ja päättymisaikojen sekä erilaisten tiedon syöttämisolosuhteiden välillä.

```
EntryTypeDailyWorkPeriod ::= INTEGER
    Begin, related time = card insertion time or time of entry           (0),
    End,   related time = card withdrawal time or time of entry         (1),
    Begin, related time manually entered (start time)                   (2),
    End,   related time manually entered (end of work period)           (3),
    Begin, related time assumed by VU                                   (4),
    End,   related time assumed by VU                                   (5)
}
```

Asetettava arvo: Standardin ISO/IEC8824-1 mukaisesti.

2.52 EquipmentType

Tunnus, jolla erotetaan erilaiset ajopiirturisovelluksessa käytettävät laitteet.

```
EquipmentType ::= INTEGER(0..255)
-- Reserved                (0),
-- Driver Card             (1),
-- Workshop Card           (2),
-- Control Card            (3),
-- Company Card            (4),
-- Manufacturing Card      (5),
-- Vehicle Unit            (6),
-- Motion Sensor           (7),
-- RFU                     (8..255)
```

Asetettava arvo: Standardin ISO/IEC8824-1 mukaisesti.

Arvo 0 on varattu tietyn jäsenvaltion tai Euroopan yksilöimiseen varmenteen CHA-kentässä.

2.53 EuropeanPublicKey

Eurooppalainen julkinen avain.

```
EuropeanPublicKey ::= PublicKey
```

2.54 EventFaultType

Tunnus, jolla merkitään tapauksen tai vian tyyppi.

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

Asetettava arvo:

'0x'H	Luonteeltaan yleiset tapaukset,
'00'H	Ei lisätietoja,
'01'H	Ei voimassa olevan kortin asettaminen laitteeseen,
'02'H	Korttiristiriita,
'03'H	Aikojen päällekkäisyys,
'04'H	Ajo ilman asianmukaista korttia,
'05'H	Kortin paikoilleen asettaminen ajon aikana,
'06'H	Edellistä kortin käyttöjaksoa ei lopetettu oikein,
'07'H	Ylinopeus,

'08'H	Keskeytynyt virransyöttö,
'09'H	Virhe liikedatassa,
'0A'H .. '0F'H	Varattu tulevaan käyttöön,
'1x'H	Ajoneuvoyksikköön liittyvät tietoturvan murtoyritykset,
'10'H	Ei lisätietoja,
'11'H	Liiketunnistimen tunnistaminen epäonnistui,
'12'H	Ajopiirturikortin tunnistaminen epäonnistui,
'13'H	Liiketunnistimen luvaton vaihtaminen,
'14'H	Virhe kortille syötettävien tietojen eheydessä,
'15'H	Virhe tallennettujen käyttäjään liittyvien tietojen eheydessä,
'16'H	Virhe sisäisessä tiedonsiirrossa,
'17'H	Laitteen kotelon luvaton avaaminen,
'18'H	Laitteiden tahallinen vahingoittaminen,
'19'H .. '1F'H	Varattu tulevaan käyttöön,
'2x'H	Liiketunnistimeen liittyvät tietoturvan murtoyritykset,
'20'H	Ei lisätietoja,
'21'H	Tunnistaminen epäonnistui,
'22'H	Virhe tallennettujen tietojen eheydessä,
'23'H	Virhe sisäisessä tiedonsiirrossa,
'24'H	Laitteen kotelon luvaton avaaminen,
'25'H	Laitteiden tahallinen vahingoittaminen,
'26'H .. '2F'H	Varattu tulevaan käyttöön,
'3x'H	Valvontalaiteviat,
'30'H	Ei lisätietoja,
'31'H	Ajoneuvoyksikön sisäinen vika,
'32'H	Vika tulostimessa,
'33'H	Vika näytössä,
'34'H	Tietojen kopioinnissa ilmennyt vika,
'35'H	Vika liiketunnistimessa,
'36'H .. '3F'H	Varattu tulevaan käyttöön,
'4x'H	Korttiviati,
'40'H	Ei lisätietoja,
'41'H .. '4F'H	Varattu tulevaan käyttöön,
'50'H .. '7F'H	Varattu tulevaan käyttöön,
'80'H .. 'FF'H	Arvo määryytyy laitevalmistajan mukaan.

2.55 EventFaultRecordPurpose

Tunnus, joka ilmaisee, miksi tietty tapaus tai vika on kirjattu.

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

Asetettava arvo:

'00'H	Yksi kymmenestä viimeksi tapahtuneesta tapauksesta tai viasta
'01'H	Pisimpään kestänyt tapaus jonain niistä kymmenestä viimeisestä päivästä, jolloin tapauksia sattui
'02'H	Yksi viidestä pisimpään kestäneestä tapauksesta viimeisen 365 vuorokauden aikana
'03'H	Päivän viimeinen tapaus jonain niistä kymmenestä viimeisestä päivästä, jolloin tapauksia sattui
'04'H	Vakavin tapaus jonain niistä kymmenestä viimeisestä päivästä, jolloin tapauksia sattui
'05'H	Yksi viidestä vakavimmasta tapauksesta viimeisen 365 vuorokauden aikana
'06'H	Ensimmäinen tapaus tai vika, joka sattui viimeisimmän kalibroinnin jälkeen
'07'H	Aktiivinen/meneillään oleva vika tai tapahtuma
'08'H .. '7F'H	Varattu tulevaan käyttöön
'80'H .. 'FF'H	Arvo määryytyy laitevalmistajan mukaan

2.56 ExtendedSerialNumber

Laitteen yksilöivä tunnus. Sitä voidaan käyttää myös laitteen julkisen avaimen tunnisteena.

```
ExtendedSerialNumber ::= SEQUENCE {
    serialNumber          INTEGER(0..232-1)
    monthYear            BCDString(SIZE(2))
    type                 OCTET STRING(SIZE(1))
    manufacturerCode     ManufacturerCode
}
```

serialNumber on laitteen sarjanumero, joka on tietyn valmistajan laitteille ainoa tietylle laitetypille ja tietyssä alla määritellyssä kuussa annettu tämä numero.

monthYear on sen kuukauden ja vuoden tunniste, jolloin laite on valmistettu (tai sarjanumero sitä varten varattu).

Asetettava arvo: Kuukausi (kaksi numeroa) ja vuosi (kaksi viimeistä numeroa) binaarikoodatussa desimaalimuodossa (BCD).

type on laitetypin tunniste.

Asetettava arvo: Arvo määräytyy laitevalmistajan mukaan; arvo 'FFh' on varattu muihin tarkoituksiin.

manufacturerCode on laitteen valmistajan numerotunniste.

2.57 FullCardNumber

Tunnus, joka täysin yksilöi ajopiirturikortin.

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

cardType on ajopiirturikortin tyyppi.

cardIssuingMemberState on kortin myöntäneen jäsenvaltion tunnus.

cardNumber on kortin numero.

2.58 HighResOdometer

Ajoneuvon matkamittarin lukema: Kokonaismatka, jonka ajoneuvo on kulkenut tähänastisen käyttöikänsä aikana.

```
HighResOdometer ::= INTEGER(0..232-1)
```

Asetettava arvo: Etumerkitön binaariluku. Arvo kilometrin kahdessadasosina alueella 0-21 055 406 km.

2.59 HighResTripDistance

Yksittäisen matkan välimatkamittarilukema.

```
HighResTripDistance ::= INTEGER(0..232-1)
```

Asetettava arvo: Etumerkitön binaariluku. Arvo kilometrin kahdessadasosina alueella 0-21 055 406 km.

2.60 HolderName

Kortin haltijan sukunimi ja etunimi (etunimet).

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


holderSurname on haltijan sukunimi. Sukunimeen ei sisällytetä titteleitä.

Asetettava arvo: Jos kortti ei ole tarkoitettu henkilökohtaiseen käyttöön, holderSurname-tietue sisältää samat tiedot kuin companyName- tai workshopName- tai controlBodyName-tietueet.

holderFirstNames on haltijan etunimi (etunimet) ja etunimen alkukirjaimet.

2.61 K-ConstantOfRecordingEquipment

Valvontalaitteen vakio (määritelmä m).

K-ConstantOfRecordingEquipment ::= INTEGER(0..2¹⁶-1)

Asetettava arvo: Impulsseja kilometriä kohti alueella 0-64 255 impulssia/km.

2.62 KeyIdentifier

Julkisen avaimen täysin yksilöivä tunniste, jota käytetään avaimen viitetietona ja avaimen valinnassa. Se yksilöi myös avaimen haltijan.

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

Ensimmäinen vaihtoehto on sopiva ajoneuvoyksikön tai ajopiirturikortin julkisen avaimen tunnisteeksi.

Toinen vaihtoehto on sopiva ajoneuvoyksikön julkisen avaimen tunnisteeksi (tapauksissa, joissa ajoneuvoyksikön sarjainumero ei ole tiedossa silloin, kun varmenne luodaan).

Kolmas vaihtoehto on sopiva jäsenvaltion julkisen avaimen tunnisteeksi.

2.63 L-TyreCircumference

Pyörien renkaiden tehollinen ympärysmitta (määritelmä u).

L-TyreCircumference ::= INTEGER(0..2¹⁶-1)

Asetettava arvo: Etumerkitön binaariluku. Arvo millimetrim kahdeksasosina alueella 0-8 031 mm.

2.64 Language

Kielen yksilöivä tunnus.

Language ::= IA5String(SIZE(2))

Asetettava arvo: ISO 639 -standardin mukainen merkintä kahdella pienellä kirjaimella.

2.65 LastCardDownload

Kuljettajakortille tallennettu viimeisimmän (muussa kuin valvontatarkoituksessa tehdyn) kortin tietojen kopiointin päivämäärä ja aika. Päivämäärä on päivitettävissä ajoneuvoyksiköstä tai mistä tahansa kortinlukulaitteesta.

LastCardDownload ::= TimeReal

Asetettava arvo: Ei lisämäärittelyjä.

2.66 ManualInputFlag

Erote, joka ilmaisee, onko kortin haltija kortin paikoilleen asettamisen yhteydessä syöttänyt kuljettajan toimintaa koskevia tietoja käsin (vaatimus 081).

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

Asetettava arvo: Ei lisämäärittelyjä.

2.67 ManufacturerCode

Valmistajan yksilöivä tunnus.

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

Asetettava arvo:

'00'H	Tietoa ei ole käytettävissä
'01'H	Varattu arvo
'02'H .. '0F'H	Varattu tulevaan käyttöön
'10'H	ACTIA
'11'H .. '17'H	Varattu valmistajille, joiden nimi alkaa 'A'-kirjaimella
'18'H .. '1F'H	Varattu valmistajille, joiden nimi alkaa 'B'-kirjaimella
'20'H .. '27'H	Varattu valmistajille, joiden nimi alkaa 'C'-kirjaimella
'28'H .. '2F'H	Varattu valmistajille, joiden nimi alkaa 'D'-kirjaimella
'30'H .. '37'H	Varattu valmistajille, joiden nimi alkaa 'E'-kirjaimella
'38'H .. '3F'H	Varattu valmistajille, joiden nimi alkaa 'F'-kirjaimella
'40'H	Giesecke & Devrient GmbH
'41'H	GEM plus
'42'H .. '47'H	Varattu valmistajille, joiden nimi alkaa 'G'-kirjaimella
'48'H .. '4F'H	Varattu valmistajille, joiden nimi alkaa 'H'-kirjaimella
'50'H .. '57'H	Varattu valmistajille, joiden nimi alkaa 'I'-kirjaimella
'58'H .. '5F'H	Varattu valmistajille, joiden nimi alkaa 'J'-kirjaimella
'60'H .. '67'H	Varattu valmistajille, joiden nimi alkaa 'K'-kirjaimella
'68'H .. '6F'H	Varattu valmistajille, joiden nimi alkaa 'L'-kirjaimella
'70'H .. '77'H	Varattu valmistajille, joiden nimi alkaa 'M'-kirjaimella
'78'H .. '7F'H	Varattu valmistajille, joiden nimi alkaa 'N'-kirjaimella
'80'H	OSCARD
'81'H .. '87'H	Varattu valmistajille, joiden nimi alkaa 'O'-kirjaimella
'88'H .. '8F'H	Varattu valmistajille, joiden nimi alkaa 'P'-kirjaimella
'90'H .. '97'H	Varattu valmistajille, joiden nimi alkaa 'Q'-kirjaimella
'98'H .. '9F'H	Varattu valmistajille, joiden nimi alkaa 'R'-kirjaimella
'A0'H	SETEC
'A1'H	SIEMENS VDO
'A2'H	STONERIDGE
'A3'H .. 'A7'H	Varattu valmistajille, joiden nimi alkaa 'S'-kirjaimella
'AA'H	TACHOCONTROL
'AB'H .. 'AF'H	Varattu valmistajille, joiden nimi alkaa 'T'-kirjaimella
'B0'H .. 'B7'H	Varattu valmistajille, joiden nimi alkaa 'U'-kirjaimella
'B8'H .. 'BF'H	Varattu valmistajille, joiden nimi alkaa 'V'-kirjaimella
'C0'H .. 'C7'H	Varattu valmistajille, joiden nimi alkaa 'W'-kirjaimella
'C8'H .. 'CF'H	Varattu valmistajille, joiden nimi alkaa 'X'-kirjaimella
'D0'H .. 'D7'H	Varattu valmistajille, joiden nimi alkaa 'Y'-kirjaimella
'D8'H .. 'DF'H	Varattu valmistajille, joiden nimi alkaa 'Z'-kirjaimella

2.68 MemberStateCertificate

Eurooppalaisen varmenneviranomaisen myöntämä jäsenvaltion julkisen avaimen varmenne.

```
MemberStateCertificate ::= Certificate
```

2.69 MemberStatePublicKey

Jäsenvaltion julkinen avain.

MemberStatePublicKey ::= PublicKey

2.70 Name

Nimi.

Name ::= SEQUENCE {

```

    codePage                INTEGER (0..255),
    name                     OCTET STRING (SIZE(35))
}

```

codePage määrittlee sen ISO/IEC 8859 -standardin osan, jonka mukaisesti nimi on koodattu,

name on ISO/IEC 8859-codePage -koodisivun mukaisesti koodattu nimi.

2.71 NationAlpha

Maan kirjainlyhenne ajoneuvoihin kiinnitettävien kansallisuustunnusten ja/tai kansainvälisesti yhdenmukaistettujen vakuutustodistusten (green cardien) mukaan.

NationAlpha ::= IA5String(SIZE(3))

Asetettava arvo:

' '	Tietoa ei ole käytettävissä,
'A'	Itävalta,
'AL'	Albania,
'AND'	Andorra,
'ARM'	Armenia,
'AZ'	Azerbaidžan,
'B'	Belgia,
'BG'	Bulgaria,
'BIH'	Bosnia-Hertsegovina,
'BY'	Valko-Venäjä,
'CH'	Sveitsi,
'CY'	Kypros,
'CZ'	Tšekki,
'D'	Saksa,
'DK'	Tanska,
'E'	Espanja,
'EST'	Viro,
'F'	Ranska,
'FIN'	Suomi,
'FL'	Liechtenstein,
'FR'	Färsaaret,
'UK'	Yhdistynyt kuningaskunta, Alderney, Guernsey, Jersey, Mansaari, Gibraltar,
'GE'	Georgia,
'GR'	Kreikka,
'H'	Unkari,
'HR'	Kroatia,
'I'	Italia,
'IRL'	Irlanti,
'IS'	Islanti,
'KZ'	Kazakstan,
'L'	Luxemburg,
'LT'	Liettua,
'LV'	Latvia,
'M'	Malta,
'MC'	Monaco,

'MD'	Moldova,
'MK'	Makedonia,
'N'	Norja,
'NL'	Alankomaat,
'P'	Portugali,
'PL'	Puola,
'RO'	Romania,
'RSM'	San Marino,
'RUS'	Venäjän federaatio,
'S'	Ruotsi,
'SK'	Slovakia,
'SLO'	Slovenia,
'TM'	Turkmenistan,
'TR'	Turkki,
'UA'	Ukraina
'V'	Vatikaani,
'YU'	Jugoslavia,
'UNK'	Tuntematon,
'EC'	Euroopan yhteisö,
'EUR'	Muu Eurooppa,
'WLD'	Muu maailma.

2.72 NationNumeric

Maan numeroviite.

NationNumeric ::= INTEGER(0..255)

Asetettava arvo:

-- Tietoa ei ole käytettävissä	(00) H,
-- Itävalta	(01) H,
-- Albania	(02) H,
-- Andorra	(03) H,
-- Armenia	(04) H,
-- Azerbaidžan	(05) H,
-- Belgia	(06) H,
-- Bulgaria	(07) H,
-- Bosnia-Hertsegovina	(08) H,
-- Valko-Venäjä	(09) H,
-- Sveitsi	(0A) H,
-- Kypros	(0B) H,
-- Tšekki	(0C) H,
-- Saksa	(0D) H,
-- Tanska	(0E) H,
-- Espanja	(0F) H,
-- Viro	(10) H,
-- Ranska	(11) H,
-- Suomi	(12) H,
-- Liechtenstein	(13) H,
-- Färsaaret	(14) H,
-- Yhdistynyt kuningaskunta	(15) H,
-- Georgia	(16) H,
-- Kreikka	(17) H,
-- Unkari	(18) H,
-- Kroatia	(19) H,
-- Italia	(1A) H,
-- Irlanti	(1B) H,
-- Islanti	(1C) H,

-- Kazakstan	(1D)H,
-- Luxemburg	(1E)H,
-- Liettua	(1F)H,
-- Latvia	(20)H,
-- Malta	(21)H,
-- Monaco	(22)H,
-- Moldova	(23)H,
-- Makedonia	(24)H,
-- Norja	(25)H,
-- Alankomaat	(26)H,
-- Portugali	(27)H,
-- Puola	(28)H,
-- Romania	(29)H,
-- San Marino	(2A)H,
-- Venäjän federaatio	(2B)H,
-- Ruotsi	(2C)H,
-- Slovakia	(2D)H,
-- Slovenia	(2E)H,
-- Turkmenistan	(2F)H,
-- Turkki	(30)H,
-- Ukraina	(31)H,
-- Vatikaani	(32)H,
-- Jugoslavia	(33)H,
-- Varattu tulevaan käyttöön	(34..FC)H,
-- Euroopan yhteisö	(FD)H,
-- Muu Eurooppa	(FE)H,
-- Muu maailma	(FF)H

2.73 NoOfCalibrationRecords

Korjaamokortille mahtuvien kalibrointitietoja sisältävien tietueiden määrä.

NoOfCalibrationRecords ::= INTEGER(0..255)

Asetettava arvo: Ks. kohta 3.

2.74 NoOfCalibrationsSinceDownload

Laskuri, joka osoittaa korjaamokortilla suoritettujen kalibrointien määrän sen jälkeen, kun kortin tietoja on viimeksi kopioitu (vaatimus 230).

NoOfCalibrationsSinceDownload ::= INTEGER(0..2¹⁶-1),

Asetettava arvo: Ei lisämäärittelyjä.

2.75 NoOfCardPlaceRecords

Kuljettaja- tai korjaamokortille mahtuvien paikkaan liittyviä tietoja sisältävien tietueiden määrä.

NoOfCardPlaceRecords ::= INTEGER(0..255)

Asetettava arvo: Ks. kohta 3.

2.76 NoOfCardVehicleRecords

Kuljettaja- tai korjaamokortille mahtuvien käytössä olleisiin ajoneuvoihin liittyviä tietoja sisältävien tietueiden määrä.

NoOfCardVehicleRecords ::= INTEGER(0..2¹⁶-1)

Asetettava arvo: Ks. kohta 3.

2.77 NoOfCompanyActivityRecords

Yrityskortille mahtuvien yrityksen toimiin liittyviä tietoja sisältävien tietueiden määrä.

NoOfCompanyActivityRecords ::= INTEGER(0..2¹⁶-1)

Asetettava arvo: Ks. kohta 3.

2.78 NoOfControlActivityRecords

Valvontakortille mahtuvien tarkastustoimiin liittyviä tietoja sisältävien tietueiden määrä.

NoOfControlActivityRecords ::= INTEGER(0..2¹⁶-1)

Asetettava arvo: Ks. kohta 3.

2.79 NoOfEventsPerType

Kortille mahtuvien tapaustyyppikohtaisiin tapausten lukumääriin liittyviä tietoja sisältävien tietueiden määrä.

NoOfEventsPerType ::= INTEGER(0..255)

Asetettava arvo: Ks. kohta 3.

2.80 NoOfFaultsPerType

Kortille mahtuvien vikatyyppikohtaisiin vikatapahtumien lukumääriin liittyviä tietoja sisältävien tietueiden määrä.

NoOfFaultsPerType ::= INTEGER(0..255)

Asetettava arvo: Ks. kohta 3.

2.81 OdometerValueMidnight

Ajoneuvon matkamittarin lukema keskiyöllä tietyinä päivinä (vaatimus 090).

OdometerValueMidnight ::= OdometerShort

Asetettava arvo: Ei lisämäärittelyjä.

2.82 OdometerShort

Ajoneuvon matkamittarin lukema lyhyessä muodossa.

OdometerShort ::= INTEGER(0..2²⁴-1)

Asetettava arvo: Etumerkitön binaariluku. Arvo alueella 0-9 999 999 km.

2.83 OverspeedNumber

Ylinopeustapausten määrä viimeksi suoritettun ylinopeustarkastuksen jälkeen.

OverspeedNumber ::= INTEGER(0..255)

Asetettava arvo: 0 tarkoittaa, ettei viimeksi suoritettun ylinopeustarkastuksen jälkeen ole sattunut ylinopeustapauksia, 1 tarkoittaa, että viimeksi suoritettun ylinopeustarkastuksen jälkeen on sattunut yksi ylinopeustapaus ... 255 tarkoittaa, että viimeksi suoritettun ylinopeustarkastuksen jälkeen on sattunut 255 tai useampia ylinopeustapauksia.

2.84 PlaceRecord

Tiedot, jotka liittyvät paikkaan, jossa päivän työaika alkaa tai päättyy (vaatimukset 087, 202, 221).

```
PlaceRecord ::= SEQUENCE {
    entryTime                TimeReal,
    entryTypeDailyWorkPeriod EntryTypeDailyWorkPeriod,
    dailyWorkPeriodCountry   NationNumeric,
    dailyWorkPeriodRegion    RegionNumeric,
    vehicleOdometerValue     OdometerShort
}
```

entryTime on syötettyyn tietoon liittyvä päivämäärä ja aika.

entryTypeDailyWorkPeriod on syötetyn tiedon tyyppi.

dailyWorkPeriodCountry on syötetty maatieto.

dailyWorkPeriodRegion on syötetty aluetieto.

vehicleOdometerValue on matkamittarin lukema silloin, kun paikkaan liittyvä tieto syötettiin.

2.85 PreviousVehicleInfo

Tiedot, jotka liittyvät ajoneuvoon, jota kuljettaja käytti asettaessaan edellisen kerran kuljettajakorttinsa ajoneuvolaitteeseen (vaatimus 081).

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

vehicleRegistrationIdentification on ajoneuvon rekisteritunnus ja ajoneuvon rekisteröinyt jäsenvaltio.

cardWithdrawalTime on päivämäärä ja aika, jolloin kortti poistettiin.

2.86 PublicKey

Julkinen RSA-avain.

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

rsaKeyModulus on avainparin kongruenssimoduuli.

rsaKeyPublicExponent on avainparin julkinen eksponentti.

2.87 RegionAlpha

Tietyn maan alueen kirjainviite.

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

Asetettava arvo:

' ' Tietoa ei ole käytettävissä,

Espanja:

'AN'	Andalusia,
'AR'	Aragonia,
'AST'	Asturia,
'C'	Kantabria,
'CAT'	Katalonia,
'CL'	Kastilia ja León,
'CM'	Kastilia-LaMancha,
'CV'	Valencia,
'EXT'	Extremadura,
'G'	Galicia,
'IB'	Baleaarit,
'IC'	Kanariansaaret,
'LR'	La Rioja,
'M'	Madrid,
'MU'	Murcia,
'NA'	Navarra,
'PV'	Baskimaa

2.88 RegionNumeric

Tietyn maan alueen numeroviite.

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

Asetettava arvo:

'00'H Tietoa ei ole käytettävissä,

Espanja:

'01'H Andalusia,
 '02'H Aragonia,
 '03'H Asturia,
 '04'H Kantabria,
 '05'H Katalonia,
 '06'H Kastilia ja León,
 '07'H Kastilia-LaMancha,
 '08'H Valencia,
 '09'H Extremadura,
 '0A'H Galicia,
 '0B'H Baleaarit,
 '0C'H Kanariansaaret,
 '0D'H La Rioja,
 '0E'H Madrid,
 '0F'H Murcia,
 '10'H Navarra,
 '11'H Baskimaa

2.89 RSAKeyModulus

RSA-avainparin kongruenssimoduuli.

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

Asetettava arvo: Ei määritelty.

2.90 RSAKeyPrivateExponent

RSA-salauksessa käytettävän avainparin salainen eksponentti.

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

Asetettava arvo: Ei määritelty.

2.91 RSAKeyPublicExponent

RSA-salauksessa käytettävän avainparin julkinen eksponentti

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

Asetettava arvo: Ei määritelty.

2.92 SensorApprovalNumber

Liiketunnistimen tyyppihyväksyntänumero.

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

Asetettava arvo: Ei määritelty.

2.93 SensorIdentification

Liiketunnistimeen tallennetut tiedot, jotka liittyvät liiketunnistimen tunnistukseen (vaatimus 077).

```

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

```


sensorSerialNumber on liiketunnistimen sarjanumero pitkässä muodossa (sisältää osanumeron ja valmistustunnuksen).

on liiketunnistimen hyväksyntänumero.

sensorSCIdentifier on liiketunnistimen turvakomponentin tunniste.

sensorOSIdentifier on liiketunnistimen käyttöjärjestelmän tunniste.

2.94 SensorInstallation

Liiketunnistimeen tallennetut tiedot, jotka liittyvät liiketunnistimen asennukseen (vaatimus 099).

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

sensorPairingDateFirst on päivämäärä, jolloin liiketunnistin ensimmäisen kerran liitettiin ajoneuvoyksikköön.

firstVuApprovalNumber on ensimmäisen liiketunnistimeen liitetyn ajoneuvoyksikön hyväksyntänumero.

firstVuSerialNumber on ensimmäisen liiketunnistimeen liitetyn ajoneuvoyksikön sarjanumero.

sensorPairingDateCurrent on päivämäärä, jolloin liiketunnistin ensimmäisen kerran liitettiin nykyiseen ajoneuvoyksikköön.

currentVuApprovalNumber on liiketunnistimeen nykyisin liitetyn ajoneuvoyksikön hyväksyntänumero.

currentVUSerialNumber on liiketunnistimeen nykyisin liitetyn ajoneuvoyksikön sarjanumero.

2.95 SensorInstallationSecData

Korjaamokortille tallennetut tiedot, jotka liittyvät niihin turvatietoihin, joita tarvitaan liitettäessä liiketunnistin ajoneuvoyksikköön (vaatimus 214).

```
SensorInstallationSecData ::= TDesSessionKey
```

Asetettava arvo: Standardin ISO 16844-3 mukaisesti.

2.96 SensorOSIdentifier

Liiketunnistimen käyttöjärjestelmän tunniste.

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

Asetettava arvo: Arvo määräytyy laitevalmistajan mukaan.

2.97 SensorPaired

Ajoneuvoyksikköön tallennetut tiedot, jotka liittyvät ajoneuvoyksikköön liitettyyn liiketunnistimeen (vaatimus 079).

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

sensorSerialNumber on ajoneuvoyksikköön nykyisin liitetyn liiketunnistimen sarjanumero.

sensorApprovalNumber on ajoneuvoyksikköön nykyisin liitetyn liiketunnistimen hyväksyntänumero.

sensorPairingDateFirst on päivämäärä, jolloin liiketunnistin ensimmäistä kertaa liitettiin ajoneuvoyksikköön, johon se nykyisin on liitetty.

2.98 **SensorPairingDate**

Päivämäärä, jolloin liiketunnistin liitettiin ajoneuvoyksikköön.

`SensorPairingDate ::= TimeReal`

Asetettava arvo: Ei määritely.

2.99 **SensorSerialNumber**

Liiketunnistimen sarjanumero.

`SensorSerialNumber ::= ExtendedSerialNumber`

2.100 **SensorSCIdentifier**

Liiketunnistimen turvakomponentin tunnistus.

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

Asetettava arvo: Arvo määräytyy komponentin valmistajan mukaan.

2.101 **Signature**

Digitaalinen allekirjoitus.

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

Asetettava arvo: Lisäyksen 11 (Yhteiset turvamekanismit) mukaisesti.

2.102 **SimilarEventsNumber**

Tietyinä päivinä sattuneiden vastaavien tapausten määrä (vaatimus 094).

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

Asetettava arvo: Arvoa 0 ei käytetä, 1 tarkoittaa, että kyseisenä päivänä on sattunut ja tallennettu yksi kyseisentyyppinen tapaus, 2 tarkoittaa, että kyseisenä päivänä on sattunut kaksi kyseisentyyppistä tapausta (vain yksi on tallennettu), ... 255 tarkoittaa, että kyseisenä päivänä on sattunut 255 tai useampia kyseisentyyppisiä tapauksia.

2.103 **SpecificConditionType**

Erytisolosuhteet yksilöivä tunnus (vaatimukset 050b, 105a, 212a ja 230a).

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

Asetettava arvo:

'00'H	Varattu tulevaan käyttöön
'01'H	Asetuksen piiriin kuulumaton — alku
'02'H	Asetuksen piiriin kuulumaton — päättymisen
'03'H	Lautta-/junakuljetus
'04'H .. 'FF'H	Varattu tulevaan käyttöön

2.104 **SpecificConditionRecord**

Kuljettajakortille, korjaamokortille tai ajoneuvoyksikköön tallennetut tiedot, jotka liittyvät erityisolosuhteisiin (vaatimukset 105a, 212a ja 230a).

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

entryTime on päivämäärä ja aika, jolloin tieto syötettiin.

specificConditionType on tunnus, joka yksilöi erityisolosuhteet.

2.105 Speed

Ajoneuvon nopeus (km/t).

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

Asetettava arvo: kilometreinä tunnissa alueella 0–220 km/t.

2.106 SpeedAuthorised

Ajoneuvon suurin sallittu nopeus (määritelmä bb).

```
SpeedAuthorised ::= Speed
```

2.107 SpeedAverage

Keskimääräinen nopeus aiemmin määritellyn jakson aikana (km/t).

```
SpeedAverage ::= Speed
```

2.108 SpeedMax

Suurin nopeus aiemmin määritellyn jakson aikana.

```
SpeedMax ::= Speed
```

2.109 TDesSessionKey

Kolminkertaisessa DES-salauksessa käytettävä avain.

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

Asetettava arvo: Ei lisämäärittelyjä.

2.110 TimeReal

Tunnus yhdistetyssä päivämäärä- ja aikakentässä, jossa päivämäärä ja aika ilmaistaan ajan kello 00:00:00 1. tammikuuta 1970 jälkeen kuluneina sekunteina (GMT).

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

Asetettava arvo — Octet Aligned (tavuittain ryhmitelty): Keskiyön 1. tammikuuta 1970 (GMT) jälkeen kuluneiden sekuntien määrä.

Viimeinen mahdollinen päivämäärä/aika on vuonna 2106.

2.111 TyreSize

Rengaskoon merkintä.

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

Asetettava arvo: Direktiivin 92/23/ETY mukaisesti.

2.112 VehicleIdentificationNumber

Ajoneuvon valmistenumero (VIN), joka viittaa koko ajoneuvoon, yleensä korin sarjanumero.

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

Asetettava arvo: Kuten standardissa ISO 3779 on määritelty.

2.113 VehicleRegistrationIdentification

Ajoneuvon tunniste, joka yksilöi eurooppalaisen ajoneuvon (rekisteritunnus ja jäsenvaltio).

```
VehicleRegistrationIdentification ::= SEQUENCE {
    vehicleRegistrationNation      NationNumeric,
    vehicleRegistrationNumber      VehicleRegistrationNumber
}
```

vehicleRegistrationNation on valtio, jossa ajoneuvo on rekisteröity.

vehicleRegistrationNumber on ajoneuvon rekisteritunnus (VRN).

2.114 VehicleRegistrationNumber

Ajoneuvon rekisteritunnus (VRN). Rekisteritunnuksen antaa ajoneuvojen rekisteröinnistä vastaava viranomainen.

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

codePage määrittelee sen ISO/IEC 8859 -standardin osan, jonka mukaisesti rekisteritunnus on koodattu,

vehicleRegNumber on ISO/IEC 8859-codePage -koodisivun mukaisesti määritelty rekisteritunnus.

Asetettava arvo: Rekisteröintimaan mukaan.

2.115 VuActivityDailyData

Ajoneuvoyksikköön tallennetut tiedot, jotka liittyvät toiminnan tyyppin muutoksiin ja/tai ajoneuvon miehityksen muutoksiin ja/tai kortin tilan muutoksiin tietyn kalenterivuorokauden aikana (vaatimus 084) ja korttiaukkojen tilaan kyseisenä päivänä klo 00.00.

```
VuActivityDailyData ::= SEQUENCE {
    noOfActivityChanges           INTEGER SIZE(0..1440),
    activityChangeInfos           SET SIZE(noOfActivityChanges) OF
    ActivityChangeInfo
}
```

noOfActivityChanges on activityChangeInfos-sarjassa olevien ActivityChangeInfo-sanojen määrä.

activityChangeInfos on ajoneuvoyksikköön tallennettu tiettyä päivää koskeva ActivityChangeInfo-sanojen sarja. Se sisältää aina kaksi ActivityChangeInfo-sanaa, jotka ilmaisevat kummankin korttiaukon tilan kyseisenä päivänä klo 00.00.

2.116 VuApprovalNumber

Ajoneuvoyksikön tyyppihväksyntänumero.

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

Asetettava arvo: Ei määritelty.

2.117 VuCalibrationData

Ajoneuvoyksikköön tallennetut tiedot, jotka liittyvät valvontalaitteen kalibrointeihin (vaatimus 098).

```
VuCalibrationData ::= SEQUENCE {
    noOfVuCalibrationRecords      INTEGER(0..255),
    vuCalibrationRecords          SET SIZE(noOfVuCalibrationRecords) OF
    VuCalibrationRecord
}
```

noOfVuCalibrationRecords on vuCalibrationRecords-tietuesarjan sisältämien tietueiden määrä.

vuCalibrationRecords on sarja kalibrointeihin liittyviä tietueita.

2.118 VuCalibrationRecord

Ajoneuvoyksikköön tallennetut tiedot, jotka kukin liittyvät valvontalaitteen yksittäiseen kalibrointiin (vaatimus 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 on syy, jonka vuoksi kalibrointi suoritettiin.

workshopName, **workshopAddress** ovat korjaamon nimi ja osoite.

workshopCardNumber yksilöi kalibroinnin aikana käytetyn korjaamokortin.

workshopCardExpiryDate on kortin viimeinen voimassaolopäivä.

vehicleIdentificationNumber on ajoneuvon valmistenumero (VIN).

vehicleRegistrationIdentification sisältää ajoneuvon rekisteritunnuksen (VRN) ja rekisteröineen jäsenvaltion.

wVehicleCharacteristicConstant on ajoneuvon ominaiskerroin.

kConstantOfRecordingEquipment on valvontalaitteen vakio.

lTyreCircumference on pyörien renkaiden tehollinen ympärysmitta.

tyreSize on ajoneuvon asennettujen renkaiden kokomerkinä.

authorisedSpeed on ajoneuvon suurin sallittu nopeus.

oldOdometerValue, **newOdometerValue** ovat matkamittarin vanha ja uusi lukema.

oldTimeValue, **newTimeValue** ovat päivämäärän ja ajan vanhat ja uudet arvot.

nextCalibrationDate on päivämäärä, jolloin valtuutetun tarkastusviranomaisen on suoritettava seuraava CalibrationPurpose-muuttujan määrittelemä kalibrointi.

2.119 VuCardIWData

Ajoneuvoyksikköön tallennetut tiedot, jotka liittyvät kuljettaja- tai korjaamokorttien ajoneuvoyksikköön asettamis- ja poistojaksoihin (vaatimus 081).

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

noOfIWRecords on vuCardIWRecords-tietuesarjassa olevien tietueiden määrä.

vuCardIWRecords on sarja tietueita, jotka liittyvät kortin paikoilleen asettamis- ja poistojaksoihin.

2.120 VuCardIWRecord

Ajoneuvoyksikköön tallennetut tiedot, jotka liittyvät yksittäiseen kuljettaja- tai korjaamokortin ajoneuvoyksikköön asettamis- ja poistojaksoon (vaatimus 081).

```
VuCardIWRecord ::= SEQUENCE {
    cardHolderName                HolderName ,
    fullCardNumber                FullCardNumber ,
    cardExpiryDate                TimeReal ,
    cardInsertionTime             TimeReal ,
    vehicleOdometerValueAtInsertion OdometerShort ,
    cardSlotNumber                CardsSlotNumber ,
    cardWithdrawalTime            TimeReal ,
    vehicleOdometerValueAtWithdrawal OdometerShort ,
    previousVehicleInfo           PreviousVehicleInfo
    manualInputFlag                ManualInputFlag
}
```

cardHolderName on kuljettaja- tai korjaamokortin haltijan sukunimi ja etunimet siinä muodossa kuin ne on tallennettu kortille.

fullCardNumber on kortin tyyppi, sen myöntänyt jäsenvaltio sekä kortin numero siinä muodossa kuin ne on tallennettu kortille.

cardExpiryDate on kortin viimeinen voimassaolopäivä siinä muodossa kuin se on tallennettu kortille.

cardInsertionTime on päivämäärä ja aika, jolloin kortti asetettiin paikoilleen.

vehicleOdometerValueAtInsertion on ajoneuvon matkamittarin lukema silloin, kun kortti asetettiin paikoilleen.

cardSlotNumber on korttiaukko, johon kortti asetettiin.

cardWithdrawalTime on päivämäärä ja aika, jolloin kortti poistettiin.

vehicleOdometerValueAtWithdrawal on ajoneuvon matkamittarin lukema silloin, kun kortti poistettiin.

previousVehicleInfo sisältää tietoja edellisestä kuljettajan käyttämästä ajoneuvosta siinä muodossa kuin ne on tallennettu kortille.

manualInputFlag on erote, joka ilmaisee, onko kortin haltija kortin paikoilleen asettamisen yhteydessä syöttänyt kuljettajan toimintaa koskevia tietoja käsin.

2.121 VuCertificate

Ajoneuvoyksikön julkisen avaimen varmenne.

```
VuCertificate ::= Certificate
```

2.122 VuCompanyLocksData

Ajoneuvoyksikköön tallennetut tiedot, jotka liittyvät yrityksen tekemiin lukituksiin (vaatimus 104).

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

noOfLocks on vuCompanyLocksRecords-tietueissa lueteltujen lukitusten määrä.

vuCompanyLocksRecords on sarja tietueita, jotka sisältävät yrityksen tekemiin lukituksiin liittyviä tietoja.

2.123 VuCompanyLocksRecord

Ajoneuvoyksikköön tallennetut tiedot, jotka liittyvät yksittäiseen yrityksen tekemään lukitukseen (vaatimus 104).

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

lockInTime, **lockOutTime** ovat päivämäärä ja aika, jolloin lukitus tehtiin ja avattiin.

companyName, **companyAddress** ovat lukitukseen liittyvän yrityksen nimi ja osoite.

companyCardNumber yksilöi lukituksessa käytetyn kortin.

2.124 VuControlActivityData

Ajoneuvoyksikköön tallennetut tiedot, jotka liittyvät tätä ajoneuvoyksikköä käytettäessä suoritettuihin tarkastuksiin (vaatimus 102).

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

noOfControls on vuControlActivityRecords-tietueissa lueteltujen tarkastusten määrä.

vuControlActivityRecords on sarja tarkastustoimiin liittyviä tietueita.

2.125 VuControlActivityRecord

Ajoneuvoyksikköön tallennetut tiedot, jotka liittyvät yksittäiseen tätä ajoneuvoyksikköä käytettäessä suoritettuun tarkastukseen (vaatimus 102).

```
VuControlActivityRecord ::= SEQUENCE {
    controlType                ControlType,
    controlTime                TimeReal,
    controlCardNumber          FullCardNumber,
    downloadPeriodBeginTime    TimeReal,
    downloadPeriodEndTime      TimeReal
}
```

controlType on tarkastuksen tyyppi.

controlTime on päivämäärä ja aika, jolloin tarkastus suoritettiin.

ControlCardNumber yksilöi valvontakortin, jota tarkastuksessa käytettiin.

downloadPeriodBeginTime on tietojen kopioinnin päättymisaika, jos kopiointia tapahtui.

downloadPeriodEndTime on tietojen kopioinnin alkamisaika, jos kopiointia tapahtui.

2.126 VuDataBlockCounter

Kortille tallennettu laskuri, joka yksilöi järjestyksessä kortin ajoneuvoyksiköihin asettamis- ja poistamisjaksot.

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

Asetettava arvo: Juokseva numero, jonka maksimiarvo on 9 999, minkä jälkeen se alkaa jälleen nolasta.

2.127 VuDetailedSpeedBlock

Ajoneuvoyksikköön tallennetut yksityiskohtaiset tiedot, jotka liittyvät ajoneuvon nopeuteen niinä minuutteina, jolloin se on ollut liikkeellä (vaatimus 093).

```
VuDetailedSpeedBlock ::= SEQUENCE {
    speedBlockBeginDate          TimeReal,
    speedsPerSecond              SEQUENCE SIZE (60) OF Speed
}
```

speedBlockBeginDate on osion ensimmäisen nopeusarvon päivämäärä ja aika.

speedsPerSecond sarja aikajärjestyksessä olevia sekunnin välein mitattuja nopeuksia, jotka liittyvät speedBlockBeginDate-muuttujan ilmaisemalla hetkellä alkaneeseen minuuttiin (kyseinen hetki mukaan lukien).

2.128 VuDetailedSpeedData

Ajoneuvoyksikköön tallennetut yksityiskohtaiset tiedot, jotka liittyvät ajoneuvon nopeuteen.

```
VuDetailedSpeedData ::= SEQUENCE
    noOfSpeedBlocks              INTEGER (0..216-1),
    vuDetailedSpeedBlocks        SET SIZE (noOfSpeedBlocks) OF
    VuDetailedSpeedBlock
}
```

noOfSpeedBlocks on vuDetailedSpeedBlocks-tietuesarjan sisältämien nopeustietueosioiden määrä.

vuDetailedSpeedBlocks on sarja tietueosioita, jotka sisältävät yksityiskohtaisia tietoja ajoneuvon nopeudesta.

2.129 VuDownloadablePeriod

Aikaisin ja viimeisin päivämäärä, jota koskevia kuljettajan toimiin liittyviä tietoja ajoneuvoyksikössä on tallennettuna (vaatimus 081, 084 tai 087).

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

minDownloadableTime on aikaisin kortin paikoilleen asettamiseen tai toiminnan muutokseen tai paikkaan liittyvä päivämäärä- ja aikatieto, joka on tallennettuna ajoneuvoyksikköön.

maxDownloadableTime on viimeisin kortin poistamiseen tai toiminnan muutokseen tai paikkaan liittyvä päivämäärä- ja aikatieto, joka on tallennettuna ajoneuvoyksikköön.

2.130 VuDownloadActivityData

Ajoneuvoyksikköön tallennetut tiedot, jotka liittyvät viimeksi tapahtuneeseen sen tietojen kopiointiin (vaatimus 105).

```
VuDownloadActivityData ::= SEQUENCE {
    downloadingTime              TimeReal,
    fullCardNumber               FullCardNumber,
    companyOrWorkshopName        Name
}
```

downloadingTime on päivämäärä ja aika, jolloin tiedot kopioitiin.

fullCardNumber yksilöi kortin, jonka oikeutta tietojen kopiointiin käytettiin.

companyOrWorkshopName on yrityksen tai korjaamon nimi.

2.131 VuEventData

Ajoneuvoyksikköön tallennetut tiedot, jotka liittyvät tapauksiin (vaatimus 094, paitsi ylinopeustapaukset).

```
VuEventData ::= SEQUENCE {
    noOfVuEvents                 INTEGER (0..255),
    vuEventRecords               SET SIZE (noOfVuEvents) OF VuEventRecord
}
```

noOfVuEvents on vuEventRecords-tietuesarjaan tallennettujen tapausten määrä.

vuEventRecords on sarja tapauksiin liittyviä tietueita.

2.132 VuEventRecord

Ajoneuvoyksikköön tallennetut tiedot, jotka liittyvät yksittäiseen tapaukseen (vaatimus 094, paitsi ylinopeustapaukset).

```
VuEventRecord ::= SEQUENCE {
    eventType                EventFaultType,
    eventRecordPurpose       EventFaultRecordPurpose,
    eventBeginTime           TimeReal,
    eventEndTime             TimeReal,
    cardNumberDriverSlotBegin FullCardNumber,
    cardNumberCodriverSlotBegin FullCardNumber,
    cardNumberDriverSlotEnd FullCardNumber,
    cardNumberCodriverSlotEnd FullCardNumber,
    similarEventsNumber      SimilarEventsNumber
}
```

eventType on tapauksen tyyppi.

eventRecordPurpose on syy, jonka vuoksi kyseinen tapaus on kirjattu.

eventBeginTime on päivämäärä ja aika, jolloin tapaus alkoi.

eventEndTime on päivämäärä ja aika, jolloin tapaus päättyi.

cardNumberDriverSlotBegin yksilöi kortin, joka oli kuljettajan korttiaukossa tapauksen alkaessa.

cardNumberCodriverSlotBegin yksilöi kortin, joka oli apukuljettajan korttiaukossa tapauksen alkaessa.

cardNumberDriverSlotEnd yksilöi kortin, joka oli kuljettajan korttiaukossa tapauksen päättyessä.

cardNumberCodriverSlotEnd yksilöi kortin, joka oli apukuljettajan korttiaukossa tapauksen päättyessä.

similarEventsNumber on kyseisenä päivänä sattuneiden vastaavien tapausten määrä.

Tätä tietueosiota voidaan käyttää kaikkien muiden paitsi ylinopeuksiin liittyvien tapausten kirjaamiseen.

2.133 VuFaultData

Ajoneuvoyksikköön tallennetut tiedot, jotka liittyvät vikoihin (vaatimus 096).

```
VuFaultData ::= SEQUENCE {
    noOfVuFaults             INTEGER(0..255),
    vuFaultRecords           SET SIZE(noOfVuFaults) OF VuFaultRecord
}
```

noOfVuFaults on vuFaultRecords-tietuesarjaan tallennettujen vikatapahtumien määrä.

vuFaultRecords on sarja vikatapahtumiin liittyviä tietueita.

2.134 VuFaultRecord

Ajoneuvoyksikköön tallennetut tiedot, jotka liittyvät yksittäiseen vikatapahtumaan (vaatimus 096).

```
VuFaultRecord ::= SEQUENCE {
    faultType                EventFaultType,
    faultRecordPurpose       EventFaultRecordPurpose,
    faultBeginTime           TimeReal,
    faultEndTime             TimeReal,
    cardNumberDriverSlotBegin FullCardNumber,
    cardNumberCodriverSlotBegin FullCardNumber,
    cardNumberDriverSlotEnd FullCardNumber,
    cardNumberCodriverSlotEnd FullCardNumber
}
```

faultType on valvontalaitteen vian tyyppi.

faultRecordPurpose on syy, jonka vuoksi kyseinen vikatapahtuma on kirjattu.

faultBeginTime on päivämäärä ja aika, jolloin vikatapahtuma alkoi.

faultEndTime on päivämäärä ja aika, jolloin vikatapahtuma päättyi.

cardNumberDriverSlotBegin yksilöi kortin, joka oli kuljettajan korttiaukossa vikatapahtuman tapauksen alkaessa.

cardNumberCodriverSlotBegin yksilöi kortin, joka oli apukuljettajan korttiaukossa vikatapahtuman tapauksen alkaessa.

cardNumberDriverSlotEnd yksilöi kortin, joka oli kuljettajan korttiaukossa vikatapahtuman tapauksen päättyessä.

cardNumberCodriverSlotEnd yksilöi kortin, joka oli apukuljettajan korttiaukossa vikatapahtuman tapauksen päättyessä.

2.135 VuIdentification

Ajoneuvoyksikköön tallennetut tiedot, jotka liittyvät ajoneuvoyksikön tunnistukseen (vaatimus 075).

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

vuManufacturerName on ajoneuvoyksikön valmistajan nimi.

vuManufacturerAddress on ajoneuvoyksikön valmistajan osoite.

vuPartNumber on ajoneuvoyksikön osanumero.

vuSerialNumber on ajoneuvoyksikön sarjanumero.

vuSoftwareIdentification yksilöi ajoneuvoyksikössä käytettävän ohjelmiston.

vuManufacturingDate on ajoneuvoyksikön valmistuspäivä.

vuApprovalNumber on ajoneuvoyksikön tyyppihyväksyntänumero.

2.136 VuManufacturerAddress

Ajoneuvoyksikön valmistajan osoite.

```
VuManufacturerAddress ::= Address
```

Asetettava arvo: Ei määriteltä.

2.137 VuManufacturerName

Ajoneuvoyksikön valmistajan nimi.

```
VuManufacturerName ::= Name
```

Asetettava arvo: Ei määriteltä.

2.138 VuManufacturingDate

Ajoneuvoyksikön valmistuspäivä.

```
VuManufacturingDate ::= TimeReal
```

Asetettava arvo: Ei määriteltä.

2.139 VuOverSpeedingControlData

Ajoneuvoyksikköön tallennetut tiedot, jotka liittyvät viimeksi suoritettua ylinopeustarkastuksen jälkeen sattuneisiin ylinopeustapauksiin (vaatimus 095).

```
VuOverSpeedingControlData ::= SEQUENCE {
    lastOverspeedControlTime      TimeReal,
    firstOverspeedSince           TimeReal,
    numberOfOverspeedSince        OverspeedNumber
}
```

lastOverspeedControlTime on päivämäärä ja aika, jolloin ylinopeustarkastus viimeksi suoritettiin.

firstOverspeedSince on päivämäärä ja aika, jolloin ensimmäinen ylinopeustapaus sattui tämän ylinopeustarkastuksen jälkeen.

numberOfOverspeedSince on viimeisen ylinopeustarkastuksen jälkeen sattuneiden ylinopeustapausten määrä.

2.140 VuOverSpeedingEventData

Ajoneuvoyksikköön tallennetut tiedot, jotka liittyvät ylinopeustapauksiin (vaatimus 094).

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

noOfVuOverSpeedingEvents on vuOverSpeedingEventRecords-tietuesarjaan tallennettujen tapausten määrä.

vuOverSpeedingEventRecords on sarja ylinopeustapauksiin liittyviä tietueita.

2.141 VuOverSpeedingEventRecord

Ajoneuvoyksikköön tallennetut tiedot, jotka liittyvät ylinopeustapauksiin (vaatimus 094).

```
VuOverSpeedingEventRecord ::= SEQUENCE {
    eventType                     EventFaultType,
    eventRecordPurpose            EventFaultRecordPurpose,
    eventBeginTime                TimeReal,
    eventEndTime                  TimeReal,
    maxSpeedValue                 SpeedMax,
    averageSpeedValue             SpeedAverage,
    cardNumberDriverSlotBegin     FullCardNumber,
    similarEventsNumber           SimilarEventsNumber
}
```

eventType on tapauksen tyyppi.

eventRecordPurpose on syy, jonka vuoksi kyseinen tapaus on kirjattu.

eventBeginTime on päivämäärä ja aika, jolloin tapaus alkoi.

eventEndTime on päivämäärä ja aika, jolloin tapaus päättyi.

maxSpeedValue on suurin tapauksen aikana mitattu nopeus.

averageSpeedValue on tapauksen aikana mitattujen nopeuslukemien aritmeettinen keskiarvo.

cardNumberDriverSlotBegin yksilöi kortin, joka oli kuljettajan korttiaukossa tapauksen alkaessa.

similarEventsNumber on kyseisenä päivänä sattuneiden vastaavien tapausten määrä.

2.142 VuPartNumber

Ajoneuvoyksikön osanumero.

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

Asetettava arvo: Arvo määrittyy ajoneuvoyksikön valmistajan mukaan.

2.143 VuPlaceDailyWorkPeriodData

Ajoneuvoyksikköön tallennetut tiedot, jotka liittyvät paikkoihin, joissa kuljettajan päivän työaika alkaa tai päättyy (vaatimus 087).

```
VuPlaceDailyWorkPeriodData ::= SEQUENCE {  
    noOfPlaceRecords                INTEGER(0..255),  
    vuPlaceDailyWorkPeriodRecords   SET SIZE(noOfPlaceRecords) OF  
                                     VuPlaceDailyWorkPeriodRecord  
}
```

noOfPlaceRecords on vuPlaceDailyWorkPeriodRecords-tietuesarjaan tallennettujen tietueiden määrä.

vuPlaceDailyWorkPeriodRecords on sarja paikkaan liittyviä tietoja sisältäviä tietueita.

2.144 VuPlaceDailyWorkPeriodRecord

Ajoneuvoyksikköön tallennetut tiedot, jotka liittyvät yksittäiseen paikkaan, jossa kuljettajan päivän työaika alkaa tai päättyy (vaatimus 087).

```
VuPlaceDailyWorkPeriodRecord ::= SEQUENCE {  
    fullCardNumber                   FullCardNumber,  
    placeRecord                       PlaceRecord  
}
```

fullCardNumber kuljettajan kortin tyyppi, kortin myöntänyt jäsenvaltio ja kortin numero.

placeRecord sisältää syötettyyn paikkaan liittyvät tiedot.

2.145 VuPrivateKey

Ajoneuvoyksikön yksityinen avain.

```
VuPrivateKey ::= RSAKeyPrivateExponent
```

2.146 VuPublicKey

Ajoneuvoyksikön julkinen avain.

```
VuPublicKey ::= PublicKey
```

2.147 VuSerialNumber

Ajoneuvoyksikön sarjanumero (vaatimus 075).

```
VuSerialNumber ::= ExtendedSerialNumber
```

2.148 VuSoftInstallationDate

Päivämäärä, jolloin ajoneuvoyksikön ohjelmistoversio asennettiin.

```
VuSoftInstallationDate ::= TimeReal
```

Asetettava arvo: Ei määritely.

2.149 VuSoftwareIdentification

Ajoneuvoyksikköön tallennetut tiedot, jotka liittyvät asennettuun ohjelmistoon.

```
VuSoftwareIdentification ::= SEQUENCE {  
    vuSoftwareVersion                 VuSoftwareVersion,  
    vuSoftInstallationDate           VuSoftInstallationDate  
}
```

vuSoftwareVersion on ajoneuvoyksikön ohjelmistoversion numero.

vuSoftInstallationDate on päivämäärä, jolloin ohjelmistoversio asennettiin.

2.150 VuSoftwareVersion

Ajoneuvoyksikön ohjelmistoversion numero.

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

Asetettava arvo: Ei määritelty.

2.151 VuSpecificConditionData

Ajoneuvoyksikköön tallennetut tiedot, jotka liittyvät erityisolosuhteisiin.

```
VuSpecificConditionData ::= SEQUENCE {
    noOfSpecificConditionRecords          INTEGER(0..216-1)
    specificConditionRecords              SET SIZE (noOfSpecificConditionRecords) OF
                                           SpecificConditionRecord
}
```

noOfSpecificConditionRecords on specificConditionRecords-tietuesarjaan tallennettujen tietueiden määrä.

specificConditionRecords on sarja erityisolosuhteisiin liittyviä tietoja sisältäviä tietueita.

2.152 VuTimeAdjustmentData

Ajoneuvoyksikköön tallennetut tiedot, jotka liittyvät ajan asettamistapahtumiin muulloin kuin tavanomaisen kalibroinnin yhteydessä (vaatimus 101).

```
VuTimeAdjustmentData ::= SEQUENCE {
    noOfVuTimeAdjRecords                  INTEGER(0..6),
    vuTimeAdjustmentRecords              SET SIZE (noOfVuTimeAdjRecords) OF
                                           VuTimeAdjustmentRecord
}
```

noOfVuTimeAdjRecords on vuTimeAdjustmentRecords-tietuesarjaan tallennettujen tietueiden määrä.

vuTimeAdjustmentRecords on sarja ajan asettamisiin liittyviä tietoja sisältäviä tietueita.

2.153 VuTimeAdjustmentRecord

Ajoneuvoyksikköön tallennetut tiedot, jotka liittyvät yksittäiseen ajan asettamistapahtumaan muulloin kuin tavanomaisen kalibroinnin yhteydessä (vaatimus 101).

```
VuTimeAdjustmentRecord ::= SEQUENCE {
    oldTimeValue                          TimeReal,
    newTimeValue                          TimeReal,
    workshopName                          Name,
    workshopAddress                       Address,
    workshopCardNumber                    FullCardNumber
}
```

oldTimeValue, **newTimeValue** ovat päivämäärän ja ajan vanhat ja uudet arvot.

workshopName, **workshopAddress** ovat korjaamon nimi ja osoite.

workshopCardNumber yksilöi ajan asettamisessa käytetyn korjaamokortin.

2.154 W-VehicleCharacteristicConstant

Ajoneuvon ominaiskerroin (määritelmä k).

```
W-VehicleCharacteristicConstant ::= INTEGER(0..216-1)
```

Asetettava arvo: Impulsseja kilometriä kohden alueella 0–64 255 impulssia/km.

2.155 WorkshopCardApplicationIdentification

Korjaamokortille tallennetut tiedot, jotka liittyvät kortilla olevan sovelluksen tunnistukseen (vaatimus 190).

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

typeOfTachographCardId määrittää kortin tunnisteiden tyyppiä.

cardStructureVersion määrittelee kortilla käytetyn datarakenteen version.

noOfEventsPerType on niiden tapauksien määrä tapaustyyppiä kohden, jotka voidaan tallentaa kortille.

noOfFaultsPerType on niiden vikatapahtumien määrä vikatyyppiä kohden, jotka voidaan tallentaa kortille.

activityStructureLength osoittaa niiden tavujen määrän, jotka ovat käytettävissä toimintaan liittyvien tietojen tallentamiseen.

noOfCardVehicleRecords on niiden ajoneuvoon liittyviä tietoja sisältävien tietueiden määrä, jotka voidaan tallentaa kortille.

noOfCardPlaceRecords on niiden paikkoihin liittyviä tietoja sisältävien tietueiden määrä, jotka voidaan tallentaa kortille.

noOfCalibrationRecords on niiden kalibrointiin liittyviä tietoja sisältävien tietueiden määrä, jotka voidaan tallentaa kortille.

2.156 WorkshopCardCalibrationData

Korjaamokortille tallennetut tiedot, jotka liittyvät kortilla suoritettuihin korjaamon toimiin (vaatimukset 227 ja 229).

```
WorkshopCardCalibrationData ::= SEQUENCE {
    calibrationTotalNumber           INTEGER(0..216-1),
    calibrationPointerNewestRecord   INTEGER(0..NoOfCalibrationRecords-1),
    calibrationRecords               SET SIZE(NoOfCalibrationRecords) OF
                                     WorkshopCardCalibrationRecord
}
```

calibrationTotalNumber on kaikkien korttia käyttäen suoritettujen kalibrointiin määrän.

calibrationPointerNewestRecord on viimeksi päivitetyn kalibrointiin liittyvän tietueen järjestysnumero.

Asetettava arvo: Numero, joka vastaa kalibrointiin liittyvän tietueen järjestysnumeroa, alkaen numerosta '0' ensimmäiselle kalibrointiin liittyvälle tietueelle datarakenteessa.

calibrationRecords on sarja tietueita, joissa on kalibrointiin ja/tai ajan asetukseen liittyviä tietoja.

2.157 WorkshopCardCalibrationRecord

Korjaamokortille tallennetut tiedot, jotka liittyvät yksittäiseen korttia käyttäen suoritettuun kalibrointiin (vaatimus 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 on syy, jonka vuoksi kalibrointi suoritettiin.

vehicleIdentificationNumber on ajoneuvon valmistenumero (VIN).

vehicleRegistration sisältää ajoneuvon rekisteritunnuksen (VRN) ja ajoneuvon rekisteröineen jäsenvaltion.

wVehicleCharacteristicConstant on ajoneuvon ominaiskerroin.

kConstantOfRecordingEquipment on valvontalaitteen vakio.

ITyreCircumference on pyörien renkaiden tehollinen ympärysmitta.

tyreSize on ajoneuvon asennettujen renkaiden kokomerkintä.

authorisedSpeed on ajoneuvon suurin sallittu nopeus.

oldOdometerValue, **newOdometerValue** ovat matkamittarin vanha ja uusi lukema.

oldTimeValue, **newTimeValue** ovat päivämäärän ja ajan vanhat ja uudet arvot.

nextCalibrationDate on päivämäärä, jolloin valtuutetun tarkastusviranomaisen on suoritettava seuraava CalibrationPurpose-muuttujan määrittelemä kalibrointi.

vuPartNumber, **vuSerialNumber** ja **sensorSerialNumber** ovat valvontalaitteen tunnistuksessa käytettävät dataelementit.

2.158 WorkshopCardHolderIdentification

Korjaamokortille tallennetut tiedot, jotka liittyvät kortin haltijan tunnistukseen (vaatimus 216).

```
WorkshopCardHolderIdentification ::= SEQUENCE {
    workshopName                Name,
    workshopAddress              Address,
    cardHolderName               HolderName,
    cardHolderPreferredLanguage  Language
}
```

workshopName on sen korjaamon nimi, jossa kortin haltija työskentelee.

workshopAddress on sen korjaamon osoite, jossa kortin haltija työskentelee.

cardHolderName on kortin haltijan (esim. mekaanikon) nimi ja etunimi (etunimet).

cardHolderPreferredLanguage on kortin haltijan ensisijaisesti käyttämä kieli.

2.159 WorkshopCardPIN

Korjaamokortin henkilökohtainen tunnusluku (vaatimus 213).

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

Asetettava arvo: Kortin haltijan tiedossa oleva henkilökohtainen tunnusluku, jonka perään tarvittaessa lisätään arvoltaan FFh olevia tavuja siten, että kokonaistavumääräksi tulee kahdeksan.

3. ARVOALUEIDEN MÄÄRITTELYT

Kohdassa 2 määriteltyjen muuttujien arvojen määrittely.

TimeRealRange ::= 2³²-1

3.1 Kuljettajakorttia koskevat määrittelyt:

Muuttujan nimi	Pienin arvo	Suurin arvo
CardActivityLengthRange	5 544 tavua (28 päivää, 93 toiminnan muutosta päivässä)	13 776 tavua (28 päivää, 240 toiminnan muutosta päivässä)
NoOfCardPlaceRecords	84	112
NoOfCardVehicleRecords	84	200
NoOfEventsPerType	6	12
NoOfFaultsPerType	12	24

3.2 Korjaamokorttia koskevat määrittelyt:

Muuttujan nimi	Pienin arvo	Suurin arvo
CardActivityLengthRange	198 tavua (1 päivä, 93 toiminnan muutosta)	492 tavua (1 päivä, 240 toiminnan muutosta)
NoOfCardPlaceRecords	6	8
NoOfCardVehicleRecords	4	8
NoOfEventsPerType	3	3
NoOfFaultsPerType	6	6
NoOfCalibrationRecords	88	255

3.3 Valvontakorttia koskevat määrittelyt:

Muuttujan nimi	Pienin arvo	Suurin arvo
NoOfControlActivityRecords	230	520

3.4 Yrityskorttia koskevat määrittelyt:

Muuttujan nimi	Pienin arvo	Suurin arvo
NoOfCompanyActivityRecords	230	520

4. MERKISTÖT

IA5 (International Alphabet 5) -merkkijonoissa käytetään standardin ISO/IEC 8824-1 mukaisia ASCII-merkkejä. Selvyyden vuoksi ja avuksi on kyseiset merkit näytetty alla. Ristiriitapauksissa on standardin ISO/IEC 8824-1 sisältö ratkaiseva.

```
! " # $ % & ' ( ) * + , - . / 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 { | } ~
```

Muissa merkkijonoissa (Address, Name, VehicleRegistrationNumber) käytetään lisäksi standardin ISO/IEC 8859-1 (latinalaisaakkosto nro 1) koodeja 192-255 vastaavia tai standardin ISO/IEC 8859-7 (kreikkalaisaakkosto) merkkejä.

5. KOODAUS

Kun koodataan ASN.1-merkintätavan koodaussääntöjä käyttäen, kaikki datatyypit on koodattava standardin ISO/IEC 8825-2 aligned-vaihtoehdon mukaisesti.

Lisäys 2

AJOPIIRTURIKORTTIEN ERITTELY

SISÄLLYSLUETTELO

1.	Johdanto	99
1.1	Lyhenteet	99
1.2	Viitetiedot	100
2.	Sähköiset ja mekaaniset ominaisuudet	100
2.1	Käyttöjännite ja virrankulutus	100
2.2	Ohjelmointijännite V_{pp}	101
2.3	Kellopulssin synnyttäminen ja kelloaajuus	101
2.4	I/O-liitin	101
2.5	Kortin toimintatilat	101
3.	Laitteisto ja viestintä	101
3.1	Johdanto	101
3.2	Lähetysprotokolla	101
3.2.1	Protokollat	101
3.2.2	ATR-signaali	102
3.2.3	PTS-komento	103
3.3	Käyttöehdot (AC)	103
3.4	Tietojen salaus	104
3.5	Komentojen ja virhekoodien tiivistelmä	104
3.6	Komentojen kuvaus	105
3.6.1	SELECT FILE	105
3.6.1.1	Valinta nimen (AID) perusteella	105
3.6.1.2	EF-tiedoston valinta sen tiedostotunnisteen perusteella	106
3.6.2	READ BINARY	106
3.6.2.1	Komento ilman salattua sanomanvälitystä	107
3.6.2.2	Komento salattua sanomanvälitystä käyttäen	107
3.6.3	UPDATE BINARY	109
3.6.3.1	Komento ilman salattua sanomanvälitystä	109
3.6.3.2	Komento salattua sanomanvälitystä käyttäen	110
3.6.4	GET CHALLENGE	111
3.6.5	VERIFY	111
3.6.6	GET RESPONSE	112
3.6.7	PSO: VERIFY CERTIFICATE	112
3.6.8	INTERNAL AUTHENTICATE	113

3.6.9	EXTERNAL AUTHENTICATE	114
3.6.10	MANAGE SECURITY ENVIRONMENT	115
3.6.11	PSO: HASH	116
3.6.12.	PERFORM HASH OF FILE	116
3.6.13	PSO: COMPUTE DIGITAL SIGNATURE	117
3.6.14	PSO: VERIFY DIGITAL SIGNATURE	118
4.	Ajopiirturikorttien tiedostorakenne	118
4.1	Kuljettajakortin tiedostorakenne	119
4.2	Korjaamokortin tiedostorakenne	121
4.3	Valvontakortin tiedostorakenne	123
4.4	Yrityskortin tiedostorakenne	125

1. JOHDANTO

1.1 Lyhenteet

Tässä lisäyksessä käytetään seuraavia lyhenteitä:

AC	(Access conditions) Käyttöehdot
AID	(Application Identifier) Sovellustunniste
ALW	(Always) ALW-ehto; Aina
APDU	(Application protocol data unit) APDU-rakenne; Sovelluserroksen tietoyksikkö
ATR	(Answer to reset) ATR-signaali; Signaali, joka annetaan vastauksena RST-komentoon
AUT	(Authenticated) AUT-ehto; Alkuperä todennettu
C6, C7	Standardin ISO/IEC 7816-2 mukaiset kortin liittimet N:o 6 ja 7
cc	(clock cycles) Kellopulssi(a)
CHV	(Card holder verification information) Kortin haltijan kontrollitiedot
CLA	APDU-komennon luokkaa ilmaiseva tavu
DF	(Dedicated Tiedosto) DF-tiedosto eli hakemistotiedosto. DF-tiedosto voi sisältää muita (EF- tai DF-) tiedostoja
EF	(Elementary Tiedosto) EF-tiedosto tiedosto, jossa varsinaiset tiedot säilytetään
ENC	Salattu: käyttö mahdollista vain salaukseen käytetyn datan avulla
etu	(elementary time unit) Ajan perusyksikkö
IC	(Integrated circuit) Integroitu piiri
ICC	(Integrated circuit card) Integroidulla piirillä varustettu kontaktillinen kortti
ID	(Identifier) Tunniste
IFD	(Interface device) Liitäntälaitte
IFS	(Information field size) Tietokentän koko
IFSC	Kortin tietokentän koko
IFSD	Laitteen (päätelaitteen) tietokentän koko
INS	APDU-komennon käskytavu
Lc	APDU-komennolla annettavan datan pituus
Le	Vastauksena odotettavan datan pituus (komennon vastauksena saatava data)
MF	(Master Tiedosto) MF-tiedosto; Root-tason hakemistotiedosto
P1-P2	Parametritavuja
NAD	(Node address) T=1-protokollassa käytettävä solmun osoite
NEV	(Never) NEV-ehto; Ei koskaan
PIN	Henkilökohtainen tunnusluku
PRO SM	(Protected with secure messaging) PRO SM -ehto; Salattu viesti
PTS	(Protocol transmission selection) PTS-komento; Lähetysprotokollan valinta)
RFU	Varattu tulevaan käyttöön

RST	Reset (of the card) RST-komento; (Kortin) alkutilaan palauttava komento
SM	(Secure messaging) Salattu sanomanvälitys
SW1-SW2	(Status bytes) Tilaa osoittavat tavut
TS	ATR-signaalin ensimmäinen merkki
VPP	Ohjelmointijännite
XXh	Heksadesimaaliluku XX
	Ketjutusmerkki; 03 04=0304

1.2 Viitetiedot

Tässä lisäyksessä käytetään seuraavia viitteitä:

EN 726-3	Identification cards systems – Telecommunications integrated circuit(s) cards and terminals – Part 3: Application independent card requirements. December 1994 (Henkilökorttijärjestelmät. Tietoliikenteessä käytettävät integroidulla piirillä varustetut kontaktilliset kortit. Osa 3: Sovelluksesta riippumattomien korttien vaatimukset. Joulukuu 1994)
ISO/CEI 7816-2	Information technology – Identification cards – Integrated circuit(s) cards with contacts – Part 2: Dimensions and location of the contacts. First edition: 1999 (Tietotekniikka. Henkilökortit. Integroidulla piirillä varustetut kontaktilliset kortit. Osa 2: Mitat ja liittimien paikat. Ensimmäinen painos: 1999)
ISO/CEI 7816-3	Information technology – Identification cards – Integrated circuit(s) cards with contacts – Part 3: Electronic signals and transmission protocol. Edition 2: 1997 (Tietotekniikka. Henkilökortit. Integroidulla piirillä varustetut kontaktilliset kortit. Osa 3: Sähköiset signaalit ja siirtoprotokollat. Toinen painos: 1997)
ISO/CEI 7816-4	Information technology – Identification cards – Integrated circuit(s) cards with contacts – Part 4: Interindustry commands for interexchange. First edition: 1995 + Amendment 1: 1997 (Tietotekniikka. Henkilökortit. Integroidulla piirillä varustetut kontaktilliset kortit. Osa 4: Yleiset siirtokomennot. Ensimmäinen painos: 1995, ensimmäinen muutos: 1997)
ISO/CEI 7816-6	Information technology – Identification cards – Integrated circuit(s) cards with contacts – Part 6: Interindustry data elements. First Edition: 1996 + Cor 1: 1998 (Tietotekniikka. Henkilökortit. Integroidulla piirillä varustetut kontaktilliset kortit. Osa 6: Yleiset dataelementit. Ensimmäinen painos: 1996, ensimmäinen korjaus: 1998)
ISO/CEI 7816-8	Information technology – Identification cards – Integrated circuit(s) cards with contacts – Part 8: Security related interindustry commands. First Edition: 1999 (Tietotekniikka. Henkilökortit. Integroidulla piirillä varustetut kontaktilliset kortit. Osa 8: Yleiset turvakomennot. Ensimmäinen painos: 1999)
ISO/CEI 9797	Information technology – Security techniques – Data integrity mechanism using a cryptographic check function employing a block cipher algorithm. Edition 2: 1994 (Tietotekniikka. Tietoturvatekniikat. Danan eheyden turvaamisen menettely, jossa käytetään lohkoittain tapahtuvan salauksen periaatteella toimivaa salakirjoituksen tarkistustoimintoa. Toinen painos: 1994)

2. SÄHKÖISET JA MEKAANISET OMINAISUUDET

TCS_200 Kaikkien sähköisten signaalien on oltava standardin ISO/IEC 7816-3 mukaisia, ellei muuta määrätä.

TCS_201 Kortin liittimien paikkojen ja mittojen on oltava standardin ISO/IEC 7816-2 mukaiset.

2.1 Käyttöjännite ja virrankulutus

TCS_202 Kortin on toimittava erittelyjen mukaisesti siten, että sen kulutus on standardissa ISO/IEC 7816-3 määritellyissä rajoissa.

TCS_203 Kortin on toimittava jännitteellä $V_{cc} = 3 \text{ V (+/- } 0,3 \text{ V)}$ tai jännitteellä $V_{cc} = 5 \text{ V (+/- } 0,5 \text{ V)}$.

Jännitteen valinnan on tapahduttava standardin ISO/IEC 7816-3 mukaisesti.

2.2 Ohjelmointijännite V_{pp}

TCS_204 Kortti ei saa tarvita ohjelmointijännitettä liittimelle C6. Liittimen C6 ei oleteta olevan kytkettynä liitäntälaitteessa. Kortin liitin C6 voidaan kytkeä jännitteeseen V_{CC} , mutta sitä ei saa kytkeä maahan. Liittimellä olevaa jännitettä ei kuitenkaan saa ottaa huomioon.

2.3 Kellopulssin synnyttäminen ja kellotaajuus

TCS_205 Kortin on toimittava taajuusalueella 1–5 MHz. Yhden kortin käyttöjakson aikana kellotaajuus saa vaihdella 2 %. Kellotaajuus synnytetään ajoneuvoyksikössä eikä itse kortilla. Pulssileveyden suhde pulssiväliin saa vaihdella rajoissa 40–60 %.

TCS_206 Kortin EF_{ICC} -tiedoston sisältämällä ehdoilla ulkoinen kello voidaan pysäyttää. EF_{ICC} -tiedoston ensimmäinen tavu määrää Clockstop-tilan ehdot (lisätietoja standardissa EN 726-3):

(Kellopulssi) 0	(Kellopulssi) 1		
Bitti 3	Bitti 2	Bitti 1	
0	0	1	Clockstop-tila sallittu, looginen taso ei merkitsevä
0	1	1	Clockstop-tila sallittu, looginen taso 1 etusijalla
1	0	1	Clockstop-tila sallittu, looginen taso 0 etusijalla
0	0	0	Clockstop-tila ei sallittu
0	1	0	Clockstop-tila sallittu vain loogisen tason ollessa 1
1	0	0	Clockstop-tila sallittu vain loogisen tason ollessa 0

Bitit 4–8 eivät ole käytössä.

2.4 I/O-liitin

TCS_207 I/O-liitin C7 vastaanottaa ja siltä lähetetään dataa liitäntälaitteelle. Korttia käytettäessä saa vain joko kortti tai liitäntälaitte olla lähetystilassa. Kortti ei kuitenkaan saa vahingoittua, vaikka molemmat olisivatkin lähetystilassa. Kortin on siirryttävä vastaanottotilaan aina, kun se ei lähetä dataa.

2.5 Kortin toimintatilat

TCS_208 Käyttöjännitteen ollessa kytkettynä kortilla on kaksi toimintatilaa:

- käyttötila, jossa kortti on suorittaessaan komentoja tai ollessaan yhteydessä ajoneuvoyksikön kanssa,
- lepotila, jossa kortti on aina muulloin; tässä tilassa kortin on säilytettävä kaikki sillä oleva data.

3. LAITTEISTO JA VIESTINTÄ

3.1 Johdanto

Tässä kohdassa kuvataan ne toiminnot, jotka ajopiirturikorteilta ja ajoneuvoyksiköiltä vähintään vaaditaan, jotta ne toimisivat oikein ja yhdessä.

Ajopiirturikortit ovat olemassa olevien ISO/IEC-standardien (erityisesti standardin ISO/IEC 7816) mukaisia niin paljon kuin mahdollista. Komennot ja protokollat on kuitenkin kuvattu täysin, jotta eräät käyttörajoitukset tai erot, mikäli niitä on, tulisivat määritellyiksi. Määritellyt komennot ovat täysin mainittujen standardien mukaisia paitsi tapauksissa, jotka on erikseen osoitettu.

3.2 Lähetysprotokolla

TCS_300 Lähetysprotokollan on oltava standardin ISO/IEC 7816-3 mukainen. Erityisesti ajoneuvoyksikön on tunnistettava kortin lähettämät odotusajan pidennykset.

3.2.1 Protokollat

TCS_301 Kortin on kyettävä käyttämään sekä T=0-protokollaa että T=1-protokollaa.

- TCS_302 T=0 on oletusarvoinen protokolla, minkä vuoksi PTS (lähetyksen protokollan valinta) -komento tarvitaan vaihtamaan käytettäväksi protokollaksi T=1.
- TCS_303 Laitteiden on tuettava suoraa koodaustapaa (direct convention) molemmissa protokollissa; suora koodaustapa on näin ollen pakollinen kortille.
- TCS_304 information field size card (kortin tietokentän koko) -tavun tulee olla ATR-signaalin merkissä TA3. Tavun arvon on oltava vähintään 'F0h' (= 240 tavua).

Protokollia koskevat seuraavat rajoitukset:

- TCS_305 T=0
- Liitäntälaitteen on kyettävä ottamaan vastaus I/O-liittimelle 400 kellopulssin kuluessa RST-signaalin etureunasta.
 - Liitäntälaitteen on kyettävä lukemaan merkkejä 12 etu-yksikön (perusaikayksikön) välein.
 - Liitäntälaitteen on luettava virheellinen merkki ja sen toisto, jos niiden välillä on 13 etu-yksikköä. Jos virheellinen merkki havaitaan, Error (virhe) -signaali voidaan antaa I/O-liittimelle 1 ja 2 etu-yksikön välillä. Laitteen on tuettava 1 etu-yksikön viivettä.
 - Liitäntälaitteen on hyväksyttävä 33-tavuinen ATR-signaali (TS (ensimmäinen merkki) + 32).
 - Jos ATR-signaalissa on merkki TC1, liitäntälaitteen lähettämille merkeille on annettava ylimääräinen varoaika, vaikka kortin lähettämät merkit voidaan silti erottaa 12 etu-yksiköllä. Tämä pätee myös kortin lähettämään ACK-merkkiin liitäntälaitteen lähettämän P3-merkin jälkeen.
 - Liitäntälaitteen on otettava huomioon kortin lähettämä NUL-merkki.
 - Liitäntälaitteen on hyväksyttävä ACK-merkin antaminen vastakkaisvaiheisena (complementary mode).
 - GET RESPONSE -komentoa ei voida käyttää chaining mode (ketjutus) -tilassa hakemaan dataa, jonka pituus saattaa ylittää 255 tavua.

- TCS_306 T=1
- NAD (solmun osoite) -tavu: ei käytössä (NAD-tavun arvoksi on asetettava '00').
 - S-lohkon ABORT-komento: ei käytössä.
 - S-lohkon VPP-tilan virheilmoitus: ei käytössä.
 - Tietokentän ketjutettu pituus ei saa ylittää 255:tä tavua (liitäntälaitteen varmistettava).
 - Liitäntälaitteen on annettava information field size device (IFSD) (laitteen tietokentän koko) -arvo heti ATR-signaalin jälkeen: Liitäntälaitteen on lähetettävä S-lohkon IFS (tietokentän koko) -pyyntö ATR-signaalin jälkeen ja kortin on lähetettävä takaisin S-lohkon IFS-tieto. IFSD:n suositeltava arvo on 254 tavua.
 - Kortti ei pyydä IFS-koon muuttamista.

3.2.2 ATR-signaali

- TCS_307 Laite tarkastaa ATR-signaalin tavut standardin ISO/IEC 7816-3 mukaisesti. ATR-signaaliin sisältyviä merkkejä, jotka liittyvät kortin historiaan (historical characters), ei todenneta.

Esimerkki kahta protokollaa tukevasta ATR-perussignaalistista standardin ISO/IEC 7816-3 mukaisesti

Merkki	Arvo	Huomautuksia
TS	'3Bh'	Osoittaa suoraa koodaustapaa
T0	'85h'	TD1-merkki mukana; mukana on 5 kortin historiaan liittyvää tavua
TD1	'80h'	TD2-merkki mukana; käytetään T=0-protokollaa
TD2	'11h'	TA3-merkki mukana; käytetään T=1-protokollaa
TA3	'XXh' (vähintään 'F0h')	Kortin tietokentän koko (IFSC)
TH1-TH5	'XXh'	Kortin historiaan liittyvät merkit
TCK	'XXh'	Tarkistusmerkki (XOR)

TCS_308 ATR-signaalin jälkeen valitaan MF-tiedosto automaattisesti oletushakemistoksi.

3.2.3 PTS-komento

TCS_309 Oletusarvoinen protokolla on T=0. T=1-protokollan valitsemiseksi on kortin lähetettävä laitteelle PTS-komento (tunnetaan myös nimellä PPS-komento).

TCS_310 Koska kortin on tuettava sekä T=0- että T=1-protokollia, sen on myös tuettava PTS (protokollan vaihto) -perustoimintoa.

Kuten standardista ISO/IEC 7816-3 ilmenee, PTS-komentoa voidaan käyttää muuttamaan siirtonopeus suuremmaksi kuin kortin ATR-signaalissa mahdollisesti (TA(1)-tavussa) ehdottama.

Suurempien siirtonopeuksien tuki kortilla on valinnainen ominaisuus.

TCS_311 Jos kortti ei tue muita kuin oletusarvoista siirtonopeutta (tai jos se ei tue valittua siirtonopeutta), kortin on vastattava PTS-komentoon standardin ISO/IEC 7816-3 mukaisesti jättämällä PPS1-tavu pois.

Seuraavassa on esimerkkejä PTS-peruskomennosta protokollan valitsemiseksi:

Merkki	Arvo	Huomautuksia
PPSS	'FFh'	Käynnistysmerkki
PPS0	'00h' tai '01h'	Tavut PPS1-PPS3 eivät ole mukana; '00h' valitsee T0, '01h' valitsee T1-protokollan
PK	'XXh'	Tarkistusmerkki: 'XXh' = 'FFh' jos PPS0 = '00h', 'XXh' = 'FEh' jos PPS0 = '01h'

3.3 Käyttöehdot (AC)

UPDATE BINARY- ja READ BINARY -komentojen käyttöehdot on määriteltävä jokaiselle EF-tiedostolle.

TCS_312 Käytettävän tiedoston käyttöehdot on täytettävä, ennen kuin tiedostoa voidaan käyttää näillä komennoilla.

Käytettävissä olevien käyttöehtojen määritelmät ovat seuraavat:

- ALW: toiminto on aina mahdollinen ja voidaan toteuttaa ilman rajoituksia.
- NEV: toiminto ei ole koskaan mahdollinen.
- AUT: ulkoista todentamista vastaavat käyttöoikeudet on otettava käyttöön (tapahtuu EXTERNAL AUTHENTICATE -komennolla).
- PRO SM: komento on lähetettävä tarkistussumman kanssa käyttäen salattua sanomanvälitystä (ks. lisäys 11).
- AUT ja PRO SM (yhdessä).

Kortille voidaan asettaa seuraavat käyttöehdot käsittelykomennoille (UPDATE BINARY ja READ BINARY):

	UPDATE BINARY	READ BINARY
ALW	Kyllä	Kyllä
NEV	Kyllä	Kyllä
AUT	Kyllä	Kyllä
PRO SM	Kyllä	Ei
AUT ja PRO SM	Kyllä	Ei

READ BINARY -komennon yhteydessä ei voida käyttää PRO SM -ehtoa. Tämä tarkoittaa, että READ-komennon yhteydessä ei koskaan vaadita salaukseen liittyvää tarkistussummaa. Käyttämällä luokassa arvoa 'OC' on kuitenkin mahdollista käyttää READ BINARY -komentoa salatun sanomanvälityksen yhteydessä, kuten kohdassa 3.6.2 on kuvattu.

3.4 Tietojen salaus

Kun on tarpeen säilyttää tiedostosta luettavat tiedot salaisina, varustetaan tiedosto Encrypted (salattu) -merkinnällä. Salaus suoritetaan käyttämällä salattua sanomanvälitystä (ks. lisäys 11).

3.5 Komentojen ja virhekoodien tiivistelmä

Komennot ja tiedostorakenne on saatu standardista ISO/IEC 7816-4 ja ne ovat tämän standardin mukaisia.

TCS_313 Tässä osassa kuvataan seuraavia APDU-rakenteen komento-vastauspareja:

Komento	Käskytavu
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 Tilaa ilmaisevat tavut SW1 ja SW2 sisällytetään kaikkiin vastausviesteihin, ja ne osoittavat komennon suorittamisen tilan.

SW1	SW2	Tarkoitus
90	00	Normaali suoritus
61	XX	Normaali suoritus. XX = vastaukseen käytettävissä olevien tavujen määrä
62	81	Varoituksen suoritus. Osa palautettavista tiedoista on voinut tuhoutua
63	CX	Väärä CHV (PIN). 'X' on jäljellä olevien yrityskertojen laskuri
64	00	Toteutusvirhe. Haihtumattoman muistin tila muuttumaton. Virhe eheydessä
65	00	Toteutusvirhe. Haihtumattoman muistin tila muuttunut
65	81	Toteutusvirhe. Haihtumattoman muistin tila muuttunut – muistivirhe
66	88	Tietoturvakirje: väärä tarkistussumma (salatun sanomanvälityksen yhteydessä) tai väärä varmenne (varmenteen todennuksen yhteydessä) tai väärä kryptogrammi (ulkoisen todennuksen yhteydessä) tai väärä allekirjoitus (allekirjoituksen todennuksen yhteydessä)
67	00	Väärä pituus (väärä Lc tai Le)
69	00	Kielletty komento (protokollassa T=0 ei käytettävissä vastausta)
69	82	Tietoturvatilan vaatimuksia ei täytetty
69	83	Todennusmenetelmän käyttö estetty
69	85	Käyttöehtoja ei täytetty
69	86	Komento ei sallittu (ei käytössä olevaa EF-tiedostoa)
69	87	Odotettuja salattuja viestitietoja puuttuu
69	88	Salatuissa viestitiedoissa virheitä
6A	82	Tiedostoa ei löydy
6A	86	Väärät parametrit P1-P2
6A	88	Kyseessä olevaa dataa ei löydy
6B	00	Väärät parametrit (suhteellinen osoite EF-tiedoston ulkopuolella)

SW1	SW2	Tarkoitus
6C	XX	Väärä pituus, SW2 osoittaa tarkan pituuden. Mitään tietokenttää ei palauteta vastauksena
6D	00	Käskykoodia ei tueta tai se ei ole voimassa
6E	00	Luokkaa ei tueta
6F	00	Muut tarkastusvirheet

3.6 Komentojen kuvaus

Tässä luvussa kuvataan ajopiirturikorttien pakolliset komennot.

Salaustoiimiin liittyviä lisätietoja on lisäyksessä 11 (Yhteiset turvamekanismit).

Kaikki komennot on kuvattu käytetystä protokollasta (T=0 tai T=1) riippumatta. APDU-rakenteen tavut CLA, INS, P1, P2, Lc ja Le on aina näytetty. Jos kuvattavassa komennossa ei tarvita Lc- tai Le-tavuja, niihin liittyvän pituuden, arvon ja kuvauksen kohta on jätetty tyhjäksi.

TCS_315 Jos molempia pituutta osoittavia tavuja (Lc ja Le) pyydetään, kuvattu komento on jaettava kahteen osaan, jos liitäntälaitte käyttää T=0-protokollaa: liitäntälaitte lähettää kuvauksen mukaisen komennon, jossa P3=Lc + data ja sen jälkeen GET RESPONSE -komennon (ks. kohta 3.6.6), jossa P3=Le.

TCS_316 Jos molempia pituutta osoittavia tavuja pyydetään ja Le=0:

- käytettäessä T=1-protokollaa, kortin on vastattava tietoon Le=0 lähettämällä kaikki tulostettavissa olevat tiedot.
- käytettäessä T=0-protokollaa, liitäntälaitteen on lähetettävä ensimmäinen komento, jossa P3=Lc + data, ja kortin on vastattava (tämä käytännössä aiheutuvaan) tietoon Le=0 tilaa osoittavilla tavuilla '61La', missä La on vastaukseen käytettävissä olevien tavujen määrä. Liitäntälaitte antaa sitten GET RESPONSE -komennon, jossa P3=La, lukeakseen tiedot.

3.6.1 SELECT FILE

Tämä komento on standardin ISO/IEC 7816-4 mukainen, mutta sen käyttö on rajoitettua standardissa määritellyn komentoa verrattuna.

SELECT FILE -komentoa käytetään:

- valitsemaan sovelluksen sisältävä DF-tiedosto (on käytettävä valintaa nimen perusteella)
- valitsemaan EF-tiedosto annetun tiedostotunnisteen perusteella

3.6.1.1 Valinta nimen (AID) perusteella

Tällä komennolla voidaan valita kortilla oleva sovelluksen sisältävä DF-tiedosto.

TCS_317 Tämä komento voidaan antaa mistä hyvänsä tiedostorakenteessa (ATR-signaalin jälkeen tai milloin hyvänsä).

TCS_318 Sovelluksen valitseminen asettaa senhetkisen tietoturva-ympäristön alkutilaansa. Kun sovelluksen valinta on tehty, mitään julkista avainta ei ole enää valittuna eikä aiempi tilapäinen avain enää ole käytettävissä salattuun sanomanvälitykseen. Myöskään AUT-käyttöehto ei enää ole voimassa.

TCS_319 Komentoviesti

Tavu	Pituus	Arvo	Selite
CLA	1	'00h'	
INS	1	'A4h'	
P1	1	'04h'	Valinta nimen (AID) perusteella
P2	1	'0Ch'	Vastausta ei odoteta
Lc	1	'NNh'	Kortille lähetettävien tavujen määrä (sovellustunnisteen (AID) pituus): '06h' ajopiirturisovellukselle
#6-#(5+NN)	NN	'XX..XXh'	AID: 'FF 54 41 43 48 4F' ajopiirturisovellukselle

SELECT FILE -komentoon ei tarvita vastausta (Le-tavu puuttuu käytettäessä T=1-protokollaa, tai vastausta ei pyydetä käytettäessä T=0-protokollaa).

TCS_320 Vastausviesti (vastausta ei pyydetty)

Tavu	Pituus	Arvo	Selite
SW	2	'XXXXh'	Tilaa osoittavat tavut (SW1, SW2)

- Jos komennon suorittaminen onnistui, kortti vastaa '9000'.
- Jos sovellustunnistetta vastaavaa sovellusta ei löytynyt, suorittamisen tilaa kuvaava vastaus on '6A82'.
- T=1-protokollaa käytettäessä tavun Le ollessa mukana tilaa kuvaava vastaus on '6700'.
- T=0-protokollaa käytettäessä, kun vastausta on pyydetty SELECT FILE -komennon jälkeen, tilaa kuvaava vastaus on '6900'.
- Jos valittu sovellus katsotaan vialliseksi (tiedoston ominaisuuksissa on todettu eheysvirhe), suorittamisen tilaa kuvaava vastaus on '6400' tai '6581'.

3.6.1.2 EF-tiedoston valinta sen tiedostotunnisteen perusteella

TCS_321 Komentoviesti

Tavu	Pituus	Arvo	Selite
CLA	1	'00h'	
INS	1	'A4h'	
P1	1	'02h'	Käytössä olevan DF-tiedoston alaisen EF-tiedoston valinta
P2	1	'0Ch'	Vastausta ei odoteta
Lc	1	'02h'	Kortille lähetettävien tavujen määrä
#6-#7	2	'XXXXh'	Tiedostotunniste

SELECT FILE -komentoon ei tarvita vastausta (Le-tavu puuttuu käytettäessä T=1-protokollaa, tai vastausta ei pyydetä käytettäessä T=0-protokollaa).

TCS_322 Vastausviesti (vastausta ei pyydetty)

Tavu	Pituus	Arvo	Selite
SW	2	'XXXXh'	Tilaa osoittavat tavut (SW1, SW2)

- Jos komennon suorittaminen onnistui, kortti vastaa '9000'.
- Jos tiedostotunnistetta vastaavaa tiedostoa ei löytynyt, suorittamisen tilaa kuvaava vastaus on '6A82'.
- T=1-protokollaa käytettäessä tavun Le ollessa mukana tilaa kuvaava vastaus on '6700'.
- T=0-protokollaa käytettäessä, kun vastausta on pyydetty SELECT FILE -komennon jälkeen, tilaa kuvaava vastaus on '6900'.
- Jos valittu tiedosto katsotaan vialliseksi (tiedoston ominaisuuksissa on todettu eheysvirhe), suorittamisen tilaa kuvaava vastaus on '6400' tai '6581'.

3.6.2 READ BINARY

Tämä komento on standardin ISO/IEC 7816-4 mukainen, mutta sen käyttö on rajoitettua standardissa määriteltyyn komentoon verrattuna.

READ BINARY -komentoa käytetään lukemaan tietoja transparent-tyyppisestä EF-tiedostosta.

Kortin vastaus koostuu luetuista tiedoista, jotka voidaan tarvittaessa suojata salatun sanomanvälityksen rakenteella.

TCS_323 Komento voidaan suorittaa vain, jos tietoturvan tila on EF-tiedostolle ja READ-toiminolle määriteltyjen tietoturvaominaisuuksien mukainen.

3.6.2.1 *Komento ilman salattua sanomanvälitystä*

Tämän komennon avulla liitäntälaite voi lukea tietoja kulloinkin valitusta EF-tiedostosta ilman salattua sanomanvälitystä.

TCS_324 Tietojen lukeminen tiedostosta, joka on merkitty salatuksi (encrypted), ei saa olla mahdollista tällä komennolla.

TCS_325 Komentoviesti

Tavu	Pituus	Arvo	Selite
CLA	1	'00h'	Salattua sanomanvälitystä ei pyydetä
INS	1	'B0h'	
P1	1	'XXh'	Suhteellinen osoite tavuina tiedoston alusta laskien: merkitsevin tavu
P2	1	'XXh'	Suhteellinen osoite tavuina tiedoston alusta laskien: vähiten merkitsevä tavu
Le	1	'XXh'	Vastauksena odotettavan datan pituus. Luettavien tavujen määrä

Huomautus: P1-tavun bitti 8 on asetettava nolllaksi.

TCS_326 Vastausviesti

Tavu	Pituus	Arvo	Selite
#1-#X	X	'XX..XXh'	Tiedot luettu
SW	2	'XXXXh'	Tilaa osoittavat tavut (SW1, SW2)

- Jos komennon suorittaminen onnistui, kortti vastaa '9000'.
- Jos mitään EF-tiedostoa ei valita, suorittamisen tilaa kuvaava vastaus on '6986'.
- Jos valitun tiedoston käyttöehtoja ei täytetty, komennon suorittaminen keskeytetään viestillä '6982'.
- Jos suhteellinen osoite ei ole EF-tiedoston koon mukainen (suhteellinen osoite > EF-tiedoston koko), suorittamisen tilaa kuvaava vastaus on '6B00'.
- Jos luettavan datan pituus ei ole EF-tiedoston koon mukainen (suhteellinen osoite + Le > EF-tiedoston koko), suorittamisen tilaa kuvaava vastaus on '6700' tai '6Cxx', jossa 'xx' ilmaisee tarkan pituuden.
- Jos tiedoston ominaisuuksissa on todettu eheysvirhe, kortin on pidettävä tiedostoa vaurioituneena ja lukukelvottomana, ja suorittamisen tilaa kuvaava vastaus on '6400' tai '6581'.
- Jos tallennetuissa tiedoissa todetaan eheysvirhe, kortin on palautettava pyydytetyt tiedot ja suorittamisen tilaa kuvaava vastaus on '6281'.

3.6.2.2 *Komento salattua sanomanvälitystä käyttäen*

Tämän komennon avulla liitäntälaite voi lukea tietoja kulloinkin valitusta EF-tiedostosta käyttäen salattua sanomanvälitystä, jonka avulla vastaanotetun datan eheys voidaan todentaa ja pitää data salassa tapauksissa, joissa EF-tiedosto on merkitty salatuksi.

TCS_327 Komentoviesti

Tavu	Pituus	Arvo	Selite
CLA	1	'0Ch'	Salattua sanomanvälitystä pyydetään
INS	1	'B0h'	INS (käskytavu)
P1	1	'XXh'	P1 (suhteellinen osoite tavuina tiedoston alusta laskien): merkitsevin tavu
P2	1	'XXh'	P2 (suhteellinen osoite tavuina tiedoston alusta laskien): vähiten merkitsevä tavu
Lc	1	'09h'	Salattua sanomanvälitystä varten kortille lähetettävän datan pituus
#6	1	'97h'	T _{LE} : odotetun pituuserittimen tuntomerkki
#7	1	'01h'	L _{LE} : odotettu datan pituus
#8	1	'NNh'	Odotetun pituuden määrite (alkueräinen Le): luettavien tavujen määrä

Tavu	Pituus	Arvo	Selite
#9	1	'8Eh'	T _{CC} : salauksen tarkistussumman tuntomerkki
#10	1	'04h'	L _{CC} : seuraavan salauksen tarkistussumman pituus
#11-#14	4	'XX..XXh'	Salauksen tarkistussumma (4 eniten merkitsevää tavua)
Le	1	'00h'	Kuten standardissa ISO/IEC 7816-4 on määritelty

TCS_328 Vastausviesti, jos EF-tiedostoa ei ole merkitty salatuksi ja salattua sanomanvälitystä varten lähetetyn datan muoto on oikea:

Tavu	Pituus	Arvo	Selite
#1	1	'81h'	T _{PV} : salaamattoman datan tuntomerkki
#2	L	'NNh' tai '81 NNh'	L _{PV} : vastauksena saadun datan pituus (= alkuperäinen Le) L sisältää kaksi tavua, jos L _{PV} > 127 tavua
#(2+L)-#(1+L+NN)	NN	'XX..XXh'	Salaamatonta dataa
#(2+L+NN)	1	'8Eh'	T _{CC} : salauksen tarkistussumman tuntomerkki
#(3+L+NN)	1	'04h'	L _{CC} : seuraavan salauksen tarkistussumman pituus
#(4+L+NN)-#(7+L+NN)	4	'XX..XXh'	Salauksen tarkistussumma (4 eniten merkitsevää tavua)
SW	2	'XXXXh'	Tilaa osoittavat tavut (SW1, SW2)

TCS_329 Vastausviesti, jos EF-tiedosto on merkitty salatuksi ja salattua sanomanvälitystä varten lähetetyn datan muoto on oikea:

Tavu	Pituus	Arvo	Selite
#1	1	'87h'	T _{PI CG} : salatun datan (kryptogrammin) tuntomerkki (tag)
#2	L	'MMh' tai '81 MMh'	L _{PI CG} : Vastauksena saadun salatun datan pituus (täyttämisen takia eri kuin komennon alkuperäinen Le) L sisältää kaksi tavua, jos L _{PI CG} > 127 tavua
#(2+L)-#(1+L+MM)	MM	'01XX..XXh'	Salattu data: täytön osoitin ja kryptogrammi
#(2+L+MM)	1	'8Eh'	T _{CC} : salauksen tarkistussumman tuntomerkki
#(3+L+MM)	1	'04h'	L _{CC} : seuraavan salauksen tarkistussumman pituus
#(4+L+MM)-#(7+L+MM)	4	'XX..XXh'	Salauksen tarkistussumma (4 eniten merkitsevää tavua)
SW	2	'XXXXh'	Tilaa osoittavat tavut (SW1, SW2)

Salatun datan ensimmäinen tavu osoittaa käytetyn täyttämistavan. Ajopiirturisuovelluksessa täyttämistavan osoitin saa aina arvon '01h', joka merkitsee, että on käytetty standardissa ISO/IEC 7816-4 määrättyä täyttämistapaa (yksi tavu arvoltaan '80h' ja sen perässä nollan arvoisia tavuja: ISO/IEC 9797 tapa 2).

READ BINARY -komennolle ilman salattua sanomanvälitystä (ks. kohta 3.6.2.1) kuvatut 'normaalit' suorittamisen tilaa kuvaavat vastaukset voidaan antaa edellä kuvattujen vastausviestirakenteiden avulla.

Tämän lisäksi saattaa ilmetä joitakin erityisesti salattuun sanomanvälitykseen liittyviä virhetilanteita. Tällöin vastauksena annetaan pelkkä suorittamisen tilan kuvaus ilman salatun sanomanvälityksen rakenteita:

TCS_330 Vastausviesti, jos salattua sanomanvälitystä varten lähetetyn datan muoto on väärä

Tavu	Pituus	Arvo	Selite
SW	2	'XXXXh'	Tilaa osoittavat tavut (SW1, SW2)

— Jos käytössä ei ole voimassa olevaa tilapäistä avainta, suorittamisen tilaa kuvaava vastaus on '6A88'. Näin tapahtuu, jos tilapäistä avainta ei vielä ole luotu tai sen voimassaolo on päättynyt (tässä tapauksessa liitäntälaitteen on suoritettava uudelleen molemminpuolinen todentamisprosessi uuden tilapäisen avaimen luomiseksi).

— Jos datasta puuttuu joitakin odotettuja osia, suorittamisen tilaa kuvaava vastaus on '6987': tämä virhe tapahtuu, jos odotettu tuntomerkki (tag) puuttuu tai komennon rakenne on väärä.

- Jos jotkin datan osat ovat virheellisiä, suorittamisen tilaa kuvaava vastaus on '6988': tämä virhe tapahtuu, jos kaikki tarvittavat tuntomerkit ovat mukana, mutta jotkin datan pituudet eroavat odotetuista pituuksista.
- Jos salauksen tarkistussumman todentaminen epäonnistuu, suorittamisen tilaa kuvaava vastaus on '6688'.

3.6.3 UPDATE BINARY

Tämä komento on standardin ISO/IEC 7816-4 mukainen, mutta sen käyttö on rajoitettua standardissa määriteltyyn komenttoon verrattuna.

UPDATE BINARY -komento käynnistää EF-binaaritedostossa jo olevien bittien päivittämisen (poistamisen + kirjoittamisen) komennon tietoyksikössä olevilla biteillä.

TCS_331 Komento voidaan suorittaa vain, jos tietoturvan tila on EF-tiedostolle UPDATE-toiminnon osalta määriteltyjen tietoturvaominaisuuksien mukainen. (Jos UPDATE-toiminnon käyttöehtoon sisältyy PRO SM -ehto, salattu sanomanvälitys on lisättävä komenttoon.)

3.6.3.1 Komento ilman salattua sanomanvälitystä

Tämän komennon avulla liitäntälaite voi kirjoittaa tietoja kulloinkin valittuun EF-tiedostoon ilman, että kortti todentaa vastaanotetun datan eheyttä. Tämä salaamaton tila on sallittu vain, jos kyseistä tiedostoa ei ole merkitty salatuksi.

TCS_332 Komentoviesti

Tavu	Pituus	Arvo	Selite
CLA	1	'00h'	Salattua sanomanvälitystä ei pyydetä
INS	1	'D6h'	Suhteellinen osoite tavuina tiedoston alusta laskien: merkitsevin tavu
P1	1	'XXh'	
P2	1	'XXh'	Suhteellinen osoite tavuina tiedoston alusta laskien: vähiten merkitsevä tavu
Lc	1	'NNh'	Lc: päivitettävän datan pituus. Kirjoitettavien tavujen määrä
#6-#(5+NN)	NN	'XX..XXh'	Kirjoitettava data

Huomautus: P1-tavun bitti 8 on asetettava nolllaksi.

TCS_333 Vastausviesti

Tavu	Pituus	Arvo	Selite
SW	2	'XXXXh'	Tilaa osoittavat tavut (SW1, SW2)

- Jos komennon suorittaminen onnistui, kortti vastaa '9000'.
- Jos mitään EF-tiedostoa ei valita, suorittamisen tilaa kuvaava vastaus on '6986'.
- Jos valitun tiedoston käyttöehtoja ei täytetty, komennon suorittaminen keskeytetään viestillä '6982'.
- Jos suhteellinen osoite ei ole EF-tiedoston koon mukainen (suhteellinen osoite > EF-tiedoston koko), suorittamisen tilaa kuvaava vastaus on '6B00'.
- Jos kirjoitettavan datan pituus ei ole EF-tiedoston koon mukainen (suhteellinen osoite + Le > EF-tiedoston koko), suorittamisen tilaa kuvaava vastaus on '6700'.
- Jos tiedoston ominaisuuksissa on todettu eheysvirhe, kortin on pidettävä tiedostoa vaurioituneena ja lukukelvottomana ja suorittamisen tilaa kuvaava vastaus on '6400' tai '6500'.
- Jos kirjoittaminen ei onnistu, suorittamisen tilaa kuvaava vastaus on '6581'.

3.6.3.2 *Komento salattua sanomanvälitystä käyttäen*

Tämän komennon avulla liitäntälaite voi kirjoittaa tietoja kulloinkin valittuun EF-tiedostoon siten, että kortti todentaa vastaanotetun datan eheyden. Koska salassapitoa ei vaadita, dataa ei salata.

TCS_334 Komentoviesti

Tavu	Pituus	Arvo	Selite
CLA	1	'0Ch'	Salattua sanomanvälitystä pyydetään
INS	1	'D6h'	INS (käskytavu)
P1	1	'XXh'	Suhteellinen osoite tavuina tiedoston alusta laskien: merkitsevin tavu
P2	1	'XXh'	Suhteellinen osoite tavuina tiedoston alusta laskien: vähiten merkitsevä tavu
Lc	1	'XXh'	Varmistetun tietokentän pituus
#6	1	'81h'	T _{PV} : salaamattoman datan tuntomerkki (tag)
#7	L	'NNh' tai '81NNh'	L _{PV} : lähetettävän datan pituus. L sisältää kaksi tavua, jos L _{PV} > 127 tavua.
#(7+L)-#(6+L+NN)	NN	'XX..XXh'	Salaamatonta dataa (kirjoitettava data)
#(7+L+NN)	1	'8Eh'	T _{CC} : salauksen tarkistussumman tuntomerkki
#(8+L+NN)	1	'04h'	L _{CC} : seuraavan salauksen tarkistussumman pituus
#(9+L+NN)-#(12+L+NN)	4	'XX..XXh'	Salauksen tarkistussumma (4 eniten merkitsevää tavua)
Le	1	'00h'	Kuten standardissa ISO/IEC 7816-4 on määritelty

TCS_335 Vastausviesti, jos salattua sanomanvälitystä varten lähetetyn datan muoto on oikea

Tavu	Pituus	Arvo	Selite
#1	1	'99h'	T _{SW} : tilaa osoittavien tavujen tuntomerkki (suojataan tarkistussummalla)
#2	1	'02h'	L _{SW} : vastauksena annettujen tilaa osoittavien tavujen pituus
#3-#4	2	'XXXXh'	Tilaa osoittavat tavut (SW1, SW2)
#5	1	'8Eh'	T _{CC} : salauksen tarkistussumman tuntomerkki
#6	1	'04h'	L _{CC} : seuraavan salauksen tarkistussumman pituus
#7-#10	4	'XX..XXh'	Salauksen tarkistussumma (4 eniten merkitsevää tavua)
SW	2	'XXXXh'	Tilaa osoittavat tavut (SW1, SW2)

UPDATE BINARY -komennolle ilman salattua sanomanvälitystä (ks. kohta 3.6.3.1), kuvatut 'normaalit' suorittamisen tilaa kuvaavat vastaukset voidaan antaa edellä kuvattujen vastausviestirakenteiden avulla.

Tämän lisäksi saattaa ilmetä joitakin erityisesti salattuun sanomanvälitykseen liittyviä virhetilanteita. Tällöin vastauksena annetaan pelkkä suorittamisen tilan kuvaus ilman salatun sanomanvälityksen rakenteita:

TCS_336 Vastausviesti jos salattua sanomanvälitystä varten lähetetyn datan muoto ei ole oikea

Tavu	Pituus	Arvo	Selite
SW	2	'XXXXh'	Tilaa osoittavat tavut (SW1, SW2)

- Jos käytössä ei ole voimassa olevaa tilapäistä avainta, suorittamisen tilaa kuvaava vastaus on '6A88'.
- Jos datasta puuttuu joitakin odotettuja osia, suorittamisen tilaa kuvaava vastaus on '6987': tämä virhe tapahtuu, jos odotettu tuntomerkki puuttuu tai komennon rakenne on väärä.
- Jos jotkin datan osat ovat virheellisiä, suorittamisen tilaa kuvaava vastaus on '6988': tämä virhe tapahtuu, jos kaikki tarvittavat tuntomerkit ovat mukana, mutta jotkin datan pituudet eroavat odotetuista pituuksista.
- Jos salauksen tarkistussumman todentaminen epäonnistuu, suorittamisen tilaa kuvaava vastaus on '6688'.

3.6.4 **GET CHALLENGE**

Tämä komento on standardin ISO/IEC 7816-4 mukainen, mutta sen käyttö on rajoitettua standardissa määriteltyyn komentoon verrattuna.

GET CHALLENGE -komento pyytää korttia antamaan haasteen (alkuluvun) käytettäväksi tietoturvaan liittyvässä menettelyssä, jolla salattua dataa lähetetään kortille.

TCS_337 Kortin antama haaste on voimassa vain seuraavassa haastetta käytävässä komennossa, joka lähetetään kortille.

TCS_338 Komentoviesti

Tavu	Pituus	Arvo	Selite
CLA	1	'00h'	CLA
INS	1	'84h'	INS
P1	1	'00h'	P1
P2	1	'00h'	P2
Le	1	'08h'	Le (odotettu haasteen pituus)

TCS_339 Vastausviesti

Tavu	Pituus	Arvo	Selite
#1-#8	8	'XX..XXh'	Haaste
SW	2	'XXXXh'	Tilaa osoittavat tavut (SW1, SW2)

- Jos komennon suorittaminen onnistui, kortti vastaa '9000'.
- Jos Le:n arvo on muu kuin '08h', tilaa kuvaava vastaus on '6700'.
- Jos parametrit P1-P2 ovat virheellisiä, suorituksen tila on '6A86'.

3.6.5 **VERIFY**

Tämä komento on standardin ISO/IEC 7816-4 mukainen, mutta sen käyttö on rajoitettua standardissa määriteltyyn komentoon verrattuna.

VERIFY-komento käynnistää komennon lähettämien kortin haltijan kontrollitietojen (käyttäjän henkilökohtaisen tunnusluvun) kortilla tapahtuvan vertaamisen sillä oleviin kortin haltijan kontrollitietoihin.

Huomaus: Liitäntälaitteen on täydennettävä käyttäjän syöttämä henkilökohtainen tunnusluku lisäämällä sen perään tavuja arvoltaan FFh siten, että sen kokonaispituudeksi tulee 8 tavua.

TCS_340 Jos komento suoritetaan onnistuneesti, kortin haltijan kontrollitietoja vastaavat oikeudet annetaan käyttöön ja tunnusluvun syöttämisyriytyksiä laskeva laskuri asetetaan takaisin alkutilaansa.

TCS_341 Jos tietojen vertailu ei anna hyväksyttävää tulosta, tämä kirjataan kortille, mikä rajoittaa kontrollitietojen tulevien käyttöyrityksien määrää.

TCS_342 Komentoviesti

Tavu	Pituus	Arvo	Selite
CLA	1	'00h'	CLA (komennon luokan ilmaiseva tavu)
INS	1	'20h'	INS
P1	1	'00h'	P1
P2	1	'00h'	P2 (todennetut kortin haltijan kontrollitiedot ovat automaattisesti tiedossa)
Lc	1	'08h'	Lähetettävien kontrollitietojen pituus
#6-#13	8	'XX..XXh'	Kortin haltijan kontrollitiedot (CHV)

TCS_343 Vastausviesti

Tavu	Pituus	Arvo	Selite
SW	2	'XXXXh'	Tilaa osoittavat tavut (SW1, SW2)

- Jos komennon suorittaminen onnistui, kortti vastaa '9000'.
- Jos vertailtavia kontrollitietoja ei löydy, suorittamisen tilaa kuvaava vastaus on '6A88'.
- Jos kontrollitietojen käyttö on estetty (jäljellä olevien tunnuksen syöttämisyritysten laskurin arvo on nolla), suorittamisen tilaa kuvaava vastaus on '6983'. Kun tämä tila syntyy, kortin haltijan kontrollitietoja ei enää koskaan voida onnistuneesti syöttää.
- Jos tietojen vertailu ei anna hyväksyttävää tulosta, jäljellä olevien yrityskertojen laskurin arvoa vähennetään ja annetaan tilaa kuvaava vastaus '63CX' (X > 0 ja X on jäljellä olevien yrityskertojen määrä. Jos X = 'F', kontrollitietojen syöttämisen yrityskertojen laskurin arvo on suurempi kuin 'F').
- Jos vertailtavat kontrollitiedot katsotaan virheellisiksi, suorittamisen tilaa kuvaava vastaus on '6400' tai '6581'.

3.6.6 GET RESPONSE

Tämä komento on standardin ISO/IEC 7816-4 mukainen.

Tätä komentoa (joka on tarpeen ja käytettävissä vain T=0-protokollan yhteydessä) käytetään lähettämään valmisteltua dataa kortilta liitäntälaitteelle (tapaus, jolloin komento on sisältänyt sekä Lc- että Le-tavun).

GET RESPONSE -komento on annettava välittömästi dataa valmistelevan komennon jälkeen; muussa tapauksessa data menetetään. GET RESPONSE -komennon suorittamisen jälkeen (paitsi silloin, kun tapahtuu virhe '61xx' tai '6Cxx', ks. alla) ei aiemmin valmisteltu data ole enää käytettävissä.

TCS_344 Komentoviesti

Tavu	Pituus	Arvo	Selite
CLA	1	'00h'	
INS	1	'C0h'	
P1	1	'00h'	
P2	1	'00h'	
Le	1	'XXh'	Odotettu tavujen määrä

TCS_345 Vastausviesti

Tavu	Pituus	Arvo	Selite
#1-#X	X	'XX..XXh'	Data
SW	2	'XXXXh'	Tilaa osoittavat tavut (SW1, SW2)

- Jos komennon suorittaminen onnistui, kortti vastaa '9000'.
- Jos kortti ei ole valmistellut dataa, suorittamisen tilaa kuvaava vastaus on '6900' tai '6F00'.
- Jos Le on suurempi kuin käytettävissä olevien tavujen määrä tai jos se on nolla, suorittamisen tilaa kuvaava vastaus on '6Cxx', missä 'xx' on käytettävissä olevien tavujen tarkka määrä. Tässä tapauksessa valmisteltu data on vielä seuraavan GET_RESPONSE -komennon käytettävissä.
- Jos Le ei ole nolla, mutta pienempi kuin käytettävissä olevien tavujen määrä, kortti lähettää vaaditun datan normaalisti ja suorittamisen tilaa kuvaava vastaus on '61xx', jossa 'xx' on seuraavan GET_RESPONSE -komennon käytettävissä olevien tavujen määrä. Jäljelle jäänyt data (jota ei pyydetty) ei enää ole käytettävissä.
- Jos komentoa ei tueta (T=1-protokolla), kortti vastaa '6D00'.

3.6.7 PSO: VERIFY CERTIFICATE

Tämä komento on standardin ISO/IEC 7816-8 mukainen, mutta sen käyttö on rajoitettua standardissa määritellyyn komentoon verrattuna.

VERIFY CERTIFICATE -komennon avulla kortti saa ulkopuolelta julkisen avaimen ja tarkastaa sen kelpoisuuden.

TCS_346 Jos VERIFY CERTIFICATE -komennon tulos on hyväksyttävä, julkinen avain tallennetaan, jotta sitä voidaan tulevaisuudessa käyttää tietoturva-ympäristössä. Tämä avain asetetaan nimenomaan MSE-komennon (ks. kohta 3.6.10) käyttöön tietoturvaan liittyvien kommentojen (INTERNAL AUTHENTICATE, EXTERNAL AUTHENTICATE tai VERIFY CERTIFICATE) yhteydessä sen avaintunnisteen avulla.

TCS_347 VERIFY CERTIFICATE -komento käyttää kuitenkin MSE-komennon aiemmin valitsemaa julkista avainta varmenteen avaamiseen. Kyseessä on oltava tietyn jäsenvaltion tai Euroopan julkinen avain.

TCS_348 Kommentoviesti

Tavu	Pituus	Arvo	Selite
CLA	1	'00h'	CLA
INS	1	'2Ah'	PSO (Suorita turvatoimi)
P1	1	'00h'	P1
P2	1	'AEh'	P2: data, jota ei ole BER-TLV-koodattu (dataelementtien ketjutus)
Lc	1	'CEh'	Lc: varmenteen pituus, 194 tavua.
#6-#199	194	'XX..XXh'	Varmenne: dataelementit ketjutettu (kuten lisäyksessä 11 on kuvattu)

TCS_349 Vastausviesti

Tavu	Pituus	Arvo	Selite
SW	2	'XXXXh'	Tilaa osoittavat tavut (SW1, SW2)

- Jos komennon suorittaminen onnistui, kortti vastaa '9000'.
- Jos varmenteen todentaminen ei onnistu, suorittamisen tilaa kuvaava vastaus on '6688'. Varmenteen todennus- ja purkumenettely on kuvattu lisäyksessä 11.
- Jos tietoturva-ympäristössä ei ole julkista avainta, vastaus on '6A88'.
- Jos valittu julkinen avain (jota käytetään varmenteen avaamiseen) katsotaan vialliseksi, suorittamisen tilaa kuvaava vastaus on '6400' tai '6581'.
- Jos (varmenteen avaamiseen käytettävän) julkisen avaimen CHA.LSB-arvo (CertificateHolderAuthorization.equipmentType) on muu kuin '00' (eli muu kuin tietyn jäsenvaltion tai Euroopan kyseinen arvo), suorittamisen tilaa kuvaava vastaus on '6985'.

3.6.8 INTERNAL AUTHENTICATE

Tämä komento on standardin ISO/IEC 7816-4 mukainen.

INTERNAL AUTHENTICATE -komennon avulla liitäntälaitte voi todentaa kortin.

Todennusmenettely on kuvattu lisäyksessä 11. Siihen sisältyy seuraavat lausumat:

TCS_350 INTERNAL AUTHENTICATE -komento käyttää kortin yksityistä avainta (valitaan automaattisesti), kun se allekirjoittaa todennusdatan, johon sisältyy K1 (ensimmäinen dataelementti tilapäisestä avaimesta sovittaessa) ja RND1, ja kulloinkin (viimeisimmän MSE-komennon avulla) valittua julkista avainta, kun se salaa allekirjoituksen ja muodostaa todennustunnisteen (lisätietoja tästä on lisäyksessä 11).

TCS_351 Kommentoviesti

Tavu	Pituus	Arvo	Selite
CLA	1	'00h'	CLA
INS	1	'88h'	INS
P1	1	'00h'	P1
P2	1	'00h'	P2
Lc	1	'10h'	Kortille lähetettävän datan pituus
#6-#13	8	'XX..XXh'	Kortin todennukseen käytettävä haaste
#14-#21	8	'XX..XXh'	VU.CHR (ks. lisäys 11)
Le	1	'80h'	Kortilta odotettavan datan pituus

TCS_352 Vastausviesti

Tavu	Pituus	Arvo	Selite
#1-#128	128	'XX..XXh'	Kortin todennustunniste (ks. lisäys 11)
SW	2	'XXXXh'	Tilaa osoittavat tavut (SW1, SW2)

- Jos komennon suorittaminen onnistui, kortti vastaa '9000'.
- Jos tietoturva ympäristössä ei ole julkista avainta, suorittamisen tilaa kuvaava vastaus on '6A88'.
- Jos tietoturva ympäristössä ei ole yksityistä avainta, suorittamisen tilaa kuvaava vastaus on '6A88'.
- Jos VU.CHR ei täsmää käytössä olevan julkisen avaimen tunnisteiden kanssa, suorittamisen tilaa kuvaava vastaus on '6A88'.
- Jos valittu yksityinen avain katsotaan vialliseksi, suorittamisen tilaa kuvaava vastaus on '6400' tai '6581'.

TCS_353 Jos INTERNAL AUTHENTICATE -komennon tulos on onnistunut, poistetaan käytössä oleva tilapäinen avain, jos sellainen on, eikä se sen jälkeen ole käytettävissä. Uusi tilapäinen avain saadaan käyttöön EXTERNAL AUTHENTICATE -komennon onnistuneen suorittamisen jälkeen.

3.6.9 EXTERNAL AUTHENTICATE

Tämä kommento on standardin ISO/IEC 7816-4 mukainen.

EXTERNAL AUTHENTICATE -komennon avulla kortti voi todentaa liitäntälaitteen.

Todennusmenettely on kuvattu lisäyksessä 11. Siihen sisältyy seuraavat lausumat:

TCS_354 Välittömästi ennen EXTERNAL AUTHENTICATE -komentoa tulee antaa GET CHALLENGE -komento. Kortti antaa ulos haasteen (RND3).

TCS_355 Kryptogrammin todennuksessa käytetään RND3-lukua (joka on kortin antama haaste), kortin yksityistä avainta (joka valitaan automaattisesti) ja aiemmin MSE-komennolla valittua julkista avainta.

TCS_356 Kortti todentaa kryptogrammin ja, jos tulos on oikea, AUT-käyttöehto saadaan käyttöön.

TCS_357 Annettuun kryptogrammiin sisältyy K2 eli järjestyksessä toinen dataelementti tilapäisestä avaimesta sovittaessa.

TCS_358 Kommentoviesti

Tavu	Pituus	Arvo	Selite
CLA	1	'00h'	CLA
INS	1	'82h'	INS
P1	1	'00h'	P1
P2	1	'00h'	P2 (käytettävä julkinen avain on automaattisesti tiedossa ja se on aiemmin valittu MSE-komennolla)
Lc	1	'80h'	Lc (kortille lähetettävän datan pituus)
#6-#133	128	'XX..XXh'	Kryptogrammi (ks. lisäys 11)

TCS_359 Vastausviesti

Tavu	Pituus	Arvo	Selite
SW	2	'XXXXh'	Tilaa osoittavat tavut (SW1, SW2)

- Jos komennon suorittaminen onnistui, kortti vastaa '9000'.
- Jos tietoturvympäristössä ei ole julkista avainta, vastaus on '6A88'.
- Jos valitun julkisen avaimen CHA (varmenteen haltijan valtuutus) ei ole ajopiirturisovelluksen tunnisteiden (AID) ja ajoneuvoyksikön tyyppin yhdistelmä, suorittamisen tilaa kuvaava vastaus on '6F00' (ks. lisäys 11).
- Jos tietoturvympäristössä ei ole yksityistä avainta, suorittamisen tilaa kuvaava vastaus on '6A88'.
- Jos kryptogrammin todentamisen tulos on väärä, suorittamisen tilaa kuvaava vastaus on '6688'.
- Jos kommentoa ei välittömästi edeltänyt GET CHALLENGE -komento, suorittamisen tilaa kuvaava vastaus on '6985'.
- Jos valittu yksityinen avain katsotaan vialliseksi, suorittamisen tilaa kuvaava vastaus on '6400' tai '6581'.

TCS_360 Jos EXTERNAL AUTHENTICATE -komennon tulos on onnistunut ja jos tilapäisen avaimen ensimmäinen osa on saatu äskettäin onnistuneesti suoritettulla INTERNAL AUTHENTICATE -komennolla, tilapäinen avain on asetettu tulevia salatun sanomanlähetystä vaativia komentoja varten.

TCS_361 Jos tilapäisen avaimen ensimmäistä osaa ei ole saatu aiemmalla INTERNAL AUTHENTICATE -komennolla, ei tilapäisen avaimen toista, liitäntälaitteen lähettämää osaa tallenneta kortille. Tällä varmistetaan se, että molemminpuolinen todennusprosessi tapahtuu lisäyksessä 11 määritellyssä järjestyksessä.

3.6.10 MANAGE SECURITY ENVIRONMENT

Tällä komennolla valitaan todennukseen käytettävä julkinen avain.

Tämä komento on standardin ISO/IEC 7816-8 mukainen. Komennon käyttö on rajoitettua siihen liittyvään standardiin nähden.

TCS_362 Avain, johon viitataan MSE-komennon datakentässä, on voimassa kaikissa ajopiirturikortin DF-tiedoston sisältämissä tiedostoissa.

TCS_363 Avain, johon viitataan MSE-komennon datakentässä, pysyy käytössä olevana julkisena avaimena siihen asti, kunnes seuraava oikein annettu MSE-komento suoritetaan.

TCS_364 Jos kyseistä avainta ei (jo) ole kortilla, ei tietoturvympäristö muutu.

TCS_365 Kommentiviesti

Tavu	Pituus	Arvo	Selite
CLA	1	'00h'	CLA
INS	1	'22h'	INS
P1	1	'C1h'	P1: avain, johon viitataan, kelpaa kaikkiin salaustoimiin
P2	1	'B6h'	P2 (digitaalista allekirjoitusta koskevan datan viite)
Lc	1	'0Ah'	Lc 1 0Ah Lc: seuraavan datakentän pituus
#6	1	'83h'	Tuntomerkki, jolla viitataan epäsymmetrisen salauksen yhteydessä käytettävään julkiseen avaimeseen
#7	1	'08h'	Avainviitteen (avaimen tunnisteiden) pituus
#8-#15	08h	'XX..XXh'	Avaimen tunniste siten kuin se on määritelty lisäyksessä 11

TCS_366 Vastausviesti

Tavu	Pituus	Arvo	Selite
SW	2	'XXXXh'	Tilaa osoittavat tavut (SW1, SW2)

- Jos komennon suorittaminen onnistui, kortti vastaa '9000'.
- Jos avainta, johon viitataan, ei ole kortilla, suorittamisen tilaa kuvaava vastaus on '6A88'.
- Jos salatun sanomanvälityksen muodossa olevasta datasta puuttuu joitakin odotettuja osia, annetaan suorittamisen tilaa kuvaava vastaus '6987'. Näin voi tapahtua, jos tuntomerkki '83h' puuttuu.
- Jos jotkin datan osat ovat virheellisiä, suorittamisen tilaa kuvaava vastaus on '6988'. Näin voi tapahtua, jos avaimen tunnusteen pituus ei ole '08h'.
- Jos valittu avain katsotaan vialliseksi, suorittamisen tilaa kuvaava vastaus on '6400' tai '6581'.

3.6.11 **PSO: HASH**

Tällä komennolla siirretään jonkin datan hash (hajautus) -algoritmillä laskettu tulos kortille. Tätä komentoa käytetään digitaalisten allekirjoitusten todentamisessa. Hash-algoritmin antama tulos tallennetaan EEPROM-muistiin seuraavaa VERIFY DIGITAL SIGNATURE -komentoa varten.

Tämä komento on standardin ISO/IEC 7816-8 mukainen. Komennon käyttö on rajoitettua siihen liittyvään standardiin nähden.

TCS_367 Komentoviesti

Tavu	Pituus	Arvo	Selite
CLA	1	'00h'	CLA
INS	1	'2Ah'	Suorita turvatoimi
P1	1	'90h'	Anna hash-algoritmin tulos
P2	1	'A0h'	Tuntomerkki: datakentässä on hash-algoritmillä käsiteltävää dataa
Lc	1	'16h'	Seuraavan datakentän pituus
#6	1	'90h'	Hash-algoritmin tuloksen tuntomerkki
#7	1	'14h'	Hash-algoritmin tuloksen pituus
#8-#27	20	'XX..XXh'	Hash-algoritmin tulos

TCS_368 Vastausviesti

Tavu	Pituus	Arvo	Selite
SW	2	'XXXXh'	Tilaa osoittavat tavut (SW1, SW2)

- Jos komennon suorittaminen onnistui, kortti vastaa '9000'.
- Jos datasta puuttuu joitain (yllä määriteltyjä) osia, annetaan suorittamisen tilaa kuvaava vastaus '6987'. Näin voi tapahtua, jos jompikumpi tuntomerkeistä arvoltaan '90h' puuttuu.
- Jos jotkin datan osat ovat virheellisiä, suorittamisen tilaa kuvaava vastaus on '6988'. Tämä virhe tapahtuu, jos vaadittava tuntomerkki on mukana, mutta pituus on muu kuin '14h'.

3.6.12 **PERFORM HASH OF FILE**

Tämä komento ei ole standardin ISO/IEC 7816-8 mukainen. Näin ollen tämän komennon luokkaa osoittava CLA-tavu osoittaa, että komentoa PERFORM SECURITY OPERATION/HASH käytetään erikoistarkoituksessa.

TCS_369 PERFORM HASH OF FILE -komennon avulla käsitellään kulloinkin valittua transparent-tyyppisen EF-tiedoston dataa hash-algoritmeilla.

TCS_370 Hash-algoritmin antama tulos tallennetaan kortille. Sitä voidaan sen jälkeen käyttää tiedoston digitaalisen allekirjoituksen luomiseen komennolla PSO: COMPUTE DIGITAL SIGNATURE. Tulos on COMPUTE DIGITAL SIGNATURE -komennon käytettävissä siihen asti, kunnes PERFORM HASH OF FILE -komento seuraavan kerran suoritetaan onnistuneesti.

TCS_371 Kommentiviesti

Tavu	Pituus	Arvo	Selite
CLA	1	'80h'	CLA
INS	1	'2Ah'	Suorita turvatoimi
P1	1	'90h'	Tuntomerkki: hash-algoritmi
P2	1	'00h'	P2: käsittele valitun transparent-tyyppisen tiedoston data hash-algoritmilla

TCS_372 Vastausviesti

Tavu	Pituus	Arvo	Selite
SW	2	'XXXXh'	Tilaa osoittavat tavut (SW1, SW2)

- Jos komennon suorittaminen onnistui, kortti vastaa '9000'.
- Jos mitään sovellusta ei valittu, annetaan suorittamisen tilaa kuvaava vastaus '6985'.
- Jos valittu EF-tiedosto katsotaan vialliseksi (tiedoston ominaisuuksissa tai tallennetuissa tiedoissa eheysvirhe), suorittamisen tilaa kuvaava vastaus on '6400' tai '6581'.
- Jos valittu tiedosto ei ole transparent-tyyppinen, suorittamisen tilaa kuvaava vastaus on '6986'.

3.6.13 PSO: COMPUTE DIGITAL SIGNATURE

Tämän komennon avulla lasketaan digitaalinen allekirjoitus aiemmin lasketun hash-algoritmin antaman tuloksen avulla (ks. PERFORM HASH OF FILE, kohta 3.6.12).

Tämä komento on standardin ISO/IEC 7816-8 mukainen. Komennon käyttö on rajoitettua siihen liittyvään standardiin nähden.

TCS_373 Digitaalinen allekirjoitus lasketaan siten, että käytetään kortin yksityistä avainta, joka on automaattisesti kortin tiedossa.

TCS_374 Kortti tekee digitaalisen allekirjoituksen käyttäen RSA-salausta koskevan PKCS1-standardin mukaista täyttömenetelmää (lisätietoja on lisäyksessä 11).

TCS_375 Kommentiviesti

Tavu	Pituus	Arvo	Selite
CLA	1	'00h'	CLA
INS	1	'2Ah'	Suorita turvatoimi
P1	1	'9Eh'	Palautettava digitaalinen allekirjoitus
P2	1	'9Ah'	Tuntomerkki: datakentässä on allekirjoitettavaa dataa. Koska mukana ei ole datakenttää, oletetaan kyseisen datan olevan jo kortilla (tiedoston hash-algoritmilla käsitelty tulos)
Le	1	'80h'	Odotetun allekirjoituksen pituus

TCS_376 Vastausviesti

Tavu	Pituus	Arvo	Selite
#1-#128	128	'XX.XXh'	Aiemmin lasketun hash-algoritmin tuloksen allekirjoitus
SW	2	'XXXXh'	Tilaa osoittavat tavut (SW1, SW2)

- Jos komennon suorittaminen onnistui, kortti vastaa '9000'.
- Jos automaattisesti valittu yksityinen avain katsotaan vialliseksi, suorittamisen tilaa kuvaava vastaus on '6400' tai '6581'.

3.6.14 PSO: VERIFY DIGITAL SIGNATURE

Tämän komennon avulla todennetaan sellaisen kortille standardin PKCS1 mukaisesti annetun viestin digitaalinen allekirjoitus, jonka hash-algoritmillä laskettu tulos on kortin tiedossa. Allekirjoitukseen käytetty algoritmi on automaattisesti kortin tiedossa.

Tämä komento on standardin ISO/IEC 7816-8 mukainen. Komennon käyttö on rajoitettua siihen liittyvään standardiin nähden.

TCS_377 VERIFY DIGITAL SIGNATURE -komento käyttää aina aiemmalla MANAGE SECURITY ENVIRONMENT -komennolla valittua julkista avainta ja aiempaa PSO: HASH -komennolla syötettyä hash-algoritmin tulosta.

TCS_378 Kommentiviesti

Tavu	Pituus	Arvo	Selite
CLA	1	'00h'	CLA
INS	1	'2Ah'	Suorita turvatoimi
P1	1	'00h'	Tuntomerkki: datakentässä on todennettava dataa
P2	1	'A8h'	
Lc	1	'83h'	Seuraavan datakentän pituus Lc
#28	1	'9Eh'	Digitaalisen allekirjoituksen tuntomerkki
#29-#30	2	'8180h'	Digitaalisen allekirjoituksen pituus (128 tavua koodattuna standardin ISO/IEC 7816-6 mukaisesti)
#31-#158	128	'XX..XXh'	Itse digitaalinen allekirjoitus

TCS_379 Vastausviesti

Tavu	Pituus	Arvo	Selite
SW	2	'XXXXh'	Tilaa osoittavat tavut (SW1, SW2)

- Jos komennon suorittaminen onnistui, kortti vastaa '9000'.
- Jos allekirjoituksen todentaminen epäonnistuu, suorittamisen tilaa kuvaava vastaus on '6688'. Todentamisprosessi on kuvattu lisäyksessä 11.
- Jos julkista avainta ei ole valittu, suorittamisen tilaa kuvaava vastaus on '6A88'.
- Jos datasta puuttuu joitain (yllä määriteltyjä) osia, annetaan suorittamisen tilaa kuvaava vastaus '6987'. Näin voi tapahtua, jos jokin vaadituista tuntomerkeistä puuttuu.
- Jos komennon suorittamiseen tarvittavaa hash-algoritmin tulosta ei ole (aiemmin suoritettun PSO: HASH -komennon tuloksena), suorittamisen tilaa kuvaava vastaus on '6985'.
- Jos jotkin datan osat ovat virheellisiä, suorittamisen tilaa kuvaava vastaus on '6988'. Näin voi tapahtua, jos jonkin vaadittavan datan osan pituus on väärä.
- Jos valittu julkinen avain katsotaan virheelliseksi, suorittamisen tilaa kuvaava vastaus on '6400' tai '6581'.

4. AJOPIIRTURIKORTTIEN TIEDOSTORAKENNE

Tässä kohdassa määritellään ajopiirturikorteilla olevan käytettävän datan tallennukseen käytettävät tiedostorakenteet.

Kortin valmistajista riippuvia sisäisiä rakenteita kuten tiedostojen ylätunnisteita ei määritellä tässä, kuten ei myöskään sellaisten dataelementtien tallennusta ja käsittelyä, joita tarvitaan vain sisäiseen käyttöön, esimerkiksi EuropeanPublicKey, CardPrivateKey, TDesSessionKey tai WorkshopCardPin.

Ajopiirturikortin käytettävissä olevan tallennuskapasiteetin on oltava vähintään 11 kilotavua. Suurempia kapasiteetteja saadaan käyttää. Tällaisissa tapauksissa kortin tiedostorakenne pysyy samana, mutta joidenkin rakenteen osien tietueiden määrä kasvaa. Tässä kohdassa määritellään näiden tietueiden vähimmäis- ja enimmäismäärät.

4.1 Kuljettajakortin tiedostorakenne

TCS_400 Sen jälkeen, kun kuljettajakorttiin on liitetty sen yksilöivät tiedot, kortilla on oltava seuraava pysyvä tiedostorakenne ja seuraavat tiedostojen käyttöehdot:

Tiedosto	Tunniste	Käyttöehdot		
		Luku	Päivitys	Salattu
MF	3F00			
└EF ICC	0002	ALW	NEV	Ei
└EF IC	0005	ALW	NEV	Ei
└DF Tachograph	0500			
└└EF Application_Identification	0501	ALW	NEV	Ei
└└EF Card_Certificate	C100	ALW	NEV	Ei
└└EF CA_Certificate	C108	ALW	NEV	Ei
└└EF Identification	0520	ALW	NEV	Ei
└└EF Card_Download	050E	ALW	ALW	Ei
└└EF Driving_Licence_Info	0521	ALW	NEV	Ei
└└EF Events_Data	0502	ALW	PRO SM / AUT	Ei
└└EF Faults_Data	0503	ALW	PRO SM / AUT	Ei
└└EF Driver_Activity_Data	0504	ALW	PRO SM / AUT	Ei
└└EF Vehicles_Used	0505	ALW	PRO SM / AUT	Ei
└└EF Places	0506	ALW	PRO SM / AUT	Ei
└└EF Current_Usage	0507	ALW	PRO SM / AUT	Ei
└└EF Control_Activity_Data	0508	ALW	PRO SM / AUT	Ei
└└EF Specific_Conditions	0522	ALW	PRO SM / AUT	Ei

TCS_401 Kaikkien EF-tiedostorakenteiden on oltava transparent-tyyppisiä.

TCS_402 Tietojen lukemisen salattua sanomanvälitystä käyttäen on oltava mahdollista kaikista DF Tachograph -tiedoston alaisista tiedostoista.

TCS_403 Kuljettajakortilla on oltava seuraava tiedostorakenne:

Tiedosto/Dataelementti	Tietueiden määrä	Koko (tavuina)		Oletusarvot
		Vähintään	Enintään	
MF		11411	24959	
└EF ICC		25	25	
└└CardIccIdentification		25	25	
└└└clockStop		1	1	{00}
└└└cardExtendedSerialNumber		8	8	{00..00}
└└└cardApprovalNumber		8	8	{20..20}
└└└cardPersonaliserID		1	1	{00}
└└└embedderIcAssemblerId		5	5	{00..00}
└└└icIdentifier		2	2	{00 00}
└EF IC		8	8	
└└CardChipIdentification		8	8	
└└└icSerialNumber		4	4	{00..00}
└└└icManufacturingReferences		4	4	{00..00}
└DF Tachograph		11378	24926	
└└EF Application_Identification		10	10	
└└└DriverCardApplicationIdentification		10	10	
└└└└typeOfTachographCardId		1	1	{00}
└└└└cardStructureVersion		2	2	{00 00}
└└└└noOfEventsPerType		1	1	{00}
└└└└noOfFaultsPerType		1	1	{00}
└└└└activityStructureLength		2	2	{00 00}
└└└└noOfCardVehicleRecords		2	2	{00 00}
└└└└noOfCardPlaceRecords		1	1	{00}
└EF Card_Certificate		194	194	
└└CardCertificate		194	194	{00..00}
└EF CA_Certificate		194	194	
└└MemberStateCertificate		194	194	{00..00}
└EF Identification		143	143	
└└CardIdentification		65	65	
└└└cardIssuingMemberState		1	1	{00}
└└└cardNumber		16	16	{20..20}
└└└cardIssuingAuthorityName		36	36	{20..20}
└└└cardIssueDate		4	4	{00..00}
└└└cardValidityBegin		4	4	{00..00}
└└└cardExpiryDate		4	4	{00..00}
└└DriverCardHolderIdentification		78	78	
└└└cardHolderName		72	72	
└└└└holderSurname		36	36	{00, 20..20}
└└└└holderFirstNames		36	36	{00, 20..20}
└└└cardHolderBirthDate		4	4	{00..00}
└└└cardHolderPreferredLanguage		2	2	{20 20}

EF Card_Download		4	4	
LastCardDownload		4	4	
EF Driving_Licence_Info		53	53	
CardDrivingLicenceInformation		53	53	
drivingLicenceIssuingAuthority		36	36	{00, 20..20}
drivingLicenceIssuingNation		1	1	{00}
drivingLicenceNumber		16	16	{20..20}
EF Events_Data		864	1728	
CardEventData		864	1728	
cardEventRecords	6	144	288	
CardEventRecord	n ₁	24	24	
eventType		1	1	{00}
eventBeginTime		4	4	{00..00}
eventEndTime		4	4	{00..00}
eventVehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
EF Faults_Data		576	1152	
CardFaultData		576	1152	
cardFaultRecords	2	288	576	
CardFaultRecord	n ₂	24	24	
faultType		1	1	{00}
faultBeginTime		4	4	{00..00}
faultEndTime		4	4	{00..00}
faultVehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
EF Driver_Activity_Data		5548	13780	
CardDriverActivity		5548	13780	
activityPointerOldestDayRecord		2	2	{00 00}
activityPointerNewestRecord		2	2	{00 00}
activityDailyRecords	n ₆	5544	13776	{00..00}
EF Vehicles_Used		2606	6202	
CardVehiclesUsed		2606	6202	
vehiclePointerNewestRecord		2	2	{00 00}
cardVehicleRecords		2604	6200	
CardVehicleRecord	n ₃	31	31	
vehicleOdometerBegin		3	3	{00..00}
vehicleOdometerEnd		3	3	{00..00}
vehicleFirstUse		4	4	{00..00}
vehicleLastUse		4	4	{00..00}
vehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
vuDataBlockCounter		2	2	{00 00}
EF Places		841	1121	
CardPlaceDailyWorkPeriod		841	1121	
placePointerNewestRecord		1	1	{00}
placeRecords		840	1120	
PlaceRecord	n ₄	10	10	
entryTime		4	4	{00..00}
entryTypeDailyWorkPeriod		1	1	{00}
dailyWorkPeriodCountry		1	1	{00}
dailyWorkPeriodRegion		1	1	{00}
vehicleOdometerValue		3	3	{00..00}
EF Current_Usage		19	19	
CardCurrentUse		19	19	
sessionOpenTime		4	4	{00..00}
sessionOpenVehicle				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
EF Control_Activity_Data		46	46	
CardControlActivityDataRecord		46	46	
controlType		1	1	{00}
controlTime		4	4	{00..00}
controlCardNumber				
cardType		1	1	{00}
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
controlVehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
controlDownloadPeriodBegin		4	4	{00..00}
controlDownloadPeriodEnd		4	4	{00..00}
EF Specific_Conditions		280	280	
SpecificConditionRecord	56	5	5	
entryTime		4	4	{00..00}
SpecificConditionType		1	1	{00}

TCS_404 Seuraavat arvot, joita on käytetty määräämään edellä olevassa taulukossa olevien tiedostojen koot, ovat pienimmät ja suurimmat tietueiden määrät, joita kuljettajakortin tiedostorakenteessa saa käyttää:

		Vähintään	Enintään
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 tavua (28 päivää * 93 toiminnan tilan muutosta)	13 776 tavua (28 päivää * 240 toiminnan tilan muutosta)

4.2 Korjaamokortin tiedostorakenne

TCS_405 Sen jälkeen, kun korjaamokorttiin on liitetty sen yksilöivät tiedot, kortilla on oltava seuraava pysyvä tiedostorakenne ja seuraavat tiedostojen käyttöehdot:

Tiedosto	Tunniste	Käyttöehdot		
		Luku	Päivitys	Salattu
MF	3F00			
EF ICC	0002	ALW	NEV	Ei
EF IC	0005	ALW	NEV	Ei
DF Tachograph	0500			
EF Application_Identification	0501	ALW	NEV	Ei
EF Card_Certificate	C100	ALW	NEV	Ei
EF CA_Certificate	C108	ALW	NEV	Ei
EF Identification	0520	ALW	NEV	Ei
EF Card_Download	0509	ALW	ALW	Ei
EF Calibration	050A	ALW	PRO SM / AUT	Ei
EF Sensor_Installation_Data	050B	ALW	NEV	Kyllä
EF Events_Data	0502	ALW	PRO SM / AUT	Ei
EF Faults_Data	0503	ALW	PRO SM / AUT	Ei
EF Driver_Activity_Data	0504	ALW	PRO SM / AUT	Ei
EF Vehicles_Used	0505	ALW	PRO SM / AUT	Ei
EF Places	0506	ALW	PRO SM / AUT	Ei
EF Current_Usage	0507	ALW	PRO SM / AUT	Ei
EF Control_Activity_Data	0508	ALW	PRO SM / AUT	Ei
EF Specific_Conditions	0522	ALW	PRO SM / AUT	Ei

TCS_406 Kaikkien EF-tiedostorakenteiden on oltava transparent-tyyppisiä.

TCS_407 Tietojen lukemisen salattua sanomanvälitystä käyttäen on oltava mahdollista kaikista DF Tachograph -tiedoston alaisista tiedostoista.

TCS_408 Korjaamokortilla on oltava seuraava tiedostorakenne:

Tiedosto/Dataelementti	Tietueiden määrä	Koko (tavuina)		Oletusarvot
		Vähintään	Enintään	
MF		11088	29061	
EF ICC		25	25	
CardIccIdentification		25	25	
clockStop		1	1	{00}
cardExtendedSerialNumber		8	8	{00..00}
cardApprovalNumber		8	8	{20..20}
cardPersonaliserID		1	1	{00}
embedderIcAssemblerId		5	5	{00..00}
icIdentifier		2	2	{00 00}
EF IC		8	8	
CardChipIdentification		8	8	
icSerialNumber		4	4	{00..00}
icManufacturingReferences		4	4	{00..00}
DF Tachograph		11055	29028	
EF Application_Identification		11	11	
WorkshopCardApplicationIdentification		11	11	
typeOfTachographCardId		1	1	{00}
cardStructureVersion		2	2	{00 00}
noOfEventsPerType		1	1	{00}
noOfFaultsPerType		1	1	{00}
activityStructureLength		2	2	{00 00}
noOfCardVehicleRecords		2	2	{00 00}
noOfCardPlaceRecords		1	1	{00}
noOfCalibrationRecords		1	1	{00}

EF Card_Certificate	194	194	
CardCertificate	194	194	{00..00}
EF CA_Certificate	194	194	
MemberStateCertificate	194	194	{00..00}
EF Identification	211	211	
CardIdentification	65	65	
cardIssuingMemberState	1	1	{00}
cardNumber	16	16	{20..20}
cardIssuingAuthorityName	36	36	{00, 20..20}
cardIssueDate	4	4	{00..00}
cardValidityBegin	4	4	{00..00}
cardExpiryDate	4	4	{00..00}
WorkshopCardHolderIdentification	146	146	
workshopName	36	36	{00, 20..20}
workshopAddress	36	36	{00, 20..20}
cardHolderName			
holderSurname	36	36	{00, 20..20}
holderFirstNames	36	36	{00, 20..20}
cardHolderPreferredLanguage	2	2	{20 20}
EF Card_Download	2	2	
NoOfCalibrationsSinceDownload	2	2	{00 00}
EF Calibration	9243	26778	
WorkshopCardCalibrationData	9243	26778	
calibrationTotalNumber	2	2	{00 00}
calibrationPointerNewestRecord	1	1	{00}
calibrationRecords	9240	26775	
WorkshopCardCalibrationRecord	n ₅	105	105
calibrationPurpose	1	1	{00}
vehicleIdentificationNumber	17	17	{20..20}
vehicleRegistration			
vehicleRegistrationNation	1	1	{00}
vehicleRegistrationNumber	14	14	{00, 20..20}
wVehicleCharacteristicConstant	2	2	{00 00}
kConstantOfRecordingEquipment	2	2	{00 00}
lTyreCircumference	2	2	{00 00}
tyreSize	15	15	{20..20}
authorisedSpeed	1	1	{00}
oldOdometerValue	3	3	{00..00}
newOdometerValue	3	3	{00..00}
oldTimeValue	4	4	{00..00}
newTimeValue	4	4	{00..00}
nextCalibrationDate	4	4	{00..00}
vuPartNumber	16	16	{20..20}
vuSerialNumber	8	8	{00..00}
sensorSerialNumber	8	8	{00..00}
EF Sensor_Installation_Data	16	16	
SensorInstallationSecData	16	16	{00..00}
EF Events_Data	432	432	
CardEventData	432	432	
cardEventRecords	6	72	72
CardEventRecord	n ₁	24	24
eventType	1	1	{00}
eventBeginTime	4	4	{00..00}
eventEndTime	4	4	{00..00}
eventVehicleRegistration			
vehicleRegistrationNation	1	1	{00}
vehicleRegistrationNumber	14	14	{00, 20..20}
EF Faults_Data	288	288	
CardFaultData	288	288	
cardFaultRecords	2	144	144
CardFaultRecord	n ₂	24	24
faultType	1	1	{00}
faultBeginTime	4	4	{00..00}
faultEndTime	4	4	{00..00}
faultVehicleRegistration			
vehicleRegistrationNation	1	1	{00}
vehicleRegistrationNumber	14	14	{00, 20..20}
EF Driver_Activity_Data	202	496	
CardDriverActivity	202	496	
activityPointerOldestDayRecord	2	2	{00 00}
activityPointerNewestRecord	2	2	{00 00}
activityDailyRecords	n ₆	198	492
EF Vehicles_Used	126	250	
CardVehiclesUsed	126	250	
vehiclePointerNewestRecord	2	2	{00 00}
cardVehicleRecords	124	248	
CardVehicleRecord	n ₃	31	31
vehicleOdometerBegin	3	3	{00..00}

vehicleOdometerEnd		3	3	{00..00}
vehicleFirstUse		4	4	{00..00}
vehicleLastUse		4	4	{00..00}
vehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
vuDataBlockCounter		2	2	{00 00}
EF Places		61	81	
CardPlaceDailyWorkPeriod		61	81	
placePointerNewestRecord		1	1	{00}
placeRecords		60	80	
PlaceRecord	n ₄	10	10	
entryTime		4	4	{00..00}
entryTypeDailyWorkPeriod		1	1	{00}
dailyWorkPeriodCountry		1	1	{00}
dailyWorkPeriodRegion		1	1	{00}
vehicleOdometerValue		3	3	{00..00}
EF Current_Usage		19	19	
CardCurrentUse		19	19	
sessionOpenTime		4	4	{00..00}
sessionOpenVehicle				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
EF Control_Activity_Data		46	46	
CardControlActivityDataRecord		46	46	
controlType		1	1	{00}
controlTime		4	4	{00..00}
controlCardNumber				
cardType		1	1	{00}
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
controlVehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
controlDownloadPeriodBegin		4	4	{00..00}
controlDownloadPeriodEnd		4	4	{00..00}
EF Specific_Conditions		10	10	
SpecificConditionRecord	2	5	5	
entryTime		4	4	{00..00}
SpecificConditionType		1	1	{00}

TCS_409 Seuraavat arvot, joita on käytetty määräämään edellä olevassa taulukossa olevien tiedostojen koot, ovat pienimmät ja suurimmat tietueiden määrät, joita korjaamokortin tiedostorakenteessa saa käyttää:

		Vähintään	Enintään
n ₁	NoOfEventsPerType	3	3
n ₂	NoOfFaultsPerType	6	6
n ₃	NoOfCardVehicleRecords	4	8
n ₄	NoOfCardPlaceRecords	6	8
n ₆	CardActivityLengthRange	88	255
n ₅	NoOfCalibrationRecords	198 tavua (1 päivä * 93 toiminnan tilan muutosta)	492 tavua (1 päivä * 240 toimin- nan tilan muutosta)

4.3 Valvontakortin tiedostorakenne

TCS_410 Sen jälkeen, kun valvontakorttiin on liitetty sen yksilöivät tiedot, kortilla on oltava seuraava pysyvä tiedostorakenne ja seuraavat tiedostojen käyttöehdot:

Tiedosto	Tunniste	Käyttöehdot		
		Luku	Päivitys	Salattu
MF	3F00			
EF ICC	0002	ALW	NEV	Ei
EF IC	0005	ALW	NEV	Ei
DF Tachograph	0500			
EF Application_Identification	0501	ALW	NEV	Ei
EF Card_Certificate	C100	ALW	NEV	Ei
EF CA_Certificate	C108	ALW	NEV	Ei
EF Identification	0520	AUT	NEV	Ei
EF Controller_Activity_Data	050C	ALW	PRO SM / AUT	Ei

TCS_411 Kaikkien EF-tiedostorakenteiden on oltava transparent-tyyppisiä.

TCS_412 Tietojen lukemisen salattua sanomanvälitystä käyttäen on oltava mahdollista kaikista DF Tachograph -tiedoston alaisista tiedostoista.

TCS_413 Valvontakortilla on oltava seuraava tiedostorakenne:

Tiedosto/Dataelementti	Tietueiden määrä	Koko (tavuina)		Oletusarvot
		Vähintään	Enintään	
MF		11219	24559	
EF ICC		25	25	
CardIccIdentification		25	25	
clockStop		1	1	{00}
cardExtendedSerialNumber		8	8	{00..00}
cardApprovalNumber		8	8	{20..20}
cardPersonaliserID		1	1	{00}
embedderIcAssemblerId		5	5	{00..00}
icIdentifier		2	2	{00 00}
EF IC		8	8	
CardChipIdentification		8	8	
icSerialNumber		4	4	{00..00}
icManufacturingReferences		4	4	{00..00}
DF Tachograph		11186	24526	
EF Application_Identification		5	5	
ControlCardApplicationIdentification		5	5	
typeOfTachographCardId		1	1	{00}
cardStructureVersion		2	2	{00 00}
noOfControlActivityRecords		2	2	{00 00}
EF Card_Certificate		194	194	
CardCertificate		194	194	{00..00}
EF CA_Certificate		194	194	
MemberStateCertificate		194	194	{00..00}
EF Identification		211	211	
CardIdentification		65	65	
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
cardIssuingAuthorityName		36	36	{00, 20..20}
cardIssueDate		4	4	{00..00}
cardValidityBegin		4	4	{00..00}
cardExpiryDate		4	4	{00..00}
ControlCardHolderIdentification		146	146	
controlBodyName		36	36	{00, 20..20}
controlBodyAddress		36	36	{00, 20..20}
cardHolderName				
holderSurname		36	36	{00, 20..20}
holderFirstNames		36	36	{00, 20..20}
cardHolderPreferredLanguage		2	2	{20 20}
EF Controller_Activity_Data		10582	23922	
ControlCardControlActivityData		10582	23922	
controlPointerNewestRecord		2	2	{00 00}
controlActivityRecords		10580	23920	
controlActivityRecord	n ₇	46	46	
controlType		1	1	{00}
controlTime		4	4	{00..00}
controlledCardNumber				
cardType		1	1	{00}
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
controlledVehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
controlDownloadPeriodBegin		4	4	{00..00}
controlDownloadPeriodEnd		4	4	{00..00}

TCS_414 Seuraavat arvot, joita on käytetty määräämään edellä olevassa taulukossa olevien tiedostojen koot, ovat pienimmät ja suurimmat tietueiden määrät, joita valvontakortin tiedostorakenteessa saa käyttää:

		Vähintään	Enintään
n ₇	NoOfControlActivityRecords	230	520

4.4 Yrityskortin tiedostorakenne

TCS_415 Sen jälkeen, kun yrityskorttiin on liitetty sen yksilöivät tiedot, kortilla on oltava seuraava pysyvä tiedostorakenne ja seuraavat tiedostojen käyttöehdot:

Tiedosto	Tunniste	Käyttöehdot		
		Luku	Päivitys	Salattu
MF	3F00			
EF ICC	0002	ALW	NEV	Ei
EF IC	0005	ALW	NEV	Ei
DF Tachograph	0500			
EF Application_Identification	0501	ALW	NEV	Ei
EF Card_Certificate	C100	ALW	NEV	Ei
EF CA_Certificate	C108	ALW	NEV	Ei
EF Identification	0520	AUT	NEV	Ei
EF Company_Activity_Data	050D	ALW	PRO SM / AUT	Ei

TCS_416 Kaikkien EF-tiedostorakenteiden on oltava transparent-tyyppisiä.

TCS_417 Tietojen lukemisen salattua sanomanvälitystä käyttäen on oltava mahdollista kaikista DF Tachograph -tiedoston alaisista tiedostoista.

TCS_418 Yrityskortilla on oltava seuraava tiedostorakenne:

Tiedosto/Dataelementti	Tietueiden määrä	Koko (tavuina)		Oletusarvot
		Vähintään	Enintään	
MF		11147	24487	
EF ICC		25	25	
CardIccIdentification		25	25	
clockStop		1	1	{00}
cardExtendedSerialNumber		8	8	{00..00}
cardApprovalNumber		8	8	{20..20}
cardPersonaliserID		1	1	{00}
embedderIcAssemblerId		5	5	{00..00}
icIdentifier		2	2	{00 00}
EF IC		8	8	
CardChipIdentification		8	8	
icSerialNumber		4	4	{00..00}
icManufacturingReferences		4	4	{00..00}
DF Tachograph		11114	24454	
EF Application_Identification		5	5	
CompanyCardApplicationIdentification		5	5	
typeOfTachographCardId		1	1	{00}
cardStructureVersion		2	2	{00 00}
noOfCompanyActivityRecords		2	2	{00 00}
EF Card_Certificate		194	194	
CardCertificate		194	194	{00..00}
EF CA_Certificate		194	194	
MemberStateCertificate		194	194	{00..00}
EF Identification		139	139	
CardIdentification		65	65	
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
cardIssuingAuthorityName		36	36	{00, 20..20}
cardIssueDate		4	4	{00..00}
cardValidityBegin		4	4	{00..00}
cardExpiryDate		4	4	{00..00}
CompanyCardHolderIdentification		74	74	
companyName		36	36	{00, 20..20}
companyAddress		36	36	{00, 20..20}
cardHolderPreferredLanguage		2	2	{20 20}
EF Company_Activity_Data		10582	23922	
CompanyActivityData		10582	23922	
companyPointerNewestRecord		2	2	{00 00}
companyActivityRecords		10580	23920	
companyActivityRecord	n ₈	46	46	
companyActivityType		1	1	{00}
companyActivityTime		4	4	{00..00}
cardNumberInformation				
cardType		1	1	{00}
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
vehicleRegistrationInformation				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}

cardNumberInformation			
cardType	1	1	{00}
cardIssuingMemberState	1	1	{00}
cardNumber	16	16	{20..20}
downloadPeriodBegin	4	4	{00..00}
downloadPeriodEnd	4	4	{00..00}

TCS_419 Seuraavat arvot, joita on käytetty määräämään edellä olevassa taulukossa olevien tiedostojen koot, ovat pienimmät ja suurimmat tietueiden määrät, joita yrityskortin tiedostorakenteessa saa käyttää:






































		Vähintään	Enintään
ng	NoOfCompanyActivityRecords	230	520

Lisäys 3









KUVAKKEET

PIC_001 Valvontalaite saa käyttää seuraavia kuvakkeita ja kuvakkeiden yhdistelmiä:






1. PERUSKUVAKKEET

	Henkilöt	Toimet	Toimintatilat
	Yritys		Yritystila
	Tarkastaja	Tarkastustoimi	Tarkastustila
	Kuljettaja	Ajo	Normaalitila
	Korjaamo/testausasema	Tarkastus/kalibrointi	Kalibrointitila
	Valmistaja		
	Toiminta	Kesto	
	Varallaolo	Kuluva varallaoloaika	
	Ajo	Keskeytymätön ajoaika	
	Lepo	Kuluva lepoaika	
	Työ	Kuluva työaika	
	Tauko	Yhteenlaskettu tauko aika	
	Tuntematon		
	Laitteet	Toiminnot	
	Kuljettajan korttiaukko		
	Apukuljettajan korttiaukko		
	Kortti		
	Kello		
	Näyttö	Tietojen näyttö	
	Ulkoinen tallennus	Tietojen kopiointi	
	Virtalähde		
	Tulostin/tuloste	Tulostus	
	Liiketunnistin		
	Rengaskoko		
	Ajoneuvo/ajoneuvoyksikkö		
	Erityisolosuhteet		
	OUT Asetuksen piiriin kuulumaton		
	Juna-/lauttamatka		
	Muut		
	! Tapaukset		× Viat
	▶ Päivittäisen työajan alkaminen		▶ Päivittäisen työajan päättymisen
	• Olinpaikka		• Kuljettajan toimintaa koskevien tietojen syöttäminen käsin
	🔒 Tietoturva		➤ Nopeus
	🕒 Aika		Σ Yhteensä/ylhteenveto
	Määrittelyt		
	24h Päivittäin		
	Viikoittain		
	Kaksi viikkoa		
	+ Jostain alkaen tai johonkin asti		




2. KUVAKKEYHDISTELMÄT

	Muut		
	🗄️ Tarkastuspaikka		▶️ Päivän työajan päättymispaikka
	🗄️▶️ Päivän työajan alkamispaikka		➕🗄️ Aikaan
	🗄️➕ Ajasta		
	🗄️➕ Ajoneuvosta		
	OUT➕ Asetuksen piiriin kuulumaton ajo alkaa		➕OUT Asetuksen piiriin kuulumaton ajo päättyy







Kortit

	Kuljettajakortti
	Yrityskortti
	Valvontakortti
	Korjaamokortti
	Ei korttia













Ajo

	Ajo miehitettynä
	Yhden viikon ajoaika
	Kahden viikon ajoaika








Tulosteet

	Kuljettajan toimintaa koskevien tietojen päivittäinen tuloste kortilta
	Kuljettajan toimintaa koskevien tietojen päivittäinen tuloste ajoneuvoyksiköstä
	Tapauksia ja vikoja koskevien tietojen tuloste kortilta
	Tapauksia ja vikoja koskevien tietojen tuloste ajoneuvoyksiköstä
	Teknisten tietojen tuloste
	Ylinopeutta koskevien tietojen tuloste






Tapaukset

	Ei voimassa olevan kortin asettaminen korttiaukkoon
	Korttiristiriitä
	Aikojen päällekkäisyys
	Ajo ilman asianmukaista korttia
	Kortin paikoilleen asetus ajon aikana
	Edellistä kortin käyttöjaksoa ei lopetettu oikein
	Ylinopeus
	Katkos virransyötössä
	Virhe liiketiedoissa
	Tietoturvamurto
	Ajan asetus (korjaamon tekemä)
	Ylinopeuden valvonta

Viat

	Korttivika (kuljettajan korttiaukko)
	Korttivika (apukuljettajan korttiaukko)
	Vika näytössä
	Tietojen kopiointiin liittyvä vika
	Vika tulostimessa
	Vika tunnistimessa
	Vika ajoneuvoyksikön sisällä

Tietojen syöttäminen käsin

	Koskevatko tiedot vielä saman päivän työaikaa?
	Päättyykö edellisen päivän työaika?
	Vahvista tai syötä paikka, jossa työaika päättyi
	Syötä aloitusaika
	Syötä paikka, jossa työaika alkaa

Huomautus: Lisäyksessä 4 on määritelty muita kuvakeyhdistelmiä, joita käytetään tulostettavien lohkojen tai tietueiden tunnisteena.

Lisäys 4

TULOSTEET

SISÄLLYSLUETTELO

1.	Yleistä	131
2.	Datalohkojen erittely	131
3.	Tulosteiden erittelyt	137
3.1	Kortilla olevia kuljettajan toimintaa koskevia tietoja sisältävä päivittäinen tuloste	138
3.2	Ajoneuvoyksikön muistissa olevia kuljettajan toimintaa koskevia tietoja sisältävä päivittäinen tuloste . . .	138
3.3	Kortilla olevia tapauksiin ja vikoihin liittyviä tietoja sisältävä tuloste	139
3.4	Ajoneuvoyksikön muistissa olevia tapauksiin ja vikoihin liittyviä tietoja sisältävä tuloste	139
3.5	Teknisiä tietoja sisältävä tuloste	140
3.6	Ylinopeuteen liittyviä tietoja sisältävä tuloste	140

- 2 **Tulostetyyppi**
Lohkon tunniste
Tulosteen kuvakeyhdistelmä (ks. lisäys 3) Nopeudenrajoittimen asetus (vain ylinopeustapauksia koskeva tuloste)
- 3 **Kortin haltijan tunniste**
Lohkon tunniste. P = henkilöihin liittyvä kuvake
Kortin haltijan sukunimi
Kortin haltijan etunimi (-nimet) (jos sellainen on)
Kortin tunniste
Kortin viimeinen voimassaolopäivä (jos sellainen on)
Jos kortti ei ole henkilökohtainen eikä sisällä kortin haltijan sukunimeä, tulostetaan sen sijaan yrityksen tai korjaamon tai valvontaelimen nimi.
- 4 **Ajoneuvon tunniste**
Lohkon tunniste
Valmistenumero (VIN)
Rekisteröinyt jäsenvaltio ja rekisteritunnus (VRN)
- 5 **Ajoneuvoyksikön tunniste**
Lohkon tunniste
Ajoneuvoyksikön valmistajan nimi
Ajoneuvoyksikön osanumero
- 6 **Valvontalaitteen viimeisin kalibrointi**
Lohkon tunniste
Korjaamon nimi
Korjaamokortin tunniste
Kalibroinnin päivämäärä
- 7 **Viimeisin (valvontaviranomaisen suorittama) tarkastus**
Lohkon tunniste
Valvontakortin tunniste
Tarkastuksen päivämäärä, aika ja tyyppi
Tarkastuksen tyyppi: enintään neljä kuvaketta. Tarkastuksen tyyppi voi olla jokin (yhdistelmä) seuraavista:
■: Kortin tietojen kopiointi, ▾: Ajoneuvoyksikön tietojen kopiointi, ▴: Tulostus, □: Näyttö.
- 8 **Kortille tallennetut kuljettajan toimintaa koskevat tiedot aikajärjestyksessä**
Lohkon tunniste
Kyseinen päivä (kalenterivuorokausi, jota tuloste koskee) + Kortin päivittäisten käyttökertojen laskuri
- 8.1 *Ajanjakso, jolloin kortti ei ollut paikoillaan laitteessa*
- 8.1a Tietueen tunniste (ajanjakson alku)
- 8.1b *Tuntematon ajanjakso.* Alkamis- ja päättymisaika, kesto
- 8.1c *Käsin syötetyt toimintaa koskevat tiedot*
Toimintakuvake, alkamis- ja päättymisajat (jaksoon kuuluvat), kesto, vähintään tunnin kestäneet lepojaksot on merkitty tähdellä.

----- ▴ -----
Picto xxx km/h

----- P -----
P Last_Name _____
First_Name _____
Card_Identification _____
dd/mm/yyyy

----- ▽ -----
▽ VIN _____
Nat/VRN _____

----- □ -----
□ VU_Manufacturer _____
VU_Part_Number _____

----- ▴ -----
▴ Last_Name _____
Card_Identification _____
▴ dd/mm/yyyy

----- □ -----
Card_Identification _____
□ dd/mm/yyyy hh:mm pppp

----- □ -----
dd/mm/yyyy xxx

----- □ -----
? hh:mm hh:mm hh:mm
A hh:mm hh:mm hh:mm *

- 8.2 *Kortin asetus korttiaukkoon S*
Tietueen tunniste; S = Korttiaukkokuvake
Ajoneuvon rekisteröinyt jäsenvaltio ja ajoneuvon rekisteritunnus
Ajoneuvon matkamittarin lukema silloin, kun kortti asetettiin paikoilleen
- 8.3 *Toiminta (kortin ollessa paikoillaan)*
Toimintakuvake, alkamis- ja päättymisajat (jaksoon kuuluvat), kesto, miehitys (miehityskuvake, jos tila on CREW, tyhjää, jos SINGLE), vähintään tunnin kestäneet lepoajat on merkitty tähdellä.
- 8.3a *Erityisolosuhteet.*
Aika, jolloin tieto syötettiin, erityisolosuhteisiin liittyvä kuvake (tai kuvakkeiden yhdistelmä).
- 8.4 *Kortin poisto*
Ajoneuvon matkamittarin lukema ja viimeisen sellaisen kortin paikoilleen asettamisen jälkeen kuljettu matka, jota vastaava matkamittarin lukema on tiedossa
- 9 **Ajoneuvoyksikköön tallennetut kuljettajan toimintaa koskevat tiedot korttiaukoittain aikajärjestyksessä**
Lohkon tunniste
Kyseinen päivä (kalenterivuorokausi, jota tuloste koskee)
Ajoneuvon matkamittarin lukema klo 00:00 ja klo 24:00
- 10 **Korttiaukkoon S liittyvät tehdyt toimet**
Lohkon tunniste
- 10.1 *Jakso, jolloin aukossa S ei ole korttia*
Tietueen tunniste.
Korttia ei ole asetettu
Ajoneuvon matkamittarin lukema jakson alussa
- 10.2 *Kortin paikoilleen asettaminen*
Kortin paikoilleen asetusta koskevan tietueen tunniste
Kuljettajan nimi
Kuljettajan etunimi
Kuljettajakortin tunniste
Kuljettajakortin viimeinen voimassaolopäivä
Kuljettajan tätä ennen käyttämän ajoneuvon rekisteröinyt jäsenvaltio ja ajoneuvon rekisteritunnus
Päivämäärä ja aika, jolloin kortti poistettiin edellisestä ajoneuvosta
Tyhjä rivi
Ajoneuvon matkamittarin lukema korttia paikoilleen asettaessa, kuljettajan toimintaa koskevien tietojen käsin syöttämisestä koskeva tunnusmerkki (M, jos käsin syötetty, muuten tyhjä).
- 10.3 *Toiminta*
Toimintakuvake, alkamis- ja päättymisajat (jaksoon kuuluvat), kesto, miehitys (miehityskuvake, jos tila on CREW, tyhjää, jos SINGLE), vähintään tunnin kestäneet lepoajat on merkitty tähdellä.

```

-----S-----
A Nat/VRN _____
x xxx xxx km

```

```

A hh:mm hh:mm hhhmm ☐☐ *

```

```

hh:mm ----- pppp -----

```

```

x xxx xxx km; x xxx km

```

```

-----☐-----
dd/mm/yyyy
x xxx xxx - x xxx xxx km

```

```

----- S -----

```

```

-----
☐☐ ---
x xxx xxx km

```

```

-----
☐ Last_Name _____
First_Name _____
Card_Identification _____
dd/mm/yyyy
A + Nat/VRN _____
dd/mm/yyyy hh:mm
x xxx xxx km M

```

```

A hh:mm hh:mm hhhmm ☐☐ *

```


11.8 Toiminnan kokonaiskestoajat (kuljettajaa kohden molemmat kortti-
aukot mukaan lukien)

Kokonaisajoaika, kuljettu matka
Työn ja varallaolon kokonaisaika
Kokonaislepoaika

Ajoneuvon miehistön toiminnan kokonaisaika

Tarvittaessa kuluva päivää koskeva päivittäinen tuloste, päivittäiset yhteenvetotiedot lasketaan tiedoista, jotka ovat käytävissä tulostushetkellä.

⊠ hhhmm x xxx km
✱ hhhmm ⊠ hhhmm
⌂ hhhmm
⊠ ⊠ hhhmm

12 Kortille tallennetut tapauksia ja/tai vikoja koskevat tiedot

12.1 Viittä viimeistä tapausta ja vikaa koskevan kortilla olevan tietuelohkon tunniste

----- ! ✱ ⊠ -----

12.2 Kaikkia tallennettuja tapauksia koskevan kortilla olevan tietuelohkon tunniste

----- ! ⊠ -----

12.3 Kaikkia tallennettuja vikoihin liittyviä tietoja koskevan kortilla olevan tietuelohkon tunniste

----- ✱ ⊠ -----

12.4 Tapausta ja/tai vikaa koskeva tietue

Tietueen tunniste

Tapausta/vikaa tarkoittava kuvake, syy tietojen tallentamiseen, alkamispäivämäärä ja -aika

Lisätietona annettu tapauksen/vian tunnus (jos on), kesto

Sen ajoneuvon rekisteröinyt jäsenvaltio ja sen ajoneuvon rekisteritunnus, jossa tapaus tai vika sattui

Pic _____ dd/mm/yyyy hh:mm
! xxx hh:mm
⌂ Nat/VRN _____

13 Ajoneuvoyksikköön tallennetut tai meneillään olevia tapauksia ja/tai vikoja koskevat tiedot

13.1 Viittä viimeistä tapausta ja vikaa koskevan, ajoneuvoyksikön muistissa olevan tietuelohkon tunniste

----- ! ✱ ⌂ -----

13.2 Kaikkia tallennettuja tai meneillään olevia tapauksia koskevan, ajoneuvoyksikön muistissa olevan tietuelohkon tunniste

----- ! ⌂ -----

13.3 Kaikkia tallennettuja tai meneillään oleviin vikoihin liittyviä tietoja koskevan, ajoneuvoyksikön muistissa olevan tietuelohkon tunniste

----- ✱ ⌂ -----

13.4 Tapausta ja/tai vikaa koskeva tietue

Tietueen tunniste

Tapausta/vikaa tarkoittava kuvake, syy tietojen tallentamiseen, alkamispäivämäärä ja -aika

Lisätietona annettu tapauksen/vian tunnus (jos on), kyseisenä päivänä sattuneiden vastaavien tapausten määrä, kesto

Tapauksen tai vikatapahtuman alkaessa paikoilleen asetettuna olleiden korttien tunnistet (enintään neljä tunnistetta ilman, että samoja kortin numeroita toistetaan)

Jos mitään korttia ei ollut asetettu paikoilleen:

Tietojen tallentamisen syy (p) on numerotunnus, joka ilmaisee, miksi tapausta tai vikaa koskevat tiedot tallennettiin. Tunnus koodataan dataelementin EventFaultRecord-Purpose määrittelyn mukaisesti.

Pic (p) dd/mm/yyyy hh:mm
! xxx (xxx) hh:mm
Card_Identification _____
Card_Identification _____
Card_Identification _____
Card_Identification _____
⊠ ---

14 Ajoneuvoyksikön tunniste

Lohkon tunniste
 Ajoneuvoyksikön valmistajan nimi
 Ajoneuvoyksikön valmistajan osoite
 Ajoneuvoyksikön osanumero
 Ajoneuvoyksikön hyväksyntänumero
 Ajoneuvoyksikön sarjanumero
 Ajoneuvoyksikön valmistusvuosi
 Ajoneuvoyksikön ohjelmiston versio ja asennuspäivä

```

-----E-----
E Name _____
  Address _____
  PartNumber _____
  Apprv _____
  S/N _____
  YYYY
  V  xx.xx.xx  dd/mm/yyyy
  
```

15 Liiketunnistimen tunniste

Lohkon tunniste
 Liiketunnistimen sarjanumero
 Liiketunnistimen hyväksyntänumero
 Päivämäärä, jolloin liiketunnistin ensi kerran asennettiin

```

-----L-----
L S/N _____
  Apprv _____
  dd/mm/yyyy
  
```

16 Kalibrointeihin liittyvät tiedot

Lohkon tunniste

```

-----T-----
  
```

16.1 Kalibrointiin liittyvä tietue

Tietueen tunniste
 Kalibroinnin suorittanut korjaamo
 Korjaamon osoite
 Korjaamokortin tunniste
 Korjaamokortin viimeinen voimassaolopäivä
 Tyhjä rivi
 Kalibroinnin päivämäärä + kalibroinnin tarkoitus
 Ajoneuvon valmistenumero
 Rekisteröinyt jäsenvaltio ja ajoneuvon rekisteritunnus
 Ajoneuvon ominaiskerroin
 Valvontalaitteen vakio
 Pyörien renkaiden tehollinen ympärysmitta
 Ajoneuvoon asennettujen renkaiden koko
 Nopeudenrajoittimen asetus
 Vanha ja uusi matkamittarin lukema
 Kalibroinnin tarkoitus (p) on numerotunnus, joka ilmaisee, miksi kalibrointiparametrit tallennettiin. Tunnus koodataan datalementin CalibrationPurpose määrittelyn mukaisesti.

```

-----
T Workshop_name _____
  Workshop_address _____
Card-Identification _____
  dd/mm/yyyy

T dd/mm/yyyy (p)
A VIN _____
  Nat/VRN _____
w xx xxx Imp/km
k xx xxx Imp/km
l xx xxx mm
● TyreSize _____
> xxx km/h
x xxx xxx - x xxx xxx km
  
```

17 Ajan asetus

Lohkon tunniste

```

-----G-----
  
```

17.1 Ajan asetusta koskeva tietue

Tietueen tunniste
 Vanha päivämäärä ja aika
 Uusi päivämäärä ja aika
 Korjaamo, joka suoritti ajan asetuksen
 Korjaamon osoite
 Korjaamokortin tunniste
 Korjaamokortin viimeinen voimassaolopäivä

```

-----
! G dd/mm/yyyy hh:mm
  G dd/mm/yyyy hh:mm
T Workshop_name _____
  Workshop_address _____
Card_Identification _____
  dd/mm/yyyy
  
```


18 **Viimeisin ajoneuvoyksikön muistiin tallennettu tapaus ja vika**

Lohkon tunniste

Viimeisimmän tapauksen päivämäärä ja aika

Viimeisimmän vian päivämäärä ja aika

```
----- ! x A -----
! dd/mm/yyyy hh:mm
x dd/mm/yyyy hh:mm
```

19 **Ylinopeuden valvontaan liittyvät tiedot**

Lohkon tunniste

Viimeisimmän OVER SPEEDING CONTROL -tarkastustoimenpiteen päivämäärä ja aika

Ensimmäisen ylinopeustapauksen päivämäärä ja aika sekä sen jälkeen sattuneiden ylinopeustapauksien määrä

```
----- >> -----
> dd/mm/yyyy hh:mm
>> dd/mm/yyyy hh:mm (nnn)
```

20 **Ylinopeuteen liittyvä tietue**

20.1 Ensimmäistä viimeisimmän kalibroinnin jälkeen sattunutta ylinopeustapausta koskevan tietuelohkon tunniste

```
----- >>T -----
```

20.2 Viittä vakavinta 365 viimeisimmän vuorokauden aikana sattunutta ylinopeustapausta koskevan tietuelohkon tunniste

```
----- >> (365) -----
```

20.3 Sen tietuelohkon tunniste, joka sisältää tiedot vakavimmista tapauksista kultakin niistä 10 viimeisimmästä päivästä, jolloin tapauksia sattui

```
----- >> (10) -----
```

20.4 Tietueen tunniste

Päivämäärä, aika ja kesto

Enimmäisnopeus ja keskimääräinen nopeus, kyseisenä päivänä sattuneiden vastaavien tapausten määrä

Kuljettajan sukunimi

Kuljettajan etunimi (etunimet)

Kuljettajakortin tunniste

```
-----
>> dd/mm/yyyy hh:mm hh:mm
xxx km/h xxx km/h (xxx)
@ Last_Name _____
First_Name _____
Card_Identification _____
```

20.5 Jos lohkoissa ole yhtään ylinopeutta koskevaa tietuetta:

```
>> - - -
```

21 **Käsin kirjoitetut tiedot**

Lohkon tunniste

21.1 Tarkastuspaikka

21.2 Tarkastajan allekirjoitus

21.3 Alkoi

21.4 Päätyi

21.5 Kuljettajan allekirjoitus

Käsin kirjoitettuja tietoja ennen on asetettava riittävä määrä tyhjiä rivejä, jotta tarvittavat tiedot tai allekirjoitus mahtuvat niille varatuille paikoille.

```
-----
@ * .....
@ .....
@ + .....
+ @ .....
@ .....
```

3. TULOSTEIDEN ERITTELYT

Tässä luvussa käytetään seuraavia muotoilujen merkintätapoja:

N
N
X/Y

Tulostetaan tulostelohko tai tietue numero N

Tulostetaan tulostelohko tai tietue numero N niin monta kertaa kuin on tarpeen

Tulostetaan tarpeen mukaan lohko tai tietue X ja/tai Y niin monta kertaa kuin on tarpeen.

3.1. Kortilla olevia kuljettajan toimintaa koskevia tietoja sisältävä päivittäinen tuloste

PRT_007 Kortilla olevia kuljettajan toimintaa koskevia tietoja sisältävän päivittäisen tulosteen on oltava seuraavassa muodossa:

1	Päivämäärä ja aika, jolloin asiakirja tulostettiin
2	Tulosteen tyyppi
3	Tarkastajan tunniste (jos ajoneuvoyksikköön on asetettu valvontakortti)
3	Kuljettajan tunniste (kortilta, jota tuloste koskee)
4	Ajoneuvon tunniste (ajoneuvon, jota tuloste koskee)
5	Ajoneuvoyksikön tunniste (ajoneuvoyksikön, jonka kautta tuloste tehtiin)
6	Kyseisen ajoneuvoyksikön viimeisin kalibrointi
7	Edellinen tarkastustoimi, jonka kohteena nyt tarkastettava kuljettaja on ollut
8	Kuljettajan toimintaa koskevien tietojen erotinmerkki
8.1a / 8.1b / 8.1c / 8.2 / 8.3 / 8.3a / 8.4	Kuljettajan toimintaa koskevat tiedot aikajärjestyksessä
11	Päivittäisen yhteenvedon erotinmerkki
11.4	Syötetyt paikkoja koskevat tiedot aikajärjestyksessä
11.5	Toiminnan kokonaiskestoajat
12.1	Kortilta tulostettavien tapauksia tai vikoja koskevien tietojen erotinmerkki
12.4	Tapauksia/vikoja koskevat tietueet (viisi viimeistä kortille tallennettua tapausta tai vikaa)
13.1	Ajoneuvoyksikön muistista tulostettavien tapauksia tai vikoja koskevien tietojen erotinmerkki
13.4	Tapauksia/vikoja koskevat tietueet (viisi viimeistä ajoneuvoyksikön muistiin tallennettua tai meneillään olevaa tapausta tai vikaa)
21.1	Tarkastuspaikka
21.2	Tarkastajan allekirjoitus
21.5	Kuljettajan allekirjoitus

3.2. Ajoneuvoyksikön muistissa olevia kuljettajan toimintaa koskevia tietoja sisältävä päivittäinen tuloste

PRT_008 Ajoneuvoyksikön muistissa olevia kuljettajan toimintaa koskevia tietoja sisältävän päivittäisen tulosteen on oltava seuraavassa muodossa:

1	Päivämäärä ja aika, jolloin asiakirja tulostettiin
2	Tulosteen tyyppi
3	Kortin haltijan tunniste (kaikkien ajoneuvoyksikössä olevien korttien)
4	Ajoneuvon tunniste (sen ajoneuvon, jota tuloste koskee)
5	Ajoneuvoyksikön tunniste (ajoneuvoyksikön, jota tuloste koskee)
6	Kyseisen ajoneuvoyksikön viimeisin kalibrointi
7	Viimeisin kyseiseen valvontalaitteeseen kohdistunut tarkastus
9	Kuljettajan toimintaa koskevien tietojen erotinmerkki
10	Kuljettajan korttiaukon erotinmerkki (korttiaukko 1)
10.1 / 10.2 / 10.3 / 10.3a / 10.4	Toimintaan liittyvät tiedot aikajärjestyksessä (kuljettajan korttiaukko)
10	Apukuljettajan korttiaukon erotinmerkki (korttiaukko 2)
10.1 / 10.2 / 10.3 / 10.3a / 10.4	Toimintaan liittyvät tiedot aikajärjestyksessä (apukuljettajan korttiaukko)
11	Päivittäisen yhteenvedon erotinmerkki
11.1	Niiden jaksojen yhteenvedo, jolloin kuljettajan korttiaukossa ei ollut korttia
11.4	Syötetyt paikkoja koskevat tiedot aikajärjestyksessä
11.6	Toiminnan kokonaiskestoajat

11.2	Niiden jaksojen yhteenveto, jolloin apukuljettajan korttiaukossa ei ollut korttia
11.4	Syötetyt paikkoja koskevat tiedot aikajärjestyksessä
11.7	Toiminnan kokonaiskestoajat
11.3	Tietyn kuljettajan toimintaa koskevien tietojen yhteenveto molemmat korttipaikat mukaan lukien
11.4	Kyseisen kuljettajan syöttämät paikkoihin liittyvät tiedot aikajärjestyksessä
11.7	Kyseisen kuljettajan toiminnan kokonaiskestoajat
13.1	Tapauksiin/vikoihin liittyvien tietojen erotinmerkki
13.4	Tapauksiin/vikoihin liittyvät tietueet (viisi viimeistä ajoneuvoyksikön muistiin tallennettua tai meneillään olevaa tapausta tai vikaa)
21.1	Tarkastuspaikka
21.2	Tarkastajan allekirjoitus
21.3	Alkamisaika (tila, johon ilman korttia oleva kuljettaja voi merkitä kyseiset ajat)
21.4	Päätymisaika
21.5	Kuljettajan allekirjoitus

3.3. Kortilla olevia tapauksiin ja vikoihin liittyviä tietoja sisältävä tuloste

PRT_009 Kortilla olevia tapauksiin ja vikoihin liittyviä tietoja sisältävän tulosteen on oltava seuraavassa muodossa:

1	Päivämäärä ja aika, jolloin asiakirja tulostettiin
2	Tulosteen tyyppi
3	Tarkastajan tunniste (jos ajoneuvoyksikköön on asetettu valvontakortti)
3	Kuljettajan tunniste (kortilta, jota tuloste koskee)
4	Ajoneuvon tunniste (sen ajoneuvon, jota tuloste koskee)
12.2	Tapauksiin liittyvien tietojen erotinmerkki
12.4	Tapauksiin liittyvät tietueet (kaikki kortille tallennetut tapaukset)
12.3	Vikoihin liittyvien tietojen erotinmerkki
12.4	Vikoihin liittyvät tietueet (kaikki kortille tallennetut viat)
21.1	Tarkastuspaikka
21.2	Tarkastajan allekirjoitus
21.5	Kuljettajan allekirjoitus

3.4. Ajoneuvoyksikön muistissa olevia tapauksiin ja vikoihin liittyviä tietoja sisältävä tuloste

PRT_010 Ajoneuvoyksikön muistissa olevia tapauksiin ja vikoihin liittyviä tietoja sisältävän tulosteen on oltava seuraavassa muodossa:

1	Päivämäärä ja aika, jolloin asiakirja tulostettiin
2	Tulosteen tyyppi
3	Kortin haltijan tunniste (kaikkien ajoneuvoyksikössä olevien korttien)
4	Ajoneuvon tunniste (sen ajoneuvon, jota tuloste koskee)
13.2	Tapauksiin liittyvien tietojen erotinmerkki
13.4	Tapauksiin liittyvät tietueet (kaikki ajoneuvoyksikön muistiin tallennetut tai meneillään olevat tapaukset)
13.3	Vikoihin liittyvien tietojen erotinmerkki
13.4	Vikoihin liittyvät tietueet (kaikki ajoneuvoyksikön muistiin tallennetut tai meneillään olevat viat)
21.1	Tarkastuspaikka
21.2	Tarkastajan allekirjoitus
21.5	Kuljettajan allekirjoitus

3.5. Teknisiä tietoja sisältävä tuloste

PRT_011 Teknisiä tietoja sisältävän tulosteen on oltava seuraavassa muodossa:

1	Päivämäärä ja aika, jolloin asiakirja tulostettiin
2	Tulosteen tyyppi
3	Kortin haltijan tunniste (kaikkien ajoneuvoyksikössä olevien korttien)
4	Ajoneuvon tunniste (sen ajoneuvon, jota tuloste koskee)
14	Ajoneuvoyksikön tunniste
15	Liiketunnistimen tunniste
16	Kalibrointiin liittyvien tietueiden erotinmerkki
16.1	Kalibrointeihin liittyvät tietueet (kaikki käytettävissä olevat tietueet aikajärjestyksessä)
17	Ajan asetuksen erotinmerkki
17.1	Ajan asetukseen liittyvät tietueet (kaikki käytettävissä olevat ajan asetukseen liittyvissä ja kalibrointitiedoissa olevat tietueet)
18	Viimeisin ajoneuvoyksikön muistiin tallennettu tapaus ja vika

3.6. Ylinopeuteen liittyviä tietoja sisältävä tuloste

PRT_012 Ylinopeuteen liittyviä tietoja sisältävän tulosteen on oltava seuraavassa muodossa:

1	Päivämäärä ja aika, jolloin asiakirja tulostettiin
2	Tulosteen tyyppi
3	Kortin haltijan tunniste (kaikkien ajoneuvoyksikössä olevien korttien)
4	Ajoneuvon tunniste (sen ajoneuvon, jota tuloste koskee)
19	Ylinopeusvalvontaan liittyvät tiedot
20.1	Ylinopeuteen liittyvien tietojen tunniste
20.4 / 20.5	Ensimmäinen ylinopeustapaus viimeisimmän kalibroinnin jälkeen
20.2	Ylinopeuteen liittyvien tietojen tunniste
20.4 / 20.5	Viisi vakavinta ylinopeustapausta 365 viimeisimmän vuorokauden aikana
20.3	Ylinopeuteen liittyvien tietojen tunniste
20.4 / 20.5	Vakavin ylinopeustapaus kultakin niistä 10 viimeisimmästä päivästä, jolloin tapauksia sattui
21.1	Tarkastuspaikka
21.2	Tarkastajan allekirjoitus
21.5	Kuljettajan allekirjoitus

Lisäys 5

NÄYTTÖ

Tässä lisäyksessä käytetään seuraavia merkintätapoja:

- **lihavoitu** teksti merkitsee tavallista tekstiä, joka näytetään (näytössä ei käytetä lihavoitua tekstiä),
- normaali teksti merkitsee muuttujia (kuvakkeita tai dataa), jotka tulostettaessa korvataan vastaavilla muuttujan arvoilla:
 - dd mm yyyy: päivä, kuukausi, vuosi,
 - hh: tunnit,
 - mm: minuutit,
 - D: kestoaikaa merkitsevä kuvake,
 - EF: tapausta tai vikaa merkitsevien kuvakkeiden yhdistelmä,
 - O: toimintatilaa merkitsevä kuvake.

DIS_001 Valvontalaitteen on näytettävä tiedot seuraavassa muodossa:

Tiedot	Format (Muoto)
Oletusarvoinen näyttö	
Paikallinen aika	hh:mm
Toimintatila	O
Kuljettajaan liittyvät tiedot	1 Dhhmm ■■hhmm
Apukuljettajaan liittyvät tiedot	2 Dhhmm
Asetuksen piiriin kuulumaton olosuhde voimassa	OUT
Varoitusnäyttö	
Keskeytymätön ajoaika yli sallitun	1 0hhmm ■■hhmm
Tapaus tai vika	EF
Muut näytöt	
UTC-päivämäärä	UTC 0 dd/mm/yyyy tai UTC 0 dd.mm.yyyy
aika	hh:mm
Kuljettajan keskeytymätön ajoaika ja yhteenlaskettu tauko-aika	1 0hhmm ■■hhmm
Apukuljettajan keskeytymätön ajoaika ja yhteenlaskettu tauko-aika	2 0hhmm ■■hhmm
Kuljettajan yhteenlaskettu ajoaika edellisen ja kuluvan viikon aikana	1 0 hhhhmm
Apukuljettajan yhteenlaskettu ajoaika edellisen ja kuluvan viikon aikana	2 0 hhhhmm

Lisäys 6

ULKOISET LIITÄNTÄLAITTEET

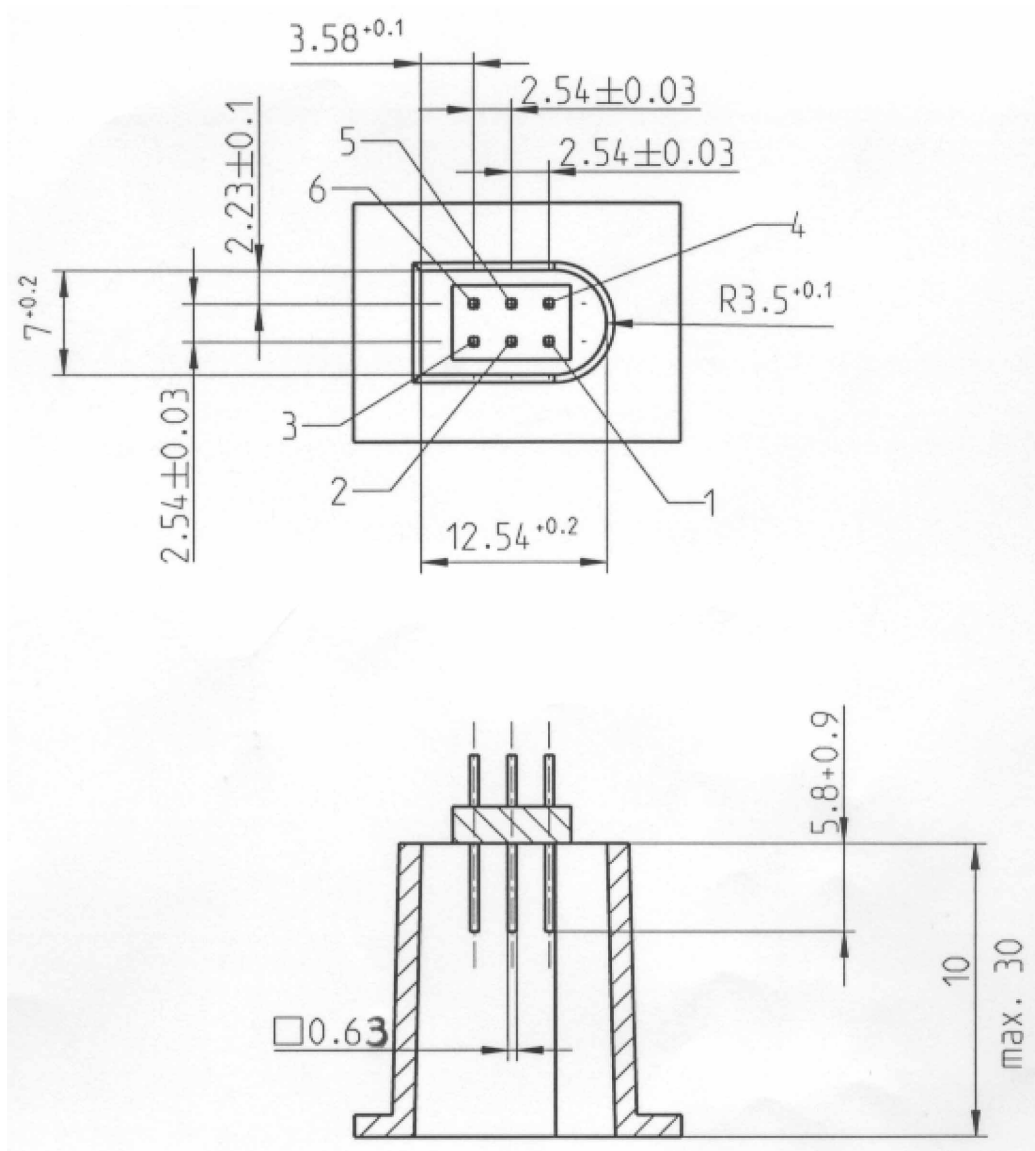
SISÄLLYSLUETTELO

1.	Laitteet	144
1.1	Liitin	144
1.2	Liittimen johdotus	146
1.3	Lohkokaavio	146
2.	Tietojen kopioinnissa käytettävä liitäntälaite	146
3.	Kalibroinnissa käytettävä liitäntälaite	147

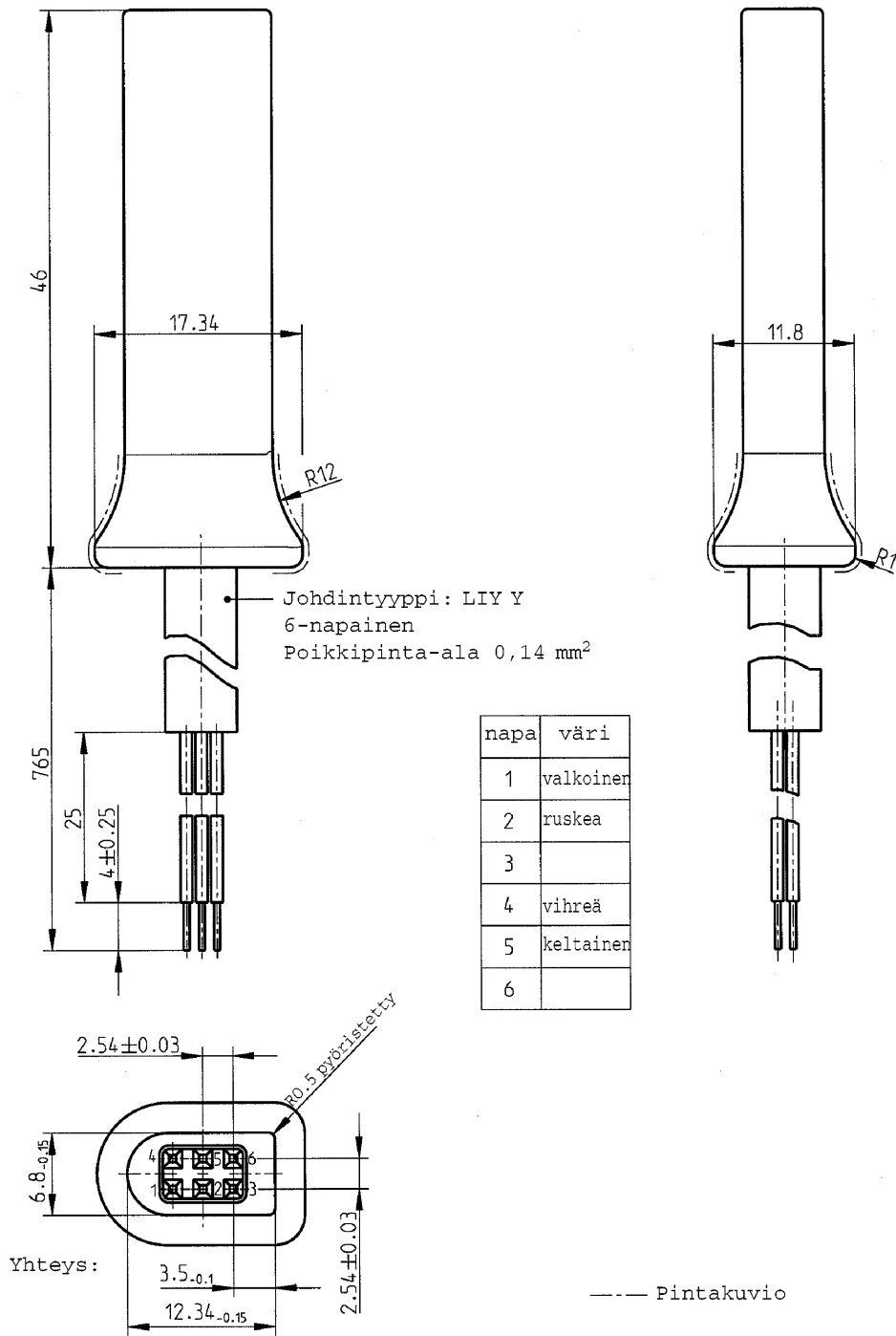
1. LAITTEET

1.1 Liitin

INT_001 Tietojen kopiointiin ja kalibrointiin käytettävän liittimen on oltava kuusinapainen ja sen on oltava käsillä laitteen etulevyssä ilman, että on tarpeen irrottaa mitään valvontalaitteen osaa. Liittimen on oltava seuraavan piirroksen mukainen (kaikki mitat millimetreinä):



Seuraavassa kuvassa on tyypillinen kuusinapainen liitinpistoke:



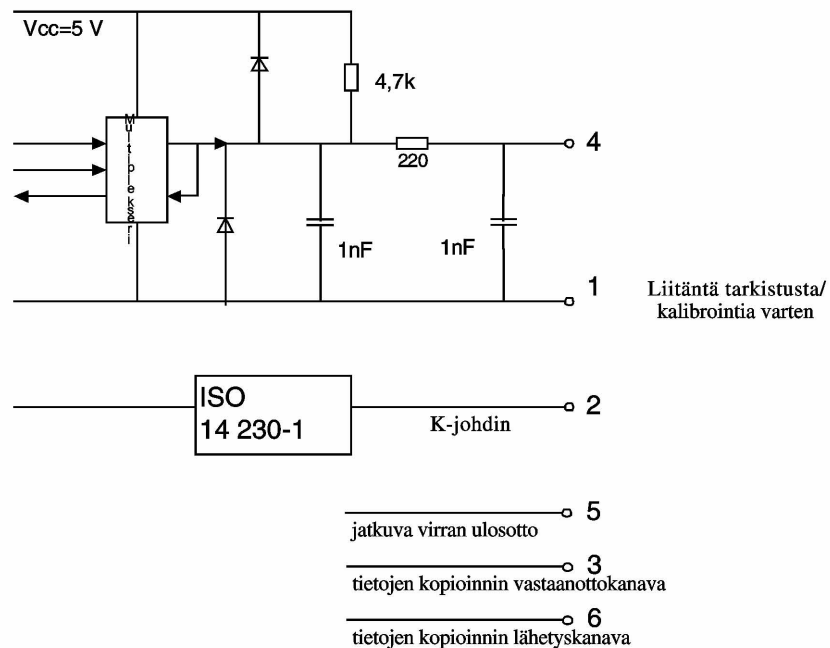
1.2 Liittimen johdotus

INT_002 Liitin on johdotettava seuraavan taulukon mukaisesti:

Napa	Kuvaus	Huomautus
1	Akun miinusnapa	Yhdistetty ajoneuvon akun miinusnapaan
2	Dataliikenne	K-johdin (standardin ISO 14230-1 mukainen)
3	RxD – Tietojen kopioinnissa käytettävä vastaanotonnapa	Datan tulosignaali valvontalaitteeseen
4	Tulo-/lähtösignaali	Kalibrointiin
5	Jatkuva virran ulosotto	Laitteen suojapiirin synnyttämän jännitehäviön vuoksi jännite on määritelty olemaan 3 V vähemmän kuin ajoneuvossa käytettävä jännite Virran ulosotto enintään 40 mA
6	TxD – Tietojen kopioinnissa käytettävä lähetysnapa	Datan lähtösignaali valvontalaitteesta

1.3 Lohkokaavio

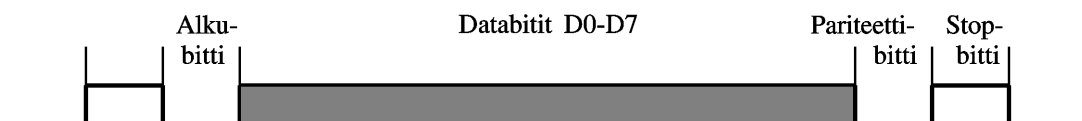
INT_003 Lohkokaavion on oltava seuraavan kuvan mukainen:



2. TIETOJEN KOPIOINNISSA KÄYTETTÄVÄ LIITÄNTÄLAITE

INT_004 Tietojen kopioinnissa käytettävän liitäntälaitteen on oltava standardin RS232 erittelyjen mukainen.

INT_005 Tietojen kopioinnissa käytettävän liitäntälaitteen on käytettävä yhtä alkubittiä, kahdeksaa databittiä vähiten merkitsevä bitti ensimmäisenä, yhtä pariteettibittiä ja yhtä stop-bittiä.



Datavavujen rakenne

- Alkubitti: yksi bitti, jonka looginen taso on 0;
- Databitit: lähetetään vähiten merkitsevä bitti ensimmäisenä;
- Pariteettibitti: parillinen
- Stop-bitti: yksi bitti, jonka looginen taso on 1

Lähetettäessä numeerista dataa, joka koostuu useammasta kuin yhdestä tavusta, lähetetään merkitsevin tavu ensimmäisenä ja vähiten merkitsevä tavu viimeisenä.

INT_006 Datansiirtonopeuden on oltava aseteltavissa välillä 9 600 bps–115 200 bps. Datansiirto on suoritettava suurimmalla mahdollisella nopeudella, mutta aloitusnopeus yhteyden syntyessä on asetettu arvoon 9 600 bps.

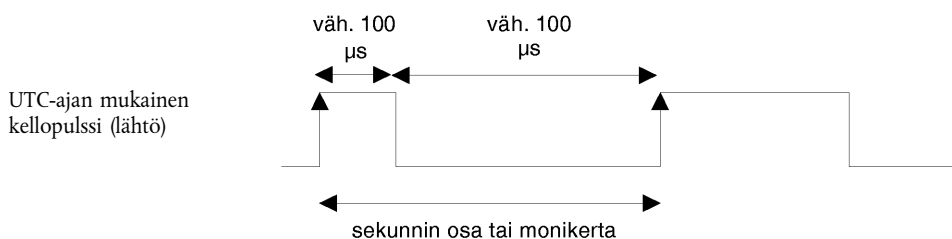
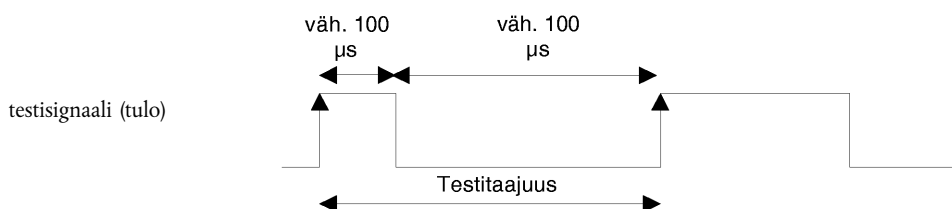
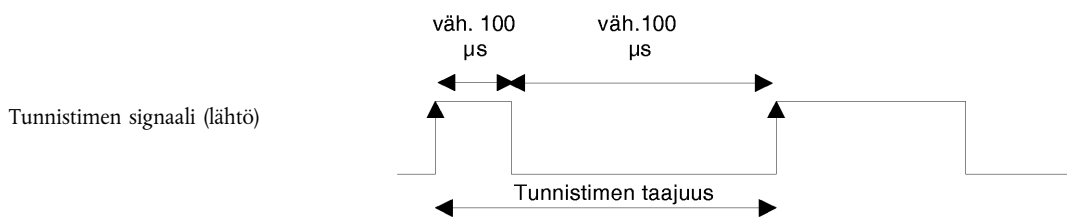
3. KALIBROINNISSA KÄYTETTÄVÄ LIITÄNTÄLAITE

INT_007 Tiedonsiirron on tapahduttava seuraavan standardin mukaisesti: ISO 14230-1 Road vehicles — Diagnostic systems — Keyword protocol 2000 — Part 1: Physical layer, First edition: 1999 (Tieliikenteessä käytettävät ajoneuvot. Diagnostiikkajärjestelmät. Avainsanaprotokolla 2000. Osa 1: Fyysinen kerros. Ensimmäinen painos: 1999).

INT_008 Tulo-/lähtösignaalin on oltava seuraavan sähköisen erittelyn mukainen:

Suure	Vähimmäisarvo	Tyypillinen arvo	Enimmäisarvo	Huomautus
U_{low} (tulo)			1,0 V	$I = 750 \mu\text{A}$
U_{high} (tulo)	4 V			$I = 200 \mu\text{A}$
Taajuus			4 kHz	
U_{low} (lähtö)			1,0 V	$I = 1 \text{ mA}$
U_{high} (lähtö)	4 V			$I = 1 \text{ mA}$

INT_009 Tulo-/lähtösignaalin on oltava seuraavien ajoituskaavioiden mukainen:



Lisäys 7

TIETOJEN KOPIOINTIPROTOKOLLAT

SISÄLLYSLUETTELO

1.	Johdanto	150
1.1	Sovellusala	150
1.2	Lyhenteet ja merkinnät	150
2.	Ajoneuvoyksikössä olevien tietojen kopiointi	151
2.1	Tietojen kopiointimenettely	151
2.2	Tietojen kopiointiprotokolla	151
2.2.1	Viestien rakenne	151
2.2.2	Viestityypit	152
2.2.2.1	Start Communication Request (SID 81)	154
2.2.2.2	Positive Response Start Communication (SID C1)	154
2.2.2.3	Start Diagnostic Session Request (SID 10)	154
2.2.2.4	Positive Response Start Diagnostic (SID 50)	154
2.2.2.5	Link Control Service (SID 87)	154
2.2.2.6	Link Control Positive Response (SID C7)	154
2.2.2.7	Request Upload (SID 35)	154
2.2.2.8	Positive Response Request Upload (SID 75)	154
2.2.2.9	Transfer Data Request (SID 36)	154
2.2.2.10	Positive Response Transfer Data (SID 76)	155
2.2.2.11	Transfer Exit Request (SID 37)	155
2.2.2.12	Positive Response Request Transfer Exit (SID 77)	155
2.2.2.13	Stop Communication Request (SID 82)	155
2.2.2.14	Positive Response Stop Communication (SID C2)	155
2.2.2.15	Acknowledge Sub Message (SID 83)	155
2.2.2.16	Negative Response (SID 7F)	155
2.2.3	Viestien kulku	156
2.2.4	Ajoitus	157
2.2.5	Virheen käsittely	157
2.2.5.1	Viestinnän aloitus (Start Communication) -vaihe	157
2.2.5.2	Viestintä (Communication) -vaihe	157
2.2.6	Vastausviestien sisältö	160
2.2.6.1	Positive Response Transfer Data Overview	160
2.2.6.2	Positive Response Transfer Data Activities	161
2.2.6.3	Positive Response Transfer Data Events and Faults	162

2.2.6.4	Positive Response Transfer Data Detailed Speed	163
2.2.6.5	Positive Response Transfer Data Technical Data	163
2.3	Tiedostojen tallennus ulkoisille tietovälineille (ESM)	164
3.	Ajopiirturikortilla olevien tietojen kopiointiprotokolla	164
3.1	Sovellusalue	164
3.2	Määritelmät	164
3.3	Kortilla olevien tietojen kopiointi	164
3.3.1	Kopioinnin aloittava komentosarja	165
3.3.2	Komentosarja tiedostoille, joilla ei ole allekirjoitusta	165
3.3.3	Komentosarja tiedostoille, joilla on allekirjoitus	165
3.3.4	Komentosarja, jolla kalibrointilaskuri asetetaan alkutilaansa	166
3.4	Tiedontallennuksen muoto	166
3.4.1	Johdanto	166
3.4.2	Tiedostomuoto	166
4.	Ajopiirturikortilla olevien tietojen kopiointi ajoneuvoyksikön kautta	167

1. JOHDANTO

Tässä lisäyksessä määritellään menettelyt, joiden avulla tietoja kopioidaan eri tavoin ulkoisille tietovälineille, sekä menettelyt, joiden avulla varmistetaan virheetön tiedonsiirto ja kopioitujen tietojen muodon täysi yhteensopivuus, jotta kuka hyvänsä tarkastaja voi tarkastaa tiedot sekä varmistua niiden aitoudesta ja eheydestä ennen niiden analysointia.

1.1 Sovellusala

Tietoja voidaan kopioida ulkoiselle tietovälineelle:

- ajoneuvoyksiköstä siihen kytketyn IDE-laitteen avulla,
- ajopiirturikortilta sellaisen IDE-laitteen avulla, johon on kytketty korttiliitäntälaitte,
- ajopiirturikortilta ajoneuvoyksikköön kytketyn IDE-laitteen avulla.

Jotta olisi mahdollista tarkastaa ulkoiselle tietovälineelle tallennettujen kopioitujen tietojen aitous ja eheys, tiedot kopioidaan liittämällä niihin lisäyksen 11 (Yhteiset turvamekanismit) mukainen allekirjoitus. Lähdelaitteen (ajoneuvoyksikön tai kortin) tunniste ja sen tietoturvaruenteet (jäsenvaltion ja laitteen) kopioidaan myös. Tietojen varmentajalla on erikseen oltava hallussaan luotettava julkinen eurooppalainen avain.

DDP_001 Yhden kopiointikerran aikana kopioidut tiedot on tallennettava ulkoiselle tietovälineelle yhteen tiedostoon.

1.2 Lyhenteet ja merkinnät

Tässä lisäyksessä käytetään seuraavia lyhenteitä:

AID	(Application identifier) Sovellustunniste
ATR	(Answer to reset) ATR-signaali; Signaali, joka annetaan vastauksena RST-komentoon
CS	(Checksum byte) Tarkistussummatavu
DF	(Dedicated file) DF-tiedosto eli hakemistotiedosto. DF-tiedosto voi sisältää muita (EF- tai DF-) tiedostoja
DS	(Diagnostic session) Diagnostinen jakso
EF	(Elementary file) EF-tiedosto; tiedosto, jossa varsinaiset tiedot säilytetään
ESM	(External storage medium) Ulkoinen tallennusväline
FID	(File identifier, file ID) Tiedoston tunniste
FMT	(Format byte) Muotoilutavu (viestin ylätunnisteen ensimmäinen tavu)
ICC	(Integrated circuit card) Integroidulla piirillä varustettu kontaktillinen kortti
IDE	(Intelligent dedicated equipment) IDE-laite: tarkoitukseen varattu laite, jonka avulla tietoja kopioidaan ulkoisille tietovälineille (esim. PC)
IFD	(Interface device) Liitäntälaitte
KWP	(Keyword protocol) Avainsanaprotokolla 2000
LEN	Pituustavu (viestin ylätunnisteen viimeinen tavu)
PPS	(Protocol parameter selection) Protokollan parametrin valinta
PSO	(Perform Security Operation) Suorita turvatoimi
SID	Palvelun tunniste
SRC	Lähdetavu
TGT	Kohdetavu
TLV	(Tag length value) TLV-koodaustapa; tuntomerkki-pituus-sisältö-koodaustapa
TREP	(Transfer Response Parameter) Lähetyspyyntöä koskevan vastauksen parametri
TRTP	(Transfer Request Parameter) Lähetyspyynnön parametri
VU	(Vehicle unit) Ajoneuvoyksikkö

2. AJONEUVOYKSIKÖSSÄ OLEVIEN TIETOJEN KOPIOINTI

2.1 Tietojen kopiointimenettely

Tiedot kopioidaan ajoneuvoyksiköstä seuraavasti:

- ajopiirturikortti asetetaan ajoneuvoyksikön korttiaukkoon ⁽¹⁾;
- IDE-laite yhdistetään ajoneuvoyksikön kopiointiliittimeen;
- luodaan yhteys IDE-laitteen ja ajoneuvoyksikön välille;
- valitaan IDE-laitteen avulla kopioitavat tiedot ja lähetetään niitä koskeva pyyntö ajoneuvoyksikölle;
- lopetetaan kopiointijakso.

2.2 Tietojen kopiointiprotokolla

Protokolla rakentuu isäntä-renki-periaatteelle siten, että IDE-laite on isäntä ja ajoneuvoyksikkö on renki.

Viestien rakenne, tyypit ja virta perustuvat periaatteessa Avainsanaprotokolla 2000:een (ISO 14230-2 Road vehicles — Diagnostic systems — Keyword protocol 2000 — Part 2: Data link layer. Tieliikenteessä käytettävät ajoneuvot. Diagnostiikkajärjestelmät. Avainsanaprotokolla 2000. Osa 2: Siirtokerros).

Sovelluserkos perustuu pääpiirteissään tähänhetkiseen 22. helmikuuta 2001 hyväksytyyn versioon 6 standardista ISO 14229-1 (Road vehicles — Diagnostic systems — Part 1: Diagnostic services. Tieliikenteessä käytettävät ajoneuvot. Diagnostiikkajärjestelmät — Osa 1: Diagnostiikkapalvelut).

2.2.1 Viestien rakenne

DDP_002 Kaikkien IDE-laitteen ja ajoneuvoyksikön välillä kulkevien viestien muoto perustuu rakenteeseen, jossa on kolme osaa:

- ylätunniste, jossa on muotoilutavu (FMT), kohdetavu (TGT), lähdetavu (SRC) sekä mahdollisesti pituustavu (LEN),
- datakenttä, jossa on palvelun tunnistetavu (SID) sekä vaihteleva määrä datatavuja, joihin voi sisältyä valinnainen diagnostiikkajakson osoitustavu (DS) tai valinnainen lähetyssparametritavu (TRTP tai TREP),
- tarkistussummatavun (CS) sisältämä tarkistussumma.

Ylätunniste				Datakenttä					Tarkistussumma
FMT	TGT	SRC	LEN	SID	DATA	CS
4 tavua				Enintään 255 tavua					1 tavu

TGT- ja SRC-tavu edustavat viestin vastaanottajan ja lähettäjän fyysisiä osoitteita. Heksadesimaalilukuina niiden arvot ovat F0h IDE-laitteelle ja EEh ajoneuvoyksikölle.

LEN-tavu on datakenttäosan pituus.

Tarkistussummatavu on kaikkien viestin sisältämien tavujen, paitsi itse CS-tavun, kahdeksan bitin ryhmissä laskettu summa modulo 256 (jakojäännös, joka syntyy, kun kyseinen summa jaetaan luvulla 256).

FMT-, SID-, DS-, TRTP- ja TREP-tavut on määritelty jäljempänä tässä asiakirjassa.

⁽¹⁾ Kopiointia ja kopioitavia tietoja koskevat käyttöoikeudet määräytyvät korttiaukkoon asetetun kortin mukaan.

DDP_003 Jos viestin sisältämän datan pituus ylittää datakentässä käytettävissä olevan tilan, lähetetään viesti useampina osaviesteinä. Jokaisella osaviestillä on ylätunniste, sama SID, TREP sekä kaksitavuinen osaviestilaskuri, joka osoittaa osaviestin järjestysnumeron kokonaisviestissä. Jotta virhetarkistus- ja viestin keskeyttämistoiminnot olisivat mahdollisia, IDE-laite kuittaa jokaisen osaviestin. IDE-laite voi joko hyväksyä kyseisen osaviestin, pyytää sen lähettämistä uudelleen, pyytää ajoneuvoyksikköä aloittamaan koko viestin uudelleen tai keskeyttää viestin lähetyksen kokonaan.

DDP_004 Jos viimeisen osaviestin datakentässä on täsmälleen 255 tavua, on kokonaisviestiin lisättävä vielä (SID-, TREP- ja osaviestilaskuritavuja lukuun ottamatta) tyhjä datakenttä osoittamaan viestin loppua.

Esimerkki:

Ylätunniste	SID	TREP	Viesti			CS
4 tavua	Enemmän kuin 255 tavua					

Lähetetään muodossa:

Ylätunniste	SID	TREP	00	01	Osaviesti 1	CS
4 tavua	255 tavua					

Ylätunniste	SID	TREP	00	02	Osaviesti 2	CS
4 tavua	255 tavua					

...

Ylätunniste	SID	TREP	xx	yy	Osaviesti n	CS
4 tavua	Vähemmän kuin 255 tavua					

tai muodossa:

Ylätunniste	SID	TREP	00	01	Osaviesti 1	CS
4 tavua	255 tavua					

Ylätunniste	SID	TREP	00	02	Osaviesti 2	CS
4 tavua	255 tavua					

...

Ylätunniste	SID	TREP	xx	yy	Osaviesti n	CS
4 tavua	255 tavua					

Ylätunniste	SID	TREP	xx	yy+1	CS
4 tavua	4 tavua				

2.2.2 Viestityypit

Tietojen kopioimiseen ajoneuvoyksikön ja IDE-laitteen välillä käytettävä viestintäprotokolla vaatii 8 erilaista viestityyppiä käyttöä.

Seuraavassa taulukossa on näiden viestityyppien yhteenvedo.

Viestin rakenne	Enintään 4 tavua Ylätunniste				Enintään 255 tavua Data			1 tavu Tarkistus- summa
	FMT	TGT	SRC	LEN	SID	DS/TRTP	DATOS	
IDE ->	<- VU							
Start Communication Request	81	EE	F0		81			E0
Positive Response Start Communication	80	F0	EE	03	C1		8F,EA	9B
Start Diagnostic Session Request	80	EE	F0	02	10	81		F1
Positive Response Start Diagnostic	80	F0	EE	02	50	81		31
Link Control Service								
Verify Baud Rate (stage 1)								
9 600 Bd	80	EE	F0	04	87		01,01,01	EC
19 200 Bd	80	EE	F0	04	87		01,01,02	ED
38 400 Bd	80	EE	F0	04	87		01,01,03	ED
57 600 Bd	80	EE	F0	04	87		01,01,04	EF
115 200 Bd	80	EE	F0	04	87		01,01,05	F0
Positive Response Verify Baud Rate	80	F0	EE	02	C7		01	28
Transition Baud Rate (stage 2)	80	EE	F0	03	87		02,03	ED
Request Upload	80	EE	F0	0A	35		00,00,00, 00,00,FF, FF,FF,FF	99
Positive Response Request Upload	80	F0	EE	03	75		00,FF	D5
Transfer Data Request								
Overview	80	EE	F0	02	36	01		97
Activities	80	EE	F0	06	36	02	Date	CS
Events & Faults	80	EE	F0	02	36	03		99
Detailed Speed	80	EE	F0	02	36	04		9A
Technical Data	80	EE	F0	02	36	05		9B
Card download	80	EE	F0	02	36	06		9C
Positive Response Transfer Data	80	F0	EE	Len	76	TREP	Data	CS
Request Transfer Exit	80	EE	F0	01	37			96
Positive Response Request Transfer Exit	80	F0	EE	01	77			D6
Stop Communication Request	80	EE	F0	01	82			E1
Positive Response Stop Communication	80	F0	EE	01	C2			21
Acknowledge sub message	80	EE	F0	Len	83		Data	CS
Negative responses -viestit								
Yleinen kieltäytyminen	80	F0	EE	03	7F	Sid Req	10	CS
Palvelua ei tueta (Service not supported)	80	F0	EE	03	7F	Sid Req	11	CS
Osatoimintoa ei tueta (Sub function not supported)	80	F0	EE	03	7F	Sid Req	12	CS
Väärä viestin pituus (Incorrect message length)	80	F0	EE	03	7F	Sid Req	13	CS
Väärät ehdot tai virhe pyynnön rakenteessa (Request sequence error)	80	F0	EE	03	7F	Sid Req	22	CS
Pyyntö alueen ulkopuolella (Request out of range)	80	F0	EE	03	7F	Sid Req	31	CS
Kopiointipyyntöä ei hyväksytty (Upload not accepted)	80	F0	EE	03	7F	Sid Req	50	CS
Vastaus annetaan myöhemmin (Response pending)	80	F0	EE	03	7F	Sid Req	78	CS
Tietoja ei käytettävissä (Data not available)	80	F0	EE	03	7F	Sid Req	FA	CS

Huomautuksia:

- Sid Req = vastaavan viestin SID (palvelun tunnistetavu), Lid Req = vastaavan viestin LID (paikallinen tunnistetavu).
- TREP = vastaavan pyynnön TRTP.
- Musta ruutu tarkoittaa, että mitään ei lähetetä.
- Sanaa upload (IDE-laitteen kannalta) on käytetty ISO 14229 -standardin mukaan. Se tarkoittaa samaa kuin download (tietojen kopiointi) (ajoneuvoyksikön kannalta).
- Mahdolliset kaksitavuiset osaviestilaskurit eivät näy tässä taulukossa.

2.2.2.1 Start Communication Request (SID 81)

DDP_005 IDE-laite aloittaa viestintäyhteyden luomisen ajoneuvoyksikön kanssa lähettämällä Start Communication Request -viestin. Alkuvaiheen viestintä tapahtuu aina 9 600 baudin nopeudella (kunnes nopeutta muutetaan tarvittavien Link Control Service -palvelujen avulla).

2.2.2.2 Positive Response Start Communication (SID C1)

DDP_006 Ajoneuvoyksikkö vastaa myöntävästi Start Communication Request -viestiin lähettämällä Positive Response Start Communication -viestin. Viestiin sisältyy tavut 8Fh ja EAh, jotka osoittavat, että ajoneuvoyksikkö tukee protokollaa, jossa on kohde-, lähde- ja pituustiedot sisältävä ylätunniste.

2.2.2.3 Start Diagnostic Session Request (SID 10)

DDP_007 IDE-laite pyytää ajoneuvoyksiköltä uutta diagnostista jaksoa lähettämällä Start Diagnostic Session Request -viestin. Ali-toiminto 'default session' (81h) osoittaa, että avattava jakso vastaa oletusarvoa.

2.2.2.4 Positive Response Start Diagnostic (SID 50)

DDP_008 Ajoneuvoyksikkö vastaa myöntävästi Diagnostic Session Request -pyyntöön lähettämällä Positive Response Start Diagnostic -viestin.

2.2.2.5 Link Control Service (SID 87)

DDP_052 IDE-laite aloittaa lähetysnopeuden muuttamisen Link Control Service -palvelulla. Tämä tapahtuu kaksivaiheisesti. Ensimmäisessä vaiheessa IDE ehdottaa nopeuden muuttamista ja uutta nopeutta. Saatuaan ajoneuvoyksiköltä myönteisen vastauksen IDE lähettää ajoneuvoyksikölle vahvistuksen nopeuden muutoksesta (toinen vaihe). Tämän jälkeen IDE siirtyy käyttämään uutta nopeutta. Ajoneuvoyksikkö siirtyy käyttämään uutta nopeutta saatuaan vahvistuksen.

2.2.2.6 Link Control Positive Response (SID C7)

DDP_053 Ajoneuvoyksikkö vastaa Link Control Service -pyyntöön myönteisesti lähettämällä Link Control Positive Response -viestin (ensimmäinen vaihe). Vahvistusviestiin (toisessa vaiheessa) ei lähetetä vastausta.

2.2.2.7 Request Upload (SID 35)

DDP_009 IDE-laite kertoo Request Upload -viestillä ajoneuvoyksikölle, että tietoja halutaan kopioida. ISO14229-standardin mukaisesti viesti sisältää tiedot pyydetyn datan osoitteesta, koosta ja formaatista. Koska nämä eivät ole IDE-laitteen tiedossa ennen kopiointia, muistiosoitteeksi asetetaan 0, formaatti ilmoitetaan salaamattomaksi ja tiivistämättömäksi ja muistikoko asetetaan mahdollisimman suureksi.

2.2.2.8 Positive Response Request Upload (SID 75)

DDP_010 Ajoneuvoyksikkö kertoo IDE-laitteelle Positive Response Request Upload -viestillä, että se on valmis kopioimaan tietoja. ISO14229-standardin mukaisesti tämä myönteinen vastausviesti sisältää IDE-laitteelle tiedon siitä, että tulevat Positive Response Transfer Data -viestit sisältävät enintään 00FFh tavua.

2.2.2.9 Transfer Data Request (SID 36)

DDP_011 IDE-laite määrittää ajoneuvoyksikölle Transfer Data Request -viestillä, minkä tyyppisiä tietoja on tarkoitus kopioida. Yhden tavun TRTP-parametri (Transfer Request Parameter) ilmoittaa siirron tyyppin.

Tiedonsiirtoja on kuudentyyppisiä:

- Yleiskatsaus (TRTP 01),
- Tietyn päivän toimintaa koskevat tiedot (TRTP 02),
- Tapauksiin ja vikoihin liittyvät tiedot (TRTP 03),
- Yksityiskohtaiset nopeustiedot (TRTP 04),
- Tekniset tiedot (TRTP 05),
- Kortilla olevien tietojen kopiointi (TRTP 06).

DDP_054 IDE-laitteen on pyydettävä yleiskatsausta (TRTP 01) kopiointitilanteessa, koska ainoastaan näin voidaan varmistaa, että ajoneuvoyksikön varmenteet tallentuvat kopioitavaan tiedostoon (ja digitaalinen allekirjoitus voidaan todentaa). Toisessa tyyppissä (TRTP 02) Transfer Data Request -viestiin sisältyy (**TimeReal** -muodossa oleva) tieto siitä kalenterivuorokaudesta, jota koskevat tiedot on tarkoitus kopioida.

2.2.2.10 *Positive Response Transfer Data (SID 76)*

DDP_012 Ajoneuvoyksikkö vastaa Transfer Data Request -viestiin lähettämällä Positive Response Transfer Data -viestin. Viesti sisältää pyydettyt tiedot ja TREP-parametrin (Transfer Response Parameter), joka vastaa pyynnön TRTP-parametria.

DDP_055 Ensimmäisessä tyyppissä (TREP01) ajoneuvoyksikkö lähettää tietoja, jotka auttavat IDE-laitteen käyttäjää valitsemaan ne tiedot, jotka hän haluaa kopioida. Tähän viestiin sisältyvät seuraavat tiedot:

- tietoturvarvarmenteet,
- ajoneuvon tunnistus,
- ajoneuvoyksikön kuuluva päivämäärä ja aika,
- ensimmäinen ja viimeinen päivämäärä, joita koskevat (ajoneuvoyksikön sisältämät) tiedot ovat kopioitavissa,
- tieto ajoneuvoyksikössä olevista korteista,
- edellinen yrityksen tekemä tietojen kopiointi,
- yrityksen asettamat lukitukset,
- aiemmat tarkastukset.

2.2.2.11 *Transfer Exit Request (SID 37)*

DDP_013 IDE-laite kertoo ajoneuvoyksikölle Request Transfer Exit -viestillä, että tietojen kopiointi on päättynyt.

2.2.2.12 *Positive Response Request Transfer Exit (SID 77)*

DDP_014 Ajoneuvoyksikkö kuittaa Transfer Exit Request -viestin lähettämällä Positive Response Request Transfer Exit -viestin.

2.2.2.13 *Stop Communication Request (SID 82)*

DDP_015 IDE-laite katkaisee viestintäyhteyden ajoneuvoyksikön kanssa lähettämällä Stop Communication Request -viestin.

2.2.2.14 *Positive Response Stop Communication (SID C2)*

DDP_016 Ajoneuvoyksikkö kuittaa Stop Communication Request -viestin lähettämällä Positive Response Stop Communication -viestin.

2.2.2.15 *Acknowledge Sub Message (SID 83)*

DDP_017 IDE-laite vahvistaa kunkin useassa osassa lähetettävän viestin osaviestin vastaanottamisen lähettämällä Acknowledge Sub Message -viestin. Datakenttä sisältää ajoneuvoyksiköltä saadun SID-tunnisteen ja kaksitavuisen koodin seuraavasti:

- MsgC +1 kuittaa osaviestin numero MsgC virheettömän vastaanottamisen.
IDE-laite pyytää ajoneuvoyksikköä lähettämään seuraavan osaviestin.
- MsgC osoittaa, että osaviestin numero MsgC vastaanottamisessa ilmeni ongelma.
IDE-laite pyytää ajoneuvoyksikköä lähettämään tämän osaviestin uudelleen.
- FFFF pyytää lopettamaan viestin lähetyksen.
IDE-laite voi käyttää tätä koodia lopettamaan ajoneuvoyksikön viestin lähetyksen mistä hyvänsä syystä.

Viestin viimeinen osaviesti (LEN-tavu < 255) voidaan kuitata millä hyvänsä näistä koodeista tai jättää kuitaamatta.

Ajoneuvoyksikön vastaukset tapauksissa, joissa viesti koostuu useista osaviesteistä, ovat:

- Positive Response Request Upload (SID 75),
- Positive Response Transfer Data (SID 76).

2.2.2.16 *Negative Response (SID 7F)*

DDP_018 Jos ajoneuvoyksikkö ei voi täyttää edellä selostetuilla viesteillä esitettyä pyyntöä, se vastaa Negative Response -viestillä. Viestin datakenttä sisältää vastauksen SID-tunnisteen (7F), pyynnön SID-tunnisteen sekä koodin, joka ilmaisee kieltävän vastauksen syyn. Käytettävissä on seuraavat koodit:

- 10 yleinen kieltäytyminen
Toimintoa ei voida suorittaa muiden kuin jäljempänä selostettujen syiden vuoksi.
- 11 palvelua ei tueta
Pyynnön SID-tunnistetta ei tunnistettu.
- 12 osatoimintoa ei tueta
Pyynnön DS_ tai TRTP-tunnistetta ei tunnistettu tai lähetettäviä osaviestejä ei enää ole.
- 13 väärä viestin pituus
Vastaanotettu viestin on väärän mittainen.
- 22 virheelliset ehdot tai virhe pyynnön rakenteessa
Pyydetty palvelu ei ole toimintavalmiudessa tai pyynnön esittäneen viestin osien järjestys on väärä.
- 31 pyyntö alueen ulkopuolella
Pynnön parametritietue (datakenttä) ei oikeanlainen.
- 50 kopiointipyyntöä ei hyväksytä
Pyyntöä ei voida noudattaa (ajoneuvoyksikkö on väärässä toimintatilassa tai yksikössä on sisäinen vika).
- 78 vastaus annetaan myöhemmin
Pyydettyä toimintoa ei ehditä suorittaa ajoissa, eikä ajoneuvoyksikkö ole valmis vastaanottamaan uutta pyyntöä.
- FA tietoja ei käytettävissä
Tiedon siirtopyynnön kohteena olevat tiedot eivät ole käytettävissä ajoneuvoyksikössä (esim. yksikköön ei ole asetettu korttia, ...).

2.2.3 Viestien kulku

Tyypillinen viestien kulku normaalin tietojen kopiointitapahtuman aikana on seuraavanlainen:

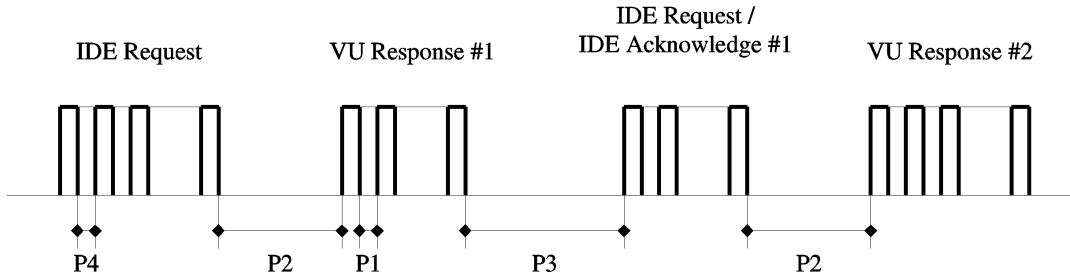
IDE-laite		Ajoneuvoyksikkö
Start Communication Request	⇒ ⇐	Positive Response (myöntävä vastaus)
Start Diagnostic Service Request	⇒ ⇐	Positive Response
Request Upload	⇒ ⇐	Positive Response
Transfer Data Request Overview	⇐ ⇒	Positive Response
Transfer Data Request nro 2	⇐	Positive Response nro 1 Positive Response nro 2 Positive Response nro m Positive Response (Datakenttä < 255 tavua)
Acknowledge Sub Message nro 1	⇐	
Acknowledge Sub Message nro 2	⇒	
Acknowledge Sub Message nro m	⇐	
Acknowledge Sub Message (valinnainen)	⇒	
...		
Transfer Data Request nro n	⇒ ⇐	Positive Response
Transfer Exit Request	⇒ ⇐	Positive Response
Stop Communication Request	⇒ ⇐	Positive Response

2.2.4 Ajoitus

DDP_019 Normaalkäytön aikana seuraavassa kuvassa näkyvät ajoitusparametrit ovat oleellisia:

Kuva 1

Viestien kulku, ajoitus



Missä:

P1 = Tavujen välinen aika ajoneuvoyksikön vastauksessa.

P2 = Aika IDE-laitteen pyynnön lopusta ajoneuvoyksikön vastauksen alkuun tai aika IDE-laitteen kuittauksen lopusta ajoneuvoyksikön seuraavan vastauksen alkuun.

P3 = Aika ajoneuvoyksikön vastauksen lopusta IDE-laitteen seuraavan pyynnön alkuun tai aika ajoneuvoyksikön vastauksen lopusta IDE-laitteen kuittauksen alkuun tai aika IDE-laitteen pyynnön lopusta IDE-laitteen seuraavan pyynnön alkuun tapauksissa, jolloin ajoneuvoyksikkö ei vastaa.

P4 = Tavujen välinen aika IDE-laitteen pyynnöissä.

P5 = Ajan P3 pidennetty arvo kortilta kopiointia varten.

Ajoitusparametrien sallitut arvot on esitetty seuraavassa taulukossa (KWP-avainsanaprotokollan laajennettu ajoitusparametritaulukko, jota käytetään fyysisessä osoitteistamisessa viestintänopeuden kohottamiseksi).

Ajoitusparametri	Pienin arvo (ms)	Suurin arvo (ms)
P1	0	20
P2	20	1 000 (*)
P3	10	5 000
P4	5	20
P5	10	20 minuuttia

(*) Jos ajoneuvoyksikkö vastaa kieltävästi Negative Response -viestillä, jossa on tilannetta 'viesti vastaanotettu virheettömästi, vastaus annetaan myöhemmin' tarkoittava koodi, tätä arvoa suurennetaan parametrin P3 ylärajaan saakka.

2.2.5 Virheen käsittely

Jos viestejä vaihdettaessa tapahtuu virhe, viestien kulku muuttuu sen mukaan, mikä laite havaitsi virheen ja mikä viesti synnytti virheen.

Kuvissa 2 ja 3 on esitetty ajoneuvoyksikön ja IDE-laitteen virheen käsittelymenettelyt.

2.2.5.1 Viestinnän aloitus (Start Communication) -vaihe

DDP_020 Jos IDE-laite havaitsee ajoituksen tai bittivirtaan liittyvän virheen viestinnän aloitusvaiheessa, se odottaa ajan P3, ennen kuin se lähettää pyynnön uudelleen.

DDP_021 Jos ajoneuvoyksikkö havaitsee virheen IDE-laitteelta tulevassa viestissä, se ei lähetä vastausta, vaan odottaa uutta Start Communication Request -viestiä ajan P3 kuluessa.

2.2.5.2 Viestintä (Communication) -vaihe

Virheen käsittely jakautuu kahteen osa-alueeseen:

1. Ajoneuvoyksikkö havaitsee virheen IDE-laitteen läheteessä.

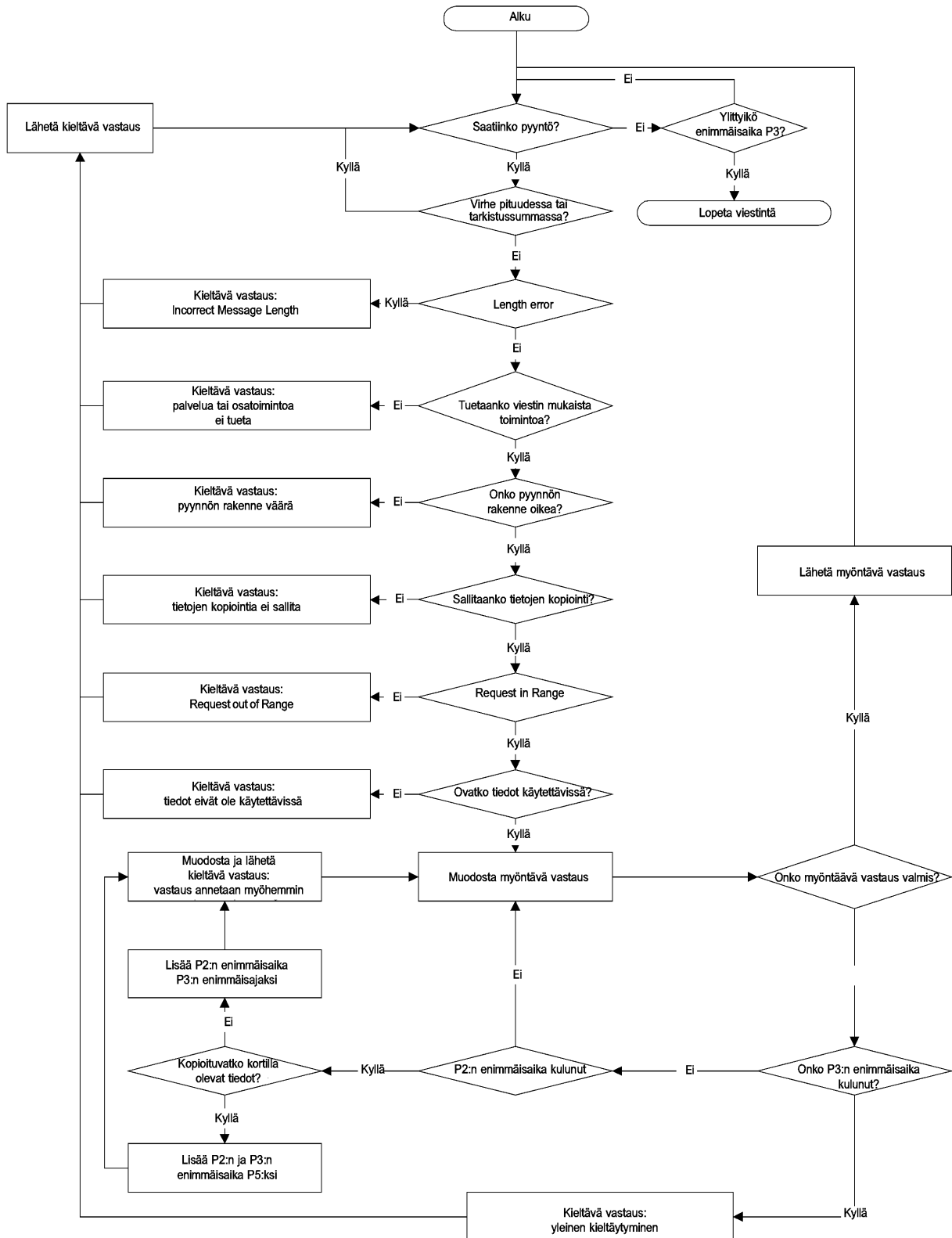
DDP_022 Ajoneuvoyksikön on havaittava kaikkien saapuvien viestien ajoitusvirheet, tavujen muotovirheet (kuten alku- ja stop-biteihin liittyvät virheet) sekä kehysten virheet (väärä vastaanotettujen tavujen määrä, väärä tarkistussummatavu).

DDP_023 Jos ajoneuvoyksikkö havaitsee jonkin edellä mainituista virheistä, se ei lähetä vastausta eikä ota kyseistä viestiä huomioon.

DDP_024 Ajoneuvoyksikkö saattaa havaita muita vastaanotetun viestin muotoon tai sisältöön liittyviä virheitä (kuten, että viestin mukaista toimintaa ei tueta), vaikka viestin pituus ja tarkistussumma olisivatkin oikein; tällöin ajoneuvoyksikön on vastattava IDE-laitteelle kieltävällä virheen luonteen selvittäväällä Negative Response -viestillä.

Kuva 2

Ajoneuvoyksikön virheenkäsitely

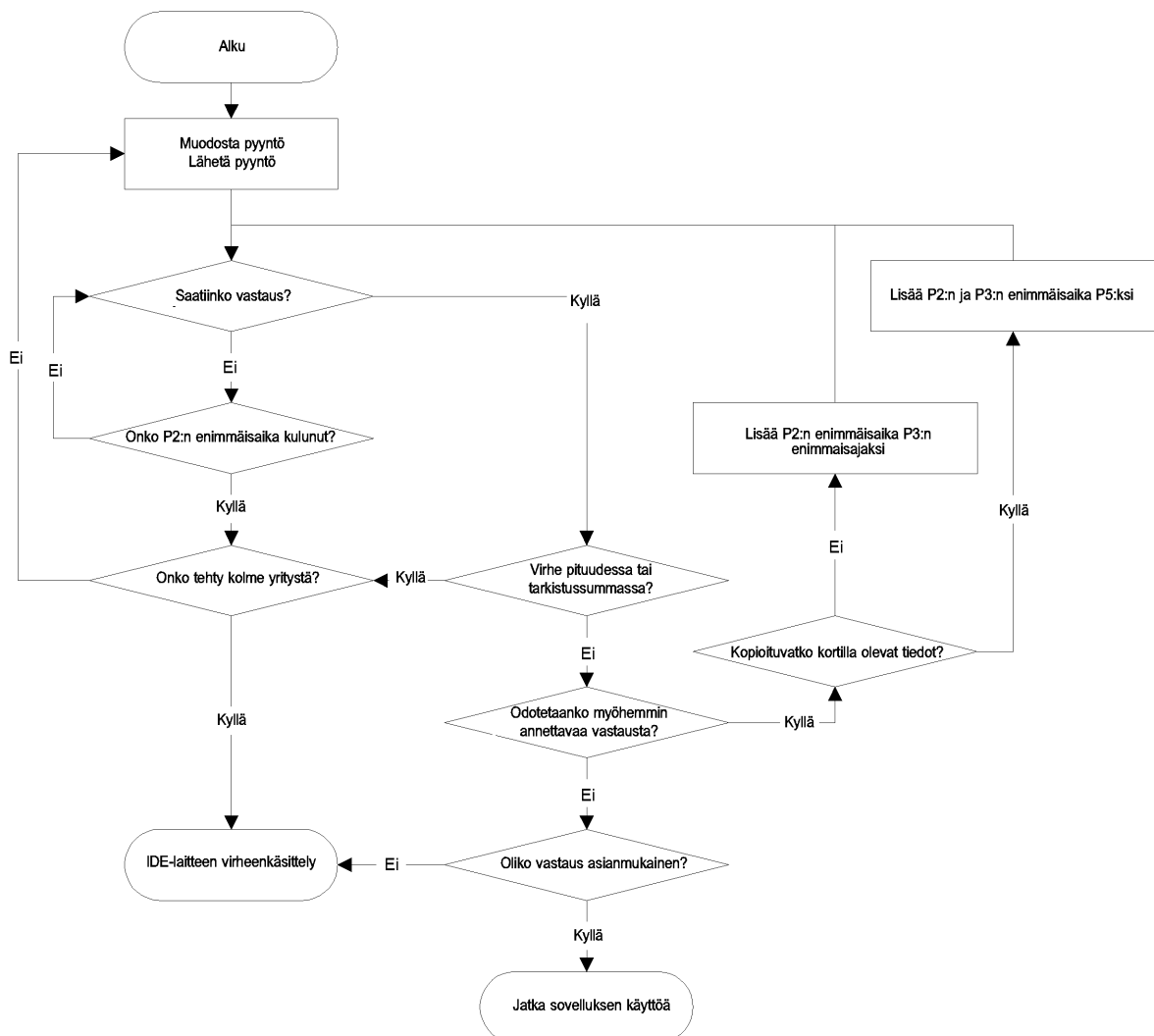


2. IDE-laite havaitsee virheen ajoneuvoyksikön läheteessä.

- DDP_025 IDE-laitteen on havaittava kaikkien saapuvien viestien ajoitusvirheet, tavujen muotovirheet (kuten alku- ja stop-bitteihin liittyvät virheet) sekä kehysten virheet (väärä vastaanotettujen tavujen määrä, väärä tarkistussummatavu).
- DDP_026 IDE-laitteen on havaittava viestien rakenteeseen liittyvät virheet, kuten peräkkäin vastaanotettujen viestien väärät osaviestilaskurin arvonmuutokset.
- DDP_027 Jos IDE-laite havaitsee viestin tai ajoneuvoyksikkö ei vastaa ajan P2 kuluessa, pyynnön sisältävä viesti lähetetään uudelleen enintään kolme kertaa. Tässä virheen havaitsemista koskevassa tarkastelussa katsotaan osaviestin kuittaava Sub Message Acknowledge -viesti ajoneuvoyksikölle osoitetuksi pyynnöksi.
- DDP_028 IDE-laitteen on odotettava vähintään P3:n vähimmäisaika ennen jokaista lähetystä; odotusaika mitataan viimeisestä virheen havaitsemisen jälkeen lasketusta stop-bitistä.

Kuva 3

IDE-laitteen virheen käsittely



2.2.6 Vastausviestien sisältö

Tässä kohdassa määritellään erilaisten myöntävien vastausviestien datakenttien sisältö.

Dataelementit on määritelty lisäyksessä 1 (Datatermistö).

2.2.6.1 Positive Response Transfer Data Overview

DDP_029 Positive Response Transfer Data Overview -viestin datakentän on sisällettävä seuraavat tiedot seuraavassa järjestyksessä palvelun SID-tunnisteen arvon ollessa 76h ja TREP-tunnisteen ollessa 01h sekä noudatettava asianmukaista osaviesteihin jakamista ja osaviestien laskemista:

Dataelementti	Pituus (Tavua)	Selite
MemberStateCertificate	194	Ajoneuvoyksikön tietoturvarvarmenteet
VUCertificate	194	
VehicleIdentificationNumber	17	Ajoneuvon tunnistetiedot
VehicleRegistrationIdentification	1	
vehicleRegistrationNation vehicleRegistrationNumber	14	
CurrentDateTime	4	Ajoneuvoyksikön kuluva päivämäärä ja aika
VuDownloadablePeriod	4	Jakso, jota koskevat tiedot ovat kopioitavissa
minDownloadableTime maxDownloadableTime	4	
CardSlotsStatus	1	Ajoneuvoyksikköön asetettujen korttien tyyppi
VuDownloadActivityData	4	Edellinen ajoneuvoyksikön tietojen kopiointi
downloadingTime	18	
fullCardNumber companyOrWorkshopName	36	
VuCompanyLocksData	1	Kaikki tallennetut yrityksen tekemät lukitukset. Jos tämä kohta on tyhjä, lähetetään vain tieto noOfLocks = 0.
noOfLocks	(98)	
...		
Vu Company Locks Record	4	
lockInTime	4	
lockOutTime	36	
companyName	36	
companyAddress	36	
companyCardNumber	18	
...		
VuControlActivityData	1	Kaikki ajoneuvoyksikköön tallennetut tarkastustoimia koskevat tiedot. Jos tämä kohta on tyhjä, lähetetään vain tieto noOfControls = 0.
noOfControls	(31)	
...		
Vu Control Activity Record	1	
controlType	4	
controlTime	18	
controlCardNumber	4	
downloadPeriodBeginTime	4	
downloadPeriodEndTime	4	
...		
Signature	128	Kaikkien tietojen (paitsi varmenteiden) RSA-allekirjoitus VehicleIdentification-Number-tiedosta viimeisen VuControl ActivityRecord-tietueen viimeiseen tavuun

2.2.6.2 Positive Response Transfer Data Activities

DDP_030 Positive Response Transfer Data Activities -viestin datakentän on sisällettävä seuraavat tiedot seuraavassa järjestyksessä palvelun SID-tunnisteen arvon ollessa 76h ja TREP-tunnisteen arvon ollessa 02h sekä noudatettava asianmukaista osaviesteihin jakamista ja osaviestien laskemista:

Dataelementti	Pituus (Tavua)	Selite
TimeReal	4	Päivämäärä, jolloin tiedot kopioitiin
OdometerValueMidnight	3	Matkamittarin lukema sen päivän lopussa, jolloin tiedot kopioitiin
VuCardIWData		
noOfVuCardIWRecords	2	Kortin paikoilleenasettamis- ja poistojaksoihin liittyvät tiedot
...	(129)	— Jos tässä kohdassa ei ole tietoja, lähetetään vain tieto noOfVuCardIWRecords = 0.
VuCardIWRecord		— Jos VuCardIWRecord-tietueen tiedot ulottuvat ajan 00:00 yli (kortti asetettu paikoilleen edellisen vuorokauden aikana) tai ajan 24:00 yli (kortti poistettu seuraavan vuorokauden aikana), tietojen on näytävä kokonaisuudessaan molempien kyseisten vuorokausien kohdalla.
cardHolderName	36	
holderSurname	36	
holderFirstNames	36	
fullCardNumber	18	
cardExpiryDate	4	
cardInsertionTime	4	
vehicleOdometerValueAtInsertion	3	
cardSlotNumber	1	
cardWithdrawalTime	4	
vehicleOdometerValueAtWithdrawal	3	
previousVehicleInfo		
vehicleRegistrationIdentification	1	
vehicleRegistrationNation	14	
vehicleRegistrationNumber	14	
cardWithdrawalTime	4	
manualInputFlag	1	
...		
VuActivityDailyData		
noOfActivityChanges	2	Korttiaukkojen tila klo 00:00 ja tallennetut toimintaa koskevat tiedot siltä päivältä, jonka tiedot kopioitiin.
...		
ActivityChangeInfo	2	
...		
VuPlaceDailyWorkPeriodData		
noOfPlaceRecords	1	Siltä päivältä tallennetut paikkoihin liittyvät tiedot, jonka tiedot kopioitiin. Jos tämä kohta on tyhjä, lähetetään vain tieto noOfPlaceRecords = 0.
...	(28)	
VuPlaceDailyWorkPeriodRecord		
fullCardNumber	18	
placeRecord		
entryTime	4	
entryTypeDailyWorkPeriod	1	
dailyWorkPeriodCountry	1	
dailyWorkPeriodRegion	1	
vehicleOdometerValue	3	
...		
VuSpecificConditionData		
noOfSpecificConditionRecords	2	Siltä päivältä tallennetut erityisolosuhteita koskevat tiedot, jonka tiedot kopioitiin. Jos tämä kohta on tyhjä, lähetetään vain tieto noOfSpecificConditionRecords = 0.
...	(5)	
SpecificConditionRecord		
EntryTime	4	
specificConditionType	1	
...		
Signature	128	Kaikkien tietojen RSA-allekirjoitus Time Real-tiedosta viimeisen erityisolosuhteita koskevan tietueen viimeiseen tavuun

2.2.6.3 Positive Response Transfer Data Events and Faults

DDP_031 Positive Response Transfer Data Events and Faults -viestin datakentän on sisällettävä seuraavat tiedot seuraavassa järjestyksessä palvelun SID-tunnisteen arvon ollessa 76h ja TREP-tunnisteen arvon ollessa 03h sekä noudatettava asianmukaista osaviesteihin jakamista ja osaviestien laskemista:

Dataelementti		Pituus (Tavua)	Selite
VuFaultData			
NoOfVuFaults		1	Kaikki ajoneuvoyksikköön tallennetut tai meneillään olevia vikoja koskevat vikatiedot. Jos tämä kohta on tyhjä, lähetetään vain tieto noOfVuFaults = 0.
...		(82)	
VuFaultRecord	FaultType	1	
	FaultRecordPurpose	1	
	FaultBeginTime	4	
	FaultEndTime	4	
	CardNumberDriverSlotBegin	18	
	cardNumberCodriverSlotBegin	18	
	CardNumberDriverSlotEnd	18	
CardNumberCodriverSlotEnd	18		
...			
VuEventData			
NoOfVuEvents		1	Kaikki ajoneuvoyksikköön tallennetut tai meneillään olevat tapaukset (paitsi ylinopeustapaukset). Jos tämä kohta on tyhjä, lähetetään vain tieto noOfVuEvents = 0.
...		(83)	
VuEventRecord	EventType	1	
	EventRecordPurpose	1	
	EventBeginTime	4	
	EventEndTime	4	
	CardNumberDriverSlotBegin	18	
	cardNumberCodriverSlotBegin	18	
	CardNumberDriverSlotEnd	18	
	CardNumberCodriverSlotEnd	18	
	SimilarEventsNumber	1	
...			
VuOverSpeedingControlData			
LastOverspeedControlTime		4	Viimeisimpään ylinopeustarkastukseen liittyvät tiedot (oletusarvo, jos tietoja ei ole)
FirstOverspeedSince		4	
NumberOfOverspeedSince		1	
VuOverSpeedingEventData			
NoOfVuOverSpeedingEvents		1	Kaikki ajoneuvoyksikköön tallennetut ylinopeustapauksiin liittyvät tiedot. Jos tämä kohta on tyhjä, lähetetään vain tieto noOfVuOverSpeedingEvents = 0.
...		(31)	
VuOverSpeedingEventRecord	EventType	1	
	EventRecordPurpose	1	
	EventBeginTime	4	
	EventEndTime	4	
	MaxSpeedValue	1	
	AverageSpeedValue	1	
	CardNumberDriverSlotBegin	18	
	SimilarEventsNumber	1	
...			
VuTimeAdjustmentData			
NoOfVuTimeAdjRecords		1	Kaikki ajoneuvoyksikköön tallennetut ajan asetuksiin liittyvät tiedot (täydellisen kalibroinnin ulkopuolella suoritettut). Jos tämä kohta on tyhjä, lähetetään vain tieto noOfVuTimeAdjRecords = 0.
...		(98)	
VuTimeAdjustmentRecord	OldTimeValue	4	
	NewTimeValue	4	
	WorkshopName	36	
	WorkshopAddress	36	
	WorkshopCardNumber	18	
...			
Signature		128	Kaikkien tietojen RSA-allekirjoitus noOfVuFaults-tiedosta viimeisen ajan asetukseen liittyvän tietueen viimeiseen tavuun

2.2.6.4 Positive Response Transfer Data Detailed Speed

DDP_032 Positive Response Transfer Data Detailed Speed -viestin datakentän on sisällettävä seuraavat tiedot seuraavassa järjestyksessä palvelun SID-tunnisteen arvon ollessa 76h ja TREP-tunnisteen arvon ollessa 04h sekä noudatettava asianmukaista osaviesteihin jakamista ja osaviestien laskemista:

Dataelementti		Pituus (Tavua)	Selite
VuDetailedSpeedData			
NoOfSpeedBlocks		2	Kaikki ajoneuvoyksikköön tallennetut yksityiskohtaiset nopeustiedot (yksi nopeustietojen tietuelohko jokaista sel-laista minuuttia kohden, jolloin ajoneuvo on ollut liikkeessä) 60 nopeuslu-kemaa minuutissa (yksi sekunnissa)
...			
VuDetailedSpeedBlock	SpeedBlockBeginDate	4	
	speedsPerSecond	60	
...			
Signature		128	Kaikkien tietojen RSA-allekirjoitus noOfSpeedBlocks-tiedosta viimeisen nopeuteen liittyvän tietuelohkon viimeiseen tavuun

2.2.6.5 Positive Response Transfer Data Technical Data

DDP_033 Positive Response Transfer Data Technical Data -viestin datakentän on sisällettävä seuraavat tiedot seuraavassa järjestyksessä palvelun SID-tunnisteen arvon ollessa 76h ja TREP-tunnisteen arvon ollessa 05h sekä noudatettava asianmukaista osaviesteihin jakamista ja osaviestien laskemista:

Dataelementti		Pituus (Tavua)	Selite
VuIdentification			
vuManufacturerName		36	Kaikki ajoneuvoyksikköön tallennetut kalibrointeihin liittyvät tiedot
vuManufacturerAddress		36	
vuPartNumber		16	
vuSerialNumber		8	
vuSoftwareIdentification			
vuSoftwareVersion		4	
vuSoftInstallationDate		4	
vuManufacturingDate		4	
vuApprovalNumber		8	
SensorPaired			
sensorSerialNumber		8	
sensorApprovalNumber		8	
sensorPairingDateFirst		4	
VuCalibrationData			
noOfVuCalibrationRecords		1	
...		(164)	
VuCalibrationRecord	calibrationPurpose	1	
	workshopName	36	
	workshopAddress	36	
	workshopCardNumber	18	
	workshopCardExpiryDate	4	
	vehicleIdentificationNumber	17	
	vehicleRegistrationIdentification		
	vehicleRegistrationNation	1	
	vehicleRegistrationNumber	14	
	wVehicleCharacteristicConstant	2	
	kConstantOfRecordingEquipment	2	
	lTyreCircumference	2	
	tyreSize	15	
	authorisedSpeed	1	
	oldOdometerValue	3	
newOdometerValue	3		
oldTimeValue	4		
newTimeValue	4		
nextCalibrationDate	4		
...			
Signature		128	Kaikkien tietojen RSA-allekirjoitus vu-ManufacturerName-tiedosta viimeisen VuCalibrationRecord-tietueen viimeiseen tavuun

2.3 Tiedostojen tallennus ulkoisille tietovälineille (ESM)

DDP_034 Kun tietojen kopiointiin on liittynyt niiden siirto ajoneuvoyksiköstä, IDE-laitteen on tallennettava yhteen fyysiseen tiedostoon kaikki ajoneuvoyksiköstä kopiointin aikana Positive Response Transfer Data -viesteissä saadut tiedot. Viestien otsikoita, osaviestien laskureita, tyhjiä osaviestejä tai tarkistussummia ei tallenneta, mutta SID- ja TREP-tunnisteet tallennetaan (vain ensimmäisen osaviestin tunnisteet tapauksissa, joissa on useita osaviestejä).

3. AJOPiIRTURIKORTILLA OLEVIIEN TIETOJEN KOPIOINTIPROTOKOLLA

3.1 Sovellusalue

Tässä kohdassa kuvataan kortilla olevien tietojen kopiointia suoraan IDE-laitteeseen. Koska IDE-laite ei ole osa tietoturvattua ympäristöä, kortin ja IDE-laitteen välillä ei suoriteta todentamista.

3.2 Määritelmät

Kopiointijakso: Jokainen kerta, jolloin ICC-kortilla olevia tietoja kopioidaan. Jaksioon sisältyy kaikki toimenpiteet IFD-laitteen ICC-kortille antamasta Reset-komennosta ICC-kortin deaktivointiin (kortin poistamiseen tai uuteen Reset-komennukseen) saakka.

Allekirjoitettu tiedosto: ICC-kortilta peräisin oleva tiedosto. Tiedosto siirretään IFD-laitteelle selväkielisenä. ICC-kortilla tiedosto käsitellään hash-algoritmilla ja allekirjoitetaan ja näin saatu allekirjoitus siirretään IFD-laitteelle.

3.3 Kortilla olevien tietojen kopiointi

DDP_035 Ajopiirturikortilla olevien tietojen kopiointi tapahtuu seuraavasti:

- Kopioidaan kortin EF-tiedostoissa ICC ja IC olevat yleiset tiedot. Nämä tiedot ovat valinnaisia, eikä niitä ole suojattu digitaalisella allekirjoituksella.
- Kopioidaan EF-tiedostojen Card_Certificate ja CA_Certificate tiedot. Niitä ei ole suojattu digitaalisella allekirjoituksella. Näiden tiedostojen tiedot on kopioitava aina, kun kortilla olevia tietoja kopioidaan.
- Kopioidaan muiden sovellustietoja sisältävien (Tachograph-DF-tiedoston alaisten) EF-tiedostojen (paitsi Card_Download-tiedoston) tiedot. Nämä tiedot on suojattu digitaalisella allekirjoituksella.
 - Aina, kun kortilla olevia tietoja kopioidaan, on kopioitava ainakin tiedot, jotka ovat EF-tiedostoissa nimeltään Application_Identification ja ID.
 - Kuljettajakortilla olevia tietoja kopioitaessa on myös kopioitava ainakin seuraavien EF-tiedostojen sisältämät tiedot:
 - Events_Data,
 - Faults_Data,
 - Driver_Activity_Data,
 - Vehicles_Used,
 - Places,
 - Control_Activity_Data,
 - Specific_Conditions.
- Kuljettajakortilla olevia tietoja kopioitaessa päivitetään EF-tiedostossa LastCard_Download sijaitseva Card_Download-päivämäärä.
- Korjaamokortilla olevia tietoja kopioitaessa asetetaan EF-tiedostossa Card_Download oleva kalibrointilaskuri alku-tilaansa.

3.3.1 Kopiointiin aloittava komentosarja

DDP_036 IDE-laitteen on aloitettava komentosarja seuraavasti:

Kortti	Komennon suunta	IDE-laite / Liitäntälaite	Merkitys / Huomautuksia
	↵	Alkutilaan asettava Reset-komento	
ATR	⇒		

Valinnaisesti voidaan PPS-toiminnon avulla valita suurempi siirtonopeus, jos kortti tukee sitä.

3.3.2 Komentosarja tiedostoille, joilla ei ole allekirjoitusta

DDP_037 EF-tiedostojen ICC, IC, Card_Certificate ja CA_Certificate sisältämät tiedot kopioidaan seuraavan komentosarjan avulla:

Kortti	Komennon suunta	IDE-laite / Liitäntälaite	Merkitys / Huomautuksia
	↵	SELECT FILE	Valitaan tiedosto tunnistensa perusteella
OK	⇒		
	↵	READ BINARY	Jos tiedostossa on enemmän tietoja kuin kortinlukulaitteen tai kortin puskuriin mahtuu, komento on toistettava, kunnes koko tiedoston tiedot on luettu
Tiedoston tiedot kunnossa (File Data OK)	⇒	Tallenna tiedot ulkoiselle muistivälille (Store data to ESM)	Kohdan 3.4, Tiedontalennuksen muoto, mukaan

Huomautus: Ennen kuin valitaan EF-tiedosto Card_Certificate EF, on valittava ajopiirturikortin sovellus (sovellustunnisteen (AID) perusteella).

3.3.3 Komentosarja tiedostoille, joilla on allekirjoitus

DDP_038 Seuraavaa komentosarjaa on käytettävä kaikille niille tiedostoille, joiden sisältämät tiedot on kopioitava allekirjoituksen kera:

Kortti	Komennon suunta	IDE-laite / Liitäntälaite	Merkitys / Huomautuksia
	↵	SELECT FILE	
OK	⇒		
	↵	PERFORM HASH OF FILE	Laskee valitun tiedoston tietoja vastaavan hash-algoritmin tuloksen lisäyksen 11 mukaisen hash-algoritmin avulla. Tämä komento ei ole ISO-standardin mukainen.
Laske tiedoston tietoja vastaava hash-algoritmin tulos ja tallenna se väliaikaisesti			
OK	⇒		
	↵	READ BINARY	Jos tiedostossa on enemmän tietoja kuin kortinlukulaitteen tai kortin puskuriin mahtuu, komento on toistettava, kunnes koko tiedoston tiedot on luettu
Tiedoston tiedot kunnossa	⇒	Tallenna vastaanotetut tiedot ulkoiselle muistivälille	Kohdan 3.4, Tiedontalennuksen muoto, mukaan
	↵	PSO: COMPUTE DIGITAL SIGNATURE	
Suorita Compute Digital Signature -turvatoimi tilapäisesti tallennetun hash-algoritmin tuloksen avulla			
Allekirjoitus kunnossa	⇒	Liitä tiedot ulkoiselle muistivälille aiemmin tallennettuihin tietoihin	Kohdan 3.4, Tiedontalennuksen muoto, mukaan

3.3.4 Kommentisarja, jolla kalibrointilaskuri asetetaan alkutilaansa

DDP_039 Card_Download-EF-tiedostossa oleva NoOfCalibrationsSinceDownload-laskuri asetetaan alkutilaansa seuraavan komentosarjan avulla:

Kortti	Komennon suunta	IDE-laite / Liitäntälaite	Merkitys / Huomautuksia
	↩	SELECT FILE EF Card_Download	Valitaan tiedosto tunnisteensa perusteella
OK	⇒		
	↩	UPDATE BINARY NoOfCalibrationsSinceDownload = '00 00'	
asettaa kortin tietojen kopiointikertoja osoittavan luvun alkutilaansa			
OK	⇒		

3.4 Tiedontalennuksen muoto

3.4.1 Johdanto

DDP_040 Kopioidut tiedot on tallennettava seuraavasti:

- Tiedot on tallennettava transparent-tiedostorakenteen mukaisesti. Tämä tarkoittaa, että sekä tavujen järjestys että tavujen sisältämien bittien järjestys on tallennettaessa säilytettävä.
- Kaikki yhdellä kertaa kopioidut kortilla olevien tiedostojen tiedot tallennetaan yhteen ulkoisen tietovälineen tiedostoon.

3.4.2 Tiedostomuoto

DDP_041 Tiedostomuoto koostuu sarjasta TLV-koodattuja (tuntomerkki, pituus, sisältö) tietueita.

DDP_042 EF-tiedoston tuntomerkin on oltava tiedostotunniste (FID), johon on lisätty jatke 00h.

DDP_043 EF-tiedoston allekirjoituksen tuntomerkin on oltava kyseisen tiedoston tiedostotunniste (FID), johon on lisätty jatke 01h.

DDP_044 Pituus ilmaistaan kahdella tavulla. Ne määrittelevät sisältökentässä olevien tavujen määrän. Pituuskentän arvo FFh FFh on varattu tulevaan käyttöön.

DDP_045 Jos tiedoston tietoja ei ole kopioitu, mitään tähän tiedostoon liittyviä tietoja ei tallenneta (ei tunnusmerkkiä eikä nollapi-tuutta).

DDP_046 Allekirjoitus on tallennettava seuraavana TLV-koodattuna tietueena heti tiedoston tiedot sisältävän TLV-koodatun tietueen jälkeen.

Määrite	Merkitys	Pituus
FID (2 tavua) '00'	EF-tiedoston tuntomerkki (FID)	3 tavua
FID (2 tavua) '01'	EF-tiedoston allekirjoituksen tuntomerkki (FID)	3 tavua
xx xx	Sisältökentän pituus	2 tavua

Esimerkki ulkoisella muistivälineellä olevaan tiedostoon kopioiduista tiedoista:

Tuntomerkki	Pituus	Sisältö
00 02 00	00 11	EF-tiedoston ICC tiedot
C1 00 00	00 C2	EF-tiedoston Card_Certificate tiedot
		...
05 05 00	0A 2E	EF-tiedoston Vehicles_Used tiedot
05 05 01	00 80	EF-tiedoston Vehicles_Used allekirjoitus

4. AJOPIIRTURIKORTILLA OLEVIEN TIETOJEN KOPIOINTI AJONEUVOYKSIKÖN KAUTTA

- DDP_047 Ajoneuvoyksikön on sallittava siihen asetetun kuljettajakortin tietojen kopioiminen siihen kytkettyyn IDE-laitteeseen.
- DDP_048 IDE-laitteen on käynnistettävä tämä toimintatila lähettämällä ajoneuvoyksikölle Transfer Data Request Card Download -viesti (ks. 2.2.2.9).
- DDP_049 Ajoneuvoyksikön on tämän jälkeen kopioitava kaikki kortilla olevat tiedot, tiedosto kerrallaan kohdassa 3 määritellyn kortilla olevien tietojen kopiointiprotokollan mukaisesti, ja siirrettävä kaikki kortilta saadut tiedot edelleen IDE-laitteeseen asianmukaisesti TLV-koodattuina (ks. 3.4.2) ja Positive Response Transfer Data -viestiin sisällytettynä.
- DDP_050 IDE-laitteen on palautettava tiedot Positive Response Transfer Data -viestistä (poistamalla kaikki ylätunnisteet, SID-tunnisteet, TREP-tunnisteet, osaviestilaskurit ja tarkistussummat) ja tallennettava ne yhteen fyysisen tiedostoon siten kuin kohdassa 2.3 on kuvattu.
- DDP_051 Ajoneuvoyksikön on sen jälkeen tarvittaessa päivitettävä kuljettajakortilla olevien ControlActivityData-tiedoston tai Card_Download-tiedoston tiedot.
-

Lisäys 8

KALIBROINTIPROTOKOLLA

SISÄLLYSLUETTELO

1.	Johdanto	170
2.	Nimitykset, määritelmät ja viitetiedot	170
3.	Palvelujen yhteenveto	170
3.1	Käytettävissä olevat palvelut	170
3.2	Vastauskoodit	171
4.	Viestintäpalvelut	171
4.1	StartCommunication-palvelu	171
4.2	StopCommunication-palvelu	173
4.2.1	Viestin kuvaus	173
4.2.2	Viestin muoto	174
4.2.3	Parametrien määrittely	175
4.3	TesterPresent-palvelu	175
4.3.1	Viestin kuvaus	175
4.3.2	Viestin muoto	175
5.	Hallintapalvelut	176
5.1	StartDiagnosticSession-palvelu	176
5.1.1	Viestin kuvaus	176
5.1.2	Viestin muoto	177
5.1.3	Parametrien määrittely	178
5.2	SecurityAccess-palvelu	178
5.2.1	Viestin kuvaus	178
5.2.2	Viestin muoto – SecurityAccess – requestSeed	179
5.2.3	Viestin muoto – SecurityAccess – sendKey	180
6.	Tiedonsiirtopalvelut	181
6.1	ReadDataByIdentifier-palvelu	181
6.1.1	Viestin kuvaus	181
6.1.2	Viestin muoto	181
6.1.3	Parametrien määrittely	182
6.2	WriteDataByIdentifier-palvelu	183
6.2.1	Viestin kuvaus	183
6.2.2	Viestin muoto	183
6.2.3	Parametrien määrittely	184
7.	Testipulslien ohjaus — tulo-/lähtösignaalien ohjauksen toimintayksikkö	184
7.1	InputOutputControlByIdentifier-palvelu	184

7.1.1	Viestin kuvaus	184
7.1.2	Viestin muoto	185
7.1.3	Parametrien määrittely	186
8.	Datatietueiden muoto	187
8.1	Lähetettävät parametriarvot	187
8.2	Datatietueiden muoto	188

1. JOHDANTO

Tässä lisäyksessä kuvataan tietojen vaihtoa ajoneuvoyksikön ja koestuslaitteen välillä käyttäen K-johdinta, joka on osa lisäyksessä 6 kuvattua kalibrointiliitäntälaitetta. Tässä lisäyksessä kuvataan myös kalibrointiliittimen tulo-/lähtösignaalijohtimen ohjausta.

K-johtimen kautta tapahtuvan viestiyhteyden luonti kuvataan kohdassa 4, Viestintäpalvelut.

Tässä lisäyksessä käytetään käsitettä diagnostiset 'jaksot', joiden avulla määritellään K-johtimen ohjauksen vaikutusala eri olosuhteissa. Oletusarvoinen jakso on StandardDiagnosticSession, jonka aikana kaikki ajoneuvoyksikössä olevat tiedot voidaan lukea, mutta ajoneuvoyksikköön ei voida kirjoittaa mitään tietoja.

Diagnostisen käyttöjakson valinta on selostettu kohdassa 5, Hallintapalvelut.

CPR_001 ECUProgrammingSession-jakson aikana voidaan syöttää tietoja ajoneuvoyksikköön. Kun syötetään kalibrointiin liittyviä tietoja (vaatimukset 097 ja 098), ajoneuvoyksikön on lisäksi oltava CALIBRATION (kalibrointi)-toimintatilassa.

K-johtimen kautta tapahtuva tiedonsiirto kuvataan kohdassa 6, Tiedonsiirtopalvelut. Siirrettävän datan formaatit kuvataan kohdassa 8, Datatietueiden formaatit.

CPR_002 ECUAdjustmentSession-jakson aikana voidaan valita kalibroinnin tulo-/lähtösignaalijohtimen tila K-johdinliitännän avulla. Kalibroinnin tulo-/lähtösignaalijohtimen ohjaus on selostettu kohdassa 7, Testipulssien ohjaus – tulo-/lähtösignaalien ohjauksen toimintayksikkö.

CPR_003 Tässä asiakirjassa on testauslaitteen osoitteesta käytetty merkintää 'tt'. Vaikka testauslaitteilla saattaakin olla ensisijaisia osoitteita, ajoneuvoyksikön on vastattava oikein mihin hyvänsä testauslaitteen osoitteeseen. Ajoneuvoyksikön fyysinen osoite on 0xEE.

2. NIMITYKSET, MÄÄRITELMÄT JA VIITETIEDOT

Protokollat, viestit ja virhekoodit perustuvat pääpiirteissään nykyiseen standardiin ISO 14229-1 (Road vehicles – Diagnostic systems – Part 1: Diagnostic services. Tieliikenteessä käytettävät ajoneuvot. Diagnostiikkajärjestelmät. Osa 1: Diagnostiikkapalvelut, versio 6, 22. helmikuuta 2001).

Palvelutunnisteet, palvelupyynnöt ja niiden vastaukset sekä standardiparametrit on esitetty tavuittain koodattuina heksadesimaalilukuina. Nimitys 'testauslaite' tarkoittaa laitteita, joilla ajoneuvoyksikköön syötetään tietoja ohjelmoinnin/kalibroinnin yhteydessä.

Nimityksiä 'asiakas' ja 'palvelin' käytetään standardin ISO 14230 mukaisesti, ja ne viittaavat testauslaitteeseen ja ajoneuvoyksikköön. Viitetiedot:

Nimitykset 'asiakas' ja 'palvelin' viittaavat testauslaitteeseen ja ajoneuvoyksikköön.

Nimitys ECU (Electronic Control Unit, elektroninen ohjausyksikkö) viittaa ajoneuvoyksikköön.

Viitetiedot:

ISO 14230-2: Road Vehicles – Diagnostic Systems – Keyword Protocol 2000 – Part 2: Data Link Layer. First edition: 1999. (Tieliikenteessä käytettävät ajoneuvot. Diagnostiikkajärjestelmät. Avainsanaprotokolla 2000. Osa 2: Siirtotaso. Ensimmäinen painos: 1999).

Ajoneuvot – Diagnostiikkajärjestelmät.

3. PALVELUJEN YHTEENVETO

3.1 Käytettävissä olevat palvelut

Seuraavassa taulukossa on yhteenveto valvontalaitteessa käytettävissä olevista palveluista, jotka on määritelty tässä asiakirjassa.

CPR_004 Taulukossa on esitetty palvelut, jotka ovat käytettävissä toimintakykyisen diagnostisen jakson aikana.

— Ensimmäisessä sarakkeessa luetellaan käytettävissä olevat palvelut.

— Toisessa sarakkeessa on sen kohdan numero tässä lisäyksessä, jossa kyseinen palvelu on määritelty.

- Kolmannessa sarakkeessa on palvelupyynnöissä käytettävä kyseisen palvelun palvelutunniste (SID).
- Neljännessä sarakkeessa määritellään ne StandardDiagnosticSession-jakson (SD) palvelut, jotka tarvitaan kaikissa ajoneuvoyksiköissä.
- Viidennessä sarakkeessa määritellään ne ECUAdjustmentSession-jakson (ECUAS) palvelut, joiden on oltava käytettävissä ajoneuvoyksikön etulevyssä olevan kalibrointiliittimen tulo-/lähtösignaalihoitimen ohjaukseen.
- Kuudennessä sarakkeessa määritellään ne ECUProgrammingSession-jakson (ECUPS) palvelut, jotka tarvitaan ajoneuvoyksikön parametrien ohjelmoimiseen.

Taulukko 1

Palvelutunnisteiden yhteenveto

Diagnostinen palvelu	Diagnostinen palvelu	Sid pyynnön arvo	Diagnostiset jaksot		
			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		■	

■ Tämä merkki tarkoittaa, että kyseinen palvelu on pakollinen tämän diagnostisen jakson aikana.
 ■ Ei merkkiä tarkoittaa, että kyseinen palvelu ei ole sallittu tämän diagnostisen jakson aikana.

3.2 Vastauskoodit

Vastauskoodit on määritelty kullekin palvelulle.

4. VIESTINTÄPALVELUT

Jotkin palvelut ovat tarpeen viestintäyhteyden luomiseksi ja ylläpitämiseksi. Ne eivät ole mukana sovellustasossa. Käytävissä olevat palvelut on esitetty seuraavassa taulukossa:

Taulukko 2

Viestintäpalvelut

Palvelu	Kuvaus
StartCommunication	Asiakas pyytää, että aloitetaan viestintäjakso palvelimen (palvelimien) kanssa
StopCommunication	Asiakas pyytää, että meneillään oleva viestintäjakso lopetetaan
TesterPresent	Asiakas ilmoittaa palvelimelle, että se on edelleen valmiudessa

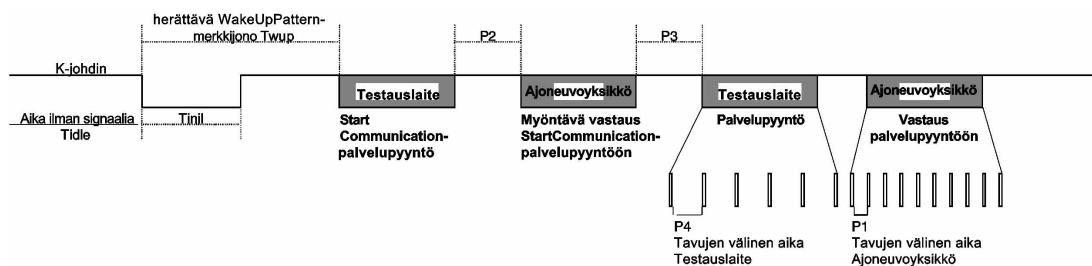
CPR_005 StartCommunication-palvelua käytetään aloittamaan viestintä. Ennen kuin mitään palvelua voidaan suorittaa, viestintäyhteys on alustettava ja viestintäparametrien on oltava halutun toimintatilan mukaisia.

4.1 StartCommunication-palvelu

CPR_006 Vastaanotettuaan StartCommunication-pyynnön esittävän perusalkion ajoneuvoyksikön on tarkastettava, voidaanko viestintäyhteys näissä olosuhteissa alustaa. Olosuhteet, joissa viestintäyhteys voidaan alustaa, on kuvattu asiakirjassa ISO 14230-2.

CPR_007 Tämän jälkeen ajoneuvoyksikön on tehtävä kaikki toimet, joita vaaditaan viestintäyhteyden alustamiseksi ja lähetettävä StartCommunication-vastauksen antava perusalkio valittujen myöntävän vastauksen (Positive Response) parametrien kanssa.

- CPR_008 Jos ajoneuvoyksikkö, joka jo on alustettu (ja aloittanut jonkin diagnostisen jakson), vastaanottaa uuden StartCommunication-pyyntö (esimerkiksi testauslaitteen virhetilasta palautumisen takia), on pyyntö hyväksyttävä ja ajoneuvoyksikkö alustettava uudelleen.
- CPR_009 Jos viestintäyhteyttä ei jostain syystä voida alustaa, ajoneuvoyksikön on jatkettava sitä toimintaa, jota se oli suorittamassa juuri ennen viestintäyhteyden alustusyritystä.
- CPR_010 StartCommunication-pyyntölle on annettava fyysinen osoite.
- CPR_011 Ajoneuvoyksikön alustus palveluja varten tapahtuu käyttäen 'nopeaa alustustapaa':
- ennen kutakin toimintoa on jakso, jolloin väylä on tyhjänä,
 - tämän jälkeen testauslaite lähettää alustusmerkkijonon,
 - kaikki viestintäyhteyden luomisessa tarvittavat tiedot sisältyvät ajoneuvoyksikön vastaukseen.
- CPR_012 Alustuksen päätyttyä:
- Kaikki viestintäparametrit on asetettu avaintavujen mukaisiin taulukossa 4 – Viestinnässä käytettävät ajoitusarvot – määritelyihin arvoihin.
 - Ajoneuvoyksikkö odottaa testauslaitteen ensimmäistä pyyntöä.
 - Ajoneuvoyksikkö on oletusarvoisessa diagnostisessa toimintatilassa eli StandardDiagnosticSession-tilassa.
 - Kalibroinnin tulo-/lähtösignaalijohdin on oletusarvoisessa eli toimintakyvyttömässä tilassa.
- CPR_014 K-johtimen nopeudeksi on säädetty 10 400 baudia.
- CPR_016 Nopea alustus alkaa siten, että testauslaite lähettää herättävän WakeUpPattern (Wup)-merkkijonon K-johtimen kautta. Merkkijono alkaa Tinil-ajan pituisella loogisen tason pidolla nollassa K-johtimen oltua siihen asti ilman signaalia. Testauslaite lähettää StartCommunication-palvelun ensimmäisen bitin, kun signaalin ensimmäisestä laskevasta reunasta on kulunut aika Twup.



- CPR_017 Nopeassa alustuksessa ja viestinnässä yleensä käytettävät ajoitusarvot on esitetty seuraavissa taulukoissa. Ilman signaalia olevalle ajalle (Tidle) on erilaisia vaihtoehtoja:
- Ensimmäinen lähetys virran kytkemisen jälkeen: Tidle = 300 ms.
 - StopCommunication-palvelun päättymisen jälkeen: Tidle = ajan P3 vähimmäisarvo.
 - Viestinnän päätyttyä P3:n enimmäisarvoa vastaavan odotusajan kuluttua: Tidle = 0.

Taulukko 3

Nopeassa alustuksessa käytettävät ajoitusarvot

Ajoitusparametri		vähimmäisarvo	enimmäisarvo
Tinil	25 ± 1 ms	24 ms	26 ms
Twup	50 ± 1 ms	49 ms	51 ms

Taulukko 4

Viestinnässä käytettävät ajoitusarvot

Ajoitus-parametri	Parametrin selite	Alemmat raja-arvot [ms]	Ylemmät raja-arvot [ms]
		vähintään	enintään
P1	Tavujen välinen aika ajoneuvoyksikön vastauksessa	0	20
P2	Testauslaitteen palvelupyynnön ja ajoneuvoyksikön vastauksen tai ajoneuvoyksikön kahden vastauksen välinen aika	25	250
P3	Ajoneuvoyksikön vastauksen lopun ja testauslaitteen uuden palvelupyynnön alun välinen aika	55	5 000
P4	Tavujen välinen aika testauslaitteen palvelupyynnössä	5	20

CPR_018 Nopeassa alustuksessa käytettävien viestien muoto on esitetty seuraavissa taulukoissa.

Taulukko 5

StartCommunication-palvelupyynnön sisältävä viesti

Tavun nro	Parametri	Arvo (Hex)	Muistikas
#1	Muototavu – fyysinen osoittaminen	81	FMT
#2	Kohteen osoitetavu	EE	TGT
#3	Lähteen osoitetavu	tt	SRC
#4	StartCommunication-palvelupyynnön tunniste	81	SCR
#5	Tarkistussumma	00-FF	CS

Taulukko 6

StartCommunication-palvelupyynnön annettavan myöntävän vastauksen sisältävä viesti

Tavun nro	Parametri	Arvo (Hex)	Muistikas
#1	Muototavu – fyysinen osoittaminen	80	FMT
#2	Kohteen osoitetavu	tt	TGT
#3	Lähteen osoitetavu	EE	SRC
#4	Pituutta osoittava lisätavu	03	LEN
#5	StartCommunication-palvelupyynnön annettavan myöntävän vastauksen tunniste	C1	SCRPR
#6	Avaintavu	EA	KB1
#7	Avaintavu 2	8F	KB2
#8	Tarkistussumma	00-FF	CS

CPR_019 StartCommunication-palvelupyynnön ei ole olemassa kieltävää vastausta; jos myöntävää vastausta ei voida lähettää, ajoneuvoyksikkö ei alusteta, mitään ei lähetetä ja ajoneuvoyksikkö jatkaa normaalia toimintaansa.

4.2 StopCommunication-palvelu

4.2.1 Viestin kuvaus

Tätä liikennekerroksen palvelua käytetään päättämään viestintäjakso.

CPR_020 Vastaanotettuaan StopCommunication-pyynnön esittävän perusalkion, ajoneuvoyksikön on tarkastettava, voidaanko viestintäyhteys näissä olosuhteissa katkaista. Tässä tapauksessa ajoneuvoyksikön on suoritettava kaikki tämän viestintäyhteyden katkaisemisessa tarvittavat toimet.

CPR_021 Jos viestintäyhteyden katkaiseminen on mahdollista, ajoneuvoyksikön on annettava StopCommunication-palvelupyynnön vastauksen esittävä perusalkio valittujen myöntävän vastauksen (Positive Response) parametrien kanssa, ennen kuin viestintäyhteys katkaistaan.

CPR_022 Jos viestintäyhteyttä ei jostain syystä voida katkaista, ajoneuvoyksikön on annettava StopCommunication-palvelupyynnön vastauksen esittävä perusalkio valittujen kieltävän vastauksen (Negative Response) parametrien kanssa.

CPR_023 Jos ajoneuvoyksikkö havaitsee, että ajan P3 enimmäisarvoa vastaava odotusaika on ylitetty, viestintäyhteys katkaistaan ilman, että annetaan mitään vastausta esittävää perusalkiota.

4.2.2 Viestin muoto

CPR_024 StopCommunication-perusalkioiden viestien muodot on esitetty seuraavassa taulukossa.

Taulukko 7

StopCommunication-palvelupyynnön sisältävä viesti

Tavun nro	Parametri	Arvo (Hex)	Muistikas
#1	Muototavu – fyysinen osoittaminen	80	FMT
#2	Kohteen osoitetavu	EE	TGT
#3	Lähteen osoitetavu	tt	SRC
#4	Pituutta osoittava lisätavu	01	LEN
#5	StopCommunication-palvelupyynnön annettavan myöntävän vastauksen tunniste	82	SPR
#6	Tarkistussumma	00-FF	CS

Taulukko 8

StopCommunication-palvelupyynnön annettavan myöntävän vastauksen sisältävä viesti

Tavun nro	Parametri	Arvo (Hex)	Muistikas
#1	Muototavu – fyysinen osoittaminen	80	FMT
#2	Kohteen osoitetavu	tt	TGT
#3	Lähteen osoitetavu	EE	SRC
#4	Pituutta osoittava lisätavu	01	LEN
#5	StopCommunication-palvelupyynnön tunniste	C2	SPRPR
#6	Tarkistussumma	00-FF	CS

Taulukko 9

StopCommunication-palvelupyynnön annettavan kieltävän vastauksen sisältävä viesti

Tavun nro	Parametri	Arvo (Hex)	Muistikas
#1	Muototavu – fyysinen osoittaminen	80	FMT
#2	Kohteen osoitetavu	tt	TGT
#3	Lähteen osoitetavu	EE	SRC
#4	Pituutta osoittava lisätavu	03	LEN
#5	Palvelupyynnön annettavan kieltävän vastauksen tunniste	7F	NR
#6	StopCommunication-palvelupyynnön tunniste	82	SPR
#7	responseCode = generalReject (vastauskoodi = yleinen hylkääminen)	10	RC_GR
#8	Tarkistussumma	00-FF	CS

4.2.3 Parametrien määrittely

Tämä palvelu ei tarvitse parametrien määrittelyä.

4.3 TesterPresent-palvelu

4.3.1 Viestin kuvaus

Testauslaite ilmoittaa TesterPresent-palvelun avulla palvelimelle olevansa vielä valmiudessa. Näin palvelin ei palaudu automaattisesti normaalitilaan ja mahdollisesti katkaise viestintäyhteyttä. Tämä määräajoin lähetettävä palvelu pitää diagnostiikkajakson/viestintäyhteyden aktiivisena nollaamalla P3-laskurin aina, kun tällainen palvelupyynnö vastaanotetaan.

4.3.2 Viestin muoto

CPR_079 TesterPresent-perusalkioiden viestien muodot on esitetty seuraavassa taulukossa.

Taulukko 10

TesterPresent-palvelupyynnön sisältävä viesti

Tavun nro	Parametri	Arvo (Hex)	Muistikas
#1	Muototavu – fyysinen osoittaminen	80	FMT
#2	Kohteen osoitetavu	EE	TGT
#3	Lähteen osoitetavu	tt	SRC
#4	Pituutta osoittava lisätavu	02	LEN
#5	TesterPresent-palvelupyynnön tunnistus	3E	TP
#6	Sub Function = responseRequired = [kyllä (yes) ei (no)]	01 02	RESPREQ_Y RESPREQ_NO
#7	Tarkistussumma	00-FF	CS

CPR_080 Jos responseRequired-parametrin arvon on 'yes', palvelin vastaa seuraavalla myönteisellä vastausviestillä. Jos arvo on 'no', palvelin ei lähetä vastausta.

Taulukko 11

TesterPresent-palvelupyynnöön annettavan myöntävän vastauksen sisältävä viesti

Tavun nro	Parametri	Arvo (Hex)	Muistikas
#1	Muototavu – fyysinen osoittaminen	80	FMT
#2	Kohteen osoitetavu	tt	TGT
#3	Lähteen osoitetavu	EE	SRC
#4	Pituutta osoittava lisätavu	01	LEN
#5	TesterPresent-palvelupyynnöön annettavan myöntävän vastauksen tunnistus	7E	TPPR
#6	Tarkistussumma	00-FF	CS

CPR_081 Palvelun on tuettava seuraavia kielteisiä vastauskoodeja:

Taulukko 12

TesterPresent-palvelupyynnön annettavan kieltävän vastauksen sisältävä viesti

Tavun nro	Parametri	Arvo (Hex)	Muistikas
#1	Muototavu – fyysinen osoittaminen	80	FMT
#2	Kohteen osoitetavu	tt	TGT
#3	Lähteen osoitetavu	EE	SRC
#4	Pituutta osoittava lisätavu	03	LEN
#5	Palvelupyynnön annettavan kieltävän vastauksen tunniste	7F	NR
#6	TesterPresent-palvelupyynnön tunniste	3E	TP
#7	responseCode = [SubFunctionNotSupported-InvalidFormat incorrectMessageLength]	12	RC_SFNS_IF
		13	RC_IML
#8	Tarkistussumma	00-FF	CS

5. HALLINTAPALVELUT

Käytettävissä olevat palvelut on esitetty seuraavassa taulukossa:

Taulukko 13

Hallintapalvelut

Palvelu	Kuvaus
StartDiagnosticSession	Asiakas pyytää, että aloitetaan diagnostinen jakso ajoneuvoyksikön kanssa
SecurityAccess	Asiakas pyytää saada käyttöönsä toimintoja, joiden käyttöoikeudet on vain tietyillä käyttäjillä

5.1 StartDiagnosticSession-palvelu

5.1.1 Viestin kuvaus

CPR_025 StartDiagnosticSession-palvelun avulla käynnistetään palvelimessa erilaisia diagnostisia jaksoja. Diagnostinen jakso mahdollistaa tiettyjen palvelujen käytön taulukon 17 – diagnosticSession-parametrin arvojen määritelmät – mukaisesti. Jakso voi mahdollistaa ajoneuvovalmistajakohtaisia palveluja, joita ei kuvata tässä asiakirjassa. Suoritussäännöt ovat seuraavien vaatimusten mukaiset:

- Ajoneuvoyksikössä on aina oltava tasan yksi diagnostinen jakso aktiivisena.
- Virran kytkeydyttyä ajoneuvoyksikön on aina käynnistettävä StandardDiagnosticSession-jakso. Ellei muuta diagnostista jaksoa aloiteta, StandardDiagnosticSession-jakson on jatkettava niin kauan kuin ajoneuvoyksikön virta on kytkettyä.
- Jos testauslaite pyytää jo aktiivisena olevaa diagnostista jaksoa, ajoneuvoyksikön on lähetettävä myönteinen vastausviesti.
- Aina testauslaitteen pyytäessä uutta diagnostista jaksoa ajoneuvoyksikkö lähettää ensin myönteisen vastauksen StartDiagnosticSession-pyyntöön ennen kuin uusi jakso aktivoituu ajoneuvoyksikössä. Jos ajoneuvoyksikkö ei voi käynnistää pyydettyä uutta diagnostista jaksoa, se vastaa StartDiagnosticSession-pyyntöön kielteisellä viestillä ja jatkaa meneillään olevaa jaksoa.

CPR_026 Diagnostinen jakso saa alkaa vain, jos asiakkaan ja ajoneuvoyksikön välille on luotu viestintäyhteys.

CPR_027 Taulukossa 4 määritellyt ajoitusparametrit on otettava käyttöön, kun StartDiagnosticSession-pyyntöön, johon on liitetty diagnosticSession-parametri asetettuna arvoon StandardDiagnosticSession, annetaan myöntävä vastaus, jos jokin diagnostinen jakso oli aikaisemmin käynnissä.

5.1.2 Viestin muoto

CPR_028 StartDiagnosticSession-perusalkioiden viestien muodot on esitetty seuraavassa taulukossa.

Taulukko 14

StartDiagnosticSession-palvelupyynnön sisältävä viesti

Tavun nro	Parametri	Arvo (Hex)	Muistikas
#1	Muototavu – fyysinen osoittaminen	80	FMT
#2	Kohteen osoitetavu	EE	TGT
#3	Lähteen osoitetavu	tt	SRC
#4	Pituutta osoittava lisätavu	02	LEN
#5	StartDiagnosticSession-palvelupyynnön tunniste	10	STDS
#6	diagnosticSession = (diagnostinen jakso) [jokin taulukon 17 arvo]	xx	DS_...
#7	Tarkistussumma	00-FF	CS

Taulukko 15

StartDiagnosticSession-palvelupyynnön annettavan myöntävän vastauksen sisältävä viesti

Tavun nro	Parametri	Arvo (Hex)	Muistikas
#1	Muototavu – fyysinen osoittaminen	80	FMT
#2	Kohteen osoitetavu	tt	TGT
#3	Lähteen osoitetavu	EE	SRC
#4	Pituutta osoittava lisätavu	02	LEN
#5	StartDiagnosticSession-palvelupyynnön annettavan myöntävän vastauksen tunniste	50	STDSPR
#6	diagnosticSession = [sama kuin tavun 6 arvo taulukossa 14]	xx	DS_...
#7	Tarkistussumma	00-FF	CS

Taulukko 16

StartDiagnosticSession-palvelupyynnön annettavan kieltävän vastauksen sisältävä viesti

Tavun nro	Parametri	Arvo (Hex)	Muistikas
#1	Muototavu – fyysinen osoittaminen	80	FMT
#2	Kohteen osoitetavu	tt	TGT
#3	Lähteen osoitetavu	EE	SRC
#4	Pituutta osoittava lisätavu	03	LEN
#5	Palvelupyynnön annettavan kieltävän vastauksen tunniste	7F	NR
#6	StartDiagnosticSession-palvelupyynnön tunniste	10	STDS
#7	ResponseCode = [subFunctionNotSupported ^(a) incorrectMessageLength ^(b) conditionsNotCorrect ^(c)]	12 13 22	RC_SFNS RC_IML RC_CNC
#8	(Checksum) Tarkistussumma	00-FF	CS

^(a) Palvelupyynnöviestin tavulle 6 annettua arvoa ei tueta, ts. sitä ei ole taulukossa 17.

^(b) Viestin pituus on väärä.

^(c) StartDiagnosticSession-pyynnölle asetetut vaatimukset eivät täyty.

5.1.3 Parametrien määrittely

CPR_029 diagnosticSession (DS_) -parametrin avulla StartDiagnosticSession-palvelu valitsee tietyn palvelimen (palvelimien) toimintatavan. Tässä asiakirjassa on määritelty seuraavat diagnostiset jaksot:

Taulukko 17

diagnosticSession-parametrin arvojen määritelmät

Hex	Kuvaus	Muistikas
81	StandardDiagnosticSession Mahdollistaa kaikki taulukossa 1, sarakkeessa 4 (SD) kuvatut palvelut. Näiden palvelujen avulla voidaan tietoja lukea palvelimelta (ajoneuvoyksiköstä). Tämä diagnostinen jakso on käynnissä sen jälkeen, kun asiakkaan (testauslaitteen) ja palvelimen (ajoneuvoyksikön) välinen alustus on onnistuneesti suoritettu. Muut tässä kohdassa määritellyt diagnostiset jaksot voivat syrjäyttää tämän diagnostisen jaksos.	SD
85	ECUProgrammingSession Mahdollistaa kaikki taulukossa 1, sarakkeessa 6 (ECUPS) kuvatut palvelut. Nämä palvelut tukevat palvelimen (ajoneuvoyksikön) muistin ohjelmointia. Muut tässä kohdassa määritellyt diagnostiset jaksot voivat syrjäyttää tämän diagnostisen jaksos.	ECUPS
87	ECUAdjustmentSession Mahdollistaa kaikki taulukossa 1, sarakkeessa 5 (ECUAS) kuvatut palvelut. Nämä palvelut tukevat palvelimen (ajoneuvoyksikön) tulo-lähtösignaalin ohjausta. Muut tässä kohdassa määritellyt diagnostiset jaksot voivat syrjäyttää tämän diagnostisen jaksos.	ECUAS

5.2 SecurityAccess-palvelu

Kalibrointitietojen kirjoittaminen tai kalibrointia varten olevan tulo-/lähtösignaalihohtimen käyttö on mahdollista vain, jos ajoneuvoyksikkö on CALIBRATION-toimintatilassa. Sen lisäksi, että ajoneuvoyksikköön on asettava voimassa oleva korjaamokortti, on siihen syötettävä oikea henkilökohtainen tunnusluku (PIN), jotta CALIBRATION-toimintatila saadaan käyttöön.

SecurityAccess-palvelun avulla voidaan syöttää PIN-tunnusluku ja antaa testauslaitteelle tieto siitä, onko ajoneuvoyksikkö CALIBRATION-toimintatilassa.

PIN-tunnusluvun syöttäminen muilla tavoin on sallittu.

5.2.1 Viestin kuvaus

SecurityAccess-palvelu muodostuu palvelun requestSeed-viestistä ja sitä seuraavasta palvelun sendKey-viestistä. SecurityAccess-palvelu on suoritettava StartDiagnosticSession-palvelun jälkeen.

CPR_033 Testauslaitteen on käytettävä SecurityAccess-palvelun requestSeed-viestiä varmistamaan, että ajoneuvoyksikkö on valmis vastaanottamaan PIN-tunnusluvun.

CPR_034 Jos ajoneuvoyksikkö on jo CALIBRATION-toimintatilassa, sen on vastattava palvelupyyntöön lähettämällä 'siemenluku' 0x0000 käyttäen SecurityAccess-palvelupyynnön myöntävää vastausta.

CPR_035 Jos ajoneuvoyksikkö on valmis vastaanottamaan PIN-tunnusluvun, jotta se voitaisiin todentaa korjaamokortin avulla, sen on vastattava lähettämällä arvoa 0x0000 suurempi 'siemenluku' käyttäen SecurityAccess-palvelupyynnön myöntävää vastausta.

CPR_036 Jos ajoneuvoyksikkö ei ole valmis vastaanottamaan PIN-tunnuslukua testauslaitteelta, joko siksi, että korjaamokortti ei ole voimassa tai siksi, että ajoneuvoyksikkö odottaa, että PIN-tunnusluku syötetään jollain muulla tavoin, sen on vastattava antamalla kieltävä vastaus, jossa vastauskoodille on asetettu vastausta conditionsNotCorrectOrRequestSequenceError vastaava arvo.

CPR_037 Testauslaitteen on lopuksi tämän jälkeen lähetettävä PIN-tunnusluku ajoneuvoyksikölle SecurityAccess-palvelun sendKey-viestin avulla. Jotta kortin tunnistamisprosessille jäisi riittävästi aikaa, ajoneuvoyksikön on jatkettava vastausaikaa kielteisellä viestillä requestCorrectlyReceived-ResponsePending. Vastausaika ei kuitenkaan saa ylittää 5:tä minuuttia. Heti kun pyydetty palvelu on suoritettu, ajoneuvoyksikön on lähetettävä myönteinen tai kielteinen vastausviesti, jolla on eri vastauskoodi Ajoneuvoyksikkö voi toistaa kielteistä vastauskoodia requestCorrectlyReceived-ResponsePending, kunnes pyydetty palvelu on suoritettu ja lopullinen vastausviesti lähetetty.

CPR_038 Ajoneuvoyksikkö saa vastata tähän pyyntöön antamalla SecurityAccess-palvelupyynnön myöntävän vastauksen vain, jos se on CALIBRATION-toimintatilassa.

CPR_039 Seuraavissa tapauksissa ajoneuvoyksikön on annettava tähän palvelupyyntöön kieltävä vastaus siten, että vastauskoodin arvoksi on asetettu:

- subFunctionNot supported: alitoimintoparametrin (accessType) väärä muoto,
- conditionsNotCorrectOrRequestSequenceError: ajoneuvoyksikkö ei ole valmis vastaanottamaan PIN-tunnuslukua,
- invalidKey: PIN-tunnusluku ei ole oikea, mutta tunnusluvun sallittujen syöttöryitysten määrää ei ole ylitetty,
- exceededNumberOfAttempts: PIN-tunnusluku ei ole oikea ja tunnusluvun sallittujen syöttöryitysten määrä on ylitetty,
- generalReject: PIN-tunnusluku on oikea, mutta yksikön ja korjaamokortin välinen todentaminen epäonnistui.

5.2.2 Viestin muoto – SecurityAccess – requestSeed

CPR_040 SecurityAccess-palvelun requestSeed-perusalkioiden viestien muodot on esitetty seuraavissa taulukoissa.

Taulukko 18

SecurityAccess-palvelupyynnön requestSeed-viesti

Tavun nro	Parametri	Arvo (Hex)	Muistikas
#1	Muototavu – fyysinen osoittaminen	80	FMT
#2	Kohteen osoitetavu	EE	TGT
#3	Lähteen osoitetavu	tt	SRC
#4	Pituutta osoittava lisätavu	02	LEN
#5	SecurityAccess-palvelupyynnön tunniste	27	SA
#6	accessType – requestSeed	7D	AT_RSD
#7	Tarkistussumma	00-FF	CS

Taulukko 19

SecurityAccess-palvelupyynnön myönteinen requestSeed-vastausviesti

Tavun nro	Parametri	Arvo (Hex)	Muistikas
#1	Muototavu – fyysinen osoittaminen	80	FMT
#2	Kohteen osoitetavu	tt	TGT
#3	Lähteen osoitetavu	EE	SRC
#4	Pituutta osoittava lisätavu	04	LEN
#5	SecurityAccess-palvelupyyntöön annettavan myöntävän vastauksen tunniste	67	SAPR
#6	accessType – requestSeed	7D	AT_RSD
#7	Siemenluvun (Seed) merkitsevämpi tavu	00-FF	SEEDH
#8	Siemenluvun (Seed) vähemmän merkitsevä tavu	00-FF	SEEDL
#9	Tarkistussumma	00-FF	CS

Taulukko 20

SecurityAccess-palvelupyynnön annettavan kieltävän vastauksen sisältävä viesti

Tavun nro	Parametri	Arvo (Hex)	Muistikas
#1	Muototavu – fyysinen osoittaminen	80	FMT
#2	Kohteen osoitetavu	tt	TGT
#3	Lähteen osoitetavu	EE	SRC
#4	Pituutta osoittava lisätavu	03	LEN
#5	Palvelupyynnön annettavan kieltävän vastauksen tunniste	7F	NR
#6	SecurityAccess-palvelupyynnön tunniste	27	SA1
#7	responseCode = [conditionsNotCorrectOrRequestSequenceError incorrectMessageLength]	22	RC_CNC
		13	RC_JML
#8	Tarkistussumma	00-FF	CS

5.2.3 **Viestin muoto – SecurityAccess – sendKey**

CPR_041 SecurityAccess-palvelun sendKey-perusalkioiden viestien muodot on esitetty seuraavissa taulukoissa.

Taulukko 21

SecurityAccess-palvelupyynnön sendKey- viesti

Tavun nro	Parametri	Arvo (Hex)	Muistikas
#1	Muototavu – fyysinen osoittaminen	80	FMT
#2	Kohteen osoitetavu	EE	TGT
#3	Lähteen osoitetavu	tt	SRC
#4	Pituutta osoittava lisätavu	m+2	LEN
#5	SecurityAccess-palvelupyynnön tunniste	27	SA
#6	accessType – sendKey	7E	AT_SK
#7–#m+6	Avaimen tavu nro 1 (merkitsevin)	xx	KEY
	
	Avaimen tavu nro m (vähiten merkitsevä, m:n arvoin tulee olla vähintään 4 ja enintään 8)	xx	
#m+7	Tarkistussumma	00-FF	CS

Taulukko 22

SecurityAccess-palvelupyynnön myönteinen sendKey-vastausviesti

Tavun nro	Parametri	Arvo (Hex)	Muistikas
#1	Muototavu – fyysinen osoittaminen	80	FMT
#2	Kohteen osoitetavu	tt	TGT
#3	Lähteen osoitetavu	EE	SRC
#4	Pituutta osoittava lisätavu	02	LEN
#5	SecurityAccess-palvelupyynnön annettavan myöntävän vastauksen tunniste	67	SAPR
#6	accessType – sendKey	7E	AT_SK
#7	Tarkistussumma	00-FF	CS

Taulukko 23

SecurityAccess-palvelupyynnön annettavan kieltävän vastauksen sisältävä viesti

Tavun nro	Parametri	Arvo (Hex)	Muistikas
#1	Muototavu – fyysinen osoittaminen	80	FMT
#2	Kohteen osoitettava	tt	TGT
#3	Lähteen osoitettava	EE	SRC
#4	Pituutta osoittava lisätavu	03	LEN
#5	Palvelupyynnön annettavan kieltävän vastauksen tunniste	7F	NR
#6	SecurityAccess-palvelupyynnön tunniste	27	SA
#7	ResponseCode = [generalReject subFunctionNotSupported incorrectMessageLength conditionsNotCorrectOrRequestSequenceError invalidKey exceededNumberOfAttempts requestCorrectlyReceived-ResponsePending]	10 12 13 22 35 36 78	RC_GR RC_SFNS RC_IML RC_CNC RC_IK RC_ENA RC_RCR_RP
#8	Tarkistussumma	00-FF	CS

6. TIEDONSIIRTOPALVELUT

Käytettävissä olevat palvelut on esitetty seuraavassa taulukossa:

Taulukko 24

Tiedonsiirtopalvelut

Palvelu	Kuvaus
ReadDataByIdentifier	Asiakas pyytää, että lähetetään recordDataIdentifier-tunnisteen perusteella käyttöön saatavan tietueen nykyinen arvo
WriteDataByIdentifier	Asiakas pyytää saada kirjoittaa recordDataIdentifier-tunnisteen perusteella käyttöön saatavan tietueen

6.1 ReadDataByIdentifier-palvelu

6.1.1 Viestin kuvaus

CPR_050 ReadDataByIdentifier-palvelun avulla asiakas pyytää datatietueiden arvoja palvelimelta. Data tunnistetaan recordDataIdentifier-tunnisteen avulla. Ajoneuvoyksikön valmistaja vastaa siitä, että palvelimen vaatimukset täytetään tätä palvelua suoritettaessa.

6.1.2 Viestin muoto

CPR_051 ReadDataByIdentifier-perusalkioiden viestien muodot on esitetty seuraavassa taulukossa.

Taulukko 25

ReadDataByIdentifier-palvelupyynnön sisältävä viesti

Tavun nro	Parametri	Arvo (Hex)	Muistikas
#1	Muototavu – fyysinen osoittaminen	80	FMT
#2	Kohteen osoitettava	EE	TGT
#3	Lähteen osoitettava	tt	SRC
#4	Pituutta osoittava lisätavu	03	LEN
#5	ReadDataByIdentifier-palvelupyynnön tunniste	22	RDBI
#6–#7	recordDataIdentifier = [arvo taulukosta 28]	xxxx	RDI_...
#8	Tarkistussumma	00-FF	CS

Taulukko 26

ReadDataByIdentifier-palvelupyyntöön annettavan myöntävän vastauksen sisältävä viesti

Tavun nro	Parametri	Arvo (Hex)	Muistikas
#1	Muototavu – fyysinen osoittaminen	80	FMT
#2	Kohteen osoitettava	tt	TGT
#3	Lähteen osoitettava	EE	SRC
#4	Pituutta osoittava lisätavu	m+3	LEN
#5	ReadDataByIdentifier-palvelupyyntöön annettavan myöntävän vastauksen tunniste	62	RDBIPR
#6–#7	recordDataIdentifier = [sama arvo kuin tavuilla 6 ja 7 taulukosta 25]	xxxx	RDI_...
#8–#m+7	dataRecord[] = [data#1 : data#m]	xx : xx	DREC_DATA1 : DREC_DATAm
#m+8	Tarkistussumma	00-FF	CS

Taulukko 27

ReadDataByIdentifier-palvelupyyntöön annettavan kieltävän vastauksen sisältävä viesti

Tavun nro	Parametri	Arvo (Hex)	Muistikas
#1	Muototavu – fyysinen osoittaminen	80	FMT
#2	Kohteen osoitettava	tt	TGT
#3	Lähteen osoitettava	EE	SRC
#4	Pituutta osoittava lisätavu	03	LEN
#5	Palvelupyyntöön annettavan kieltävän vastauksen tunniste	7F	NR
#6	ReadDataByIdentifier-palvelupyyntöön tunniste	22	RDBI
#7	ResponseCode = [requestOutOfRange incorrectMessageLength conditionsNotCorrect]	31 13 22	RC_ROOR RC_IML RC_CNC
#8	Tarkistussumma	00-FF	CS

6.1.3 Parametrien määrittely

CPR_052 ReadDataByIdentifier-pyyntöön parametri recordDataIdentifier (RDI_) määrittää datatietueen.

CPR_053 Tässä asiakirjassa määritellyt RecordDataIdentifier-parametrin arvot on esitetty seuraavassa taulukossa.

RecordDataIdentifier-parametria koskevassa taulukossa on neljä saraketta ja useita rivejä.

- Ensimmäinen sarake (Hex) sisältää kolmannessa sarakkeessa määritellylle recordDataIdentifier-parametrille annetun arvon heksadesimaalilukuna.
- Toinen sarake (dataelementti) määrittelee lisäyksessä 1 määritellyn dataelementin, johon recordDataIdentifier-parametri perustuu (muunto saattaa olla tarpeen).
- Kolmas sarake (parametrin kuvaus) määrittelee vastaavan recordDataIdentifier-parametrin nimen.
- Neljäs sarake (Muistikas) määrittelee kyseisen recordDataIdentifier-parametrin muistikkaan.

Taulukko 28

recordDataIdentifier-parametrin arvojen määritelmät

Hex	Dataelementti	Nimi Ks. muoto kohdasta 8.2	Muistikas
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 ReadDataByIdentifier-palvelupyynnön annettavan myönteisen vastauksen sisältävässä viestissä käytetään dataRecord (DREC_) -parametria hakemaan recordDataIdentifier-tunnisteen mukainen tietue asiakkaalle (testauslaitteelle). Dataformaatit määritellään kohdassa 8. Käyttäjä voi toteuttaa valinnaisia dataRecord-parametrin arvoja esimerkiksi ajoneuvo-yksikkökohtaisille syöttö- ja tulostustiedoille ja laitteen sisäiseen tiedonsiirtoon. Näitä ei määritellä tässä asiakirjassa.

6.2 WriteDataByIdentifier-palvelu**6.2.1 Viestin kuvaus**

CPR_056 WriteDataByIdentifier-palvelun avulla asiakas voi kirjoittaa datatietueiden arvoja palvelimelle. Data tunnistetaan recordDataIdentifier-tunnisteen avulla. Ajoneuvoyksikön valmistaja vastaa siitä, että palvelimen vaatimukset täytetään tätä palvelua suoritettaessa. Taulukossa 28 lueteltuja parametreja voidaan päivittää vain, kun ajoneuvoyksikkö on CALIBRATION-toimintatilassa.

6.2.2 Viestin muoto

CPR_057 WriteDataByIdentifier-perusalkioiden viestien muodot on esitetty seuraavassa taulukossa.

Taulukko 29

WriteDataByIdentifier-palvelupyynnön sisältävä viesti

Tavun nro	Parametri	Arvo (Hex)	Muistikas
#1	Muototavu – fyysinen osoittaminen	80	FMT
#2	Kohteen osoitettava	EE	TGT
#3	Lähteen osoitettava	tt	SRC
#4	Pituutta osoittava lisätavu	m+3	LEN
#5	WriteDataByIdentifier-palvelupyynnön tunniste	2E	WDBI
#6–#7	recordDataIdentifier = [arvo taulukosta 28]	xxxx	RDI_...
#8–#m+7	dataRecord[] = [data#1 : data#m]	xx : xx	DREC_DATA1 : DREC_DATAm
#m+8	Tarkistussumma	00-FF	CS

Taulukko 30

WriteDataByIdentifier-palvelupyynnön annettavan myöntävän vastauksen sisältävä viesti

Tavun nro	Parametri	Arvo (Hex)	Muistikas
#1	Muototavu – fyysinen osoittaminen	80	FMT
#2	Kohteen osoitetavu	tt	TGT
#3	Lähteen osoitetavu	EE	SRC
#4	Pituutta osoittava lisätavu	03	LEN
#5	WriteDataByIdentifier-palvelupyynnön annettavan myöntävän vastauksen tunniste	6E	WDBIPR
#6–#7	recordDataIdentifier = [sama arvo kuin taulukon 29 tavuilla 6 ja 7]	xxxx	RDI_...
#m+8	Tarkistussumma	00-FF	CS

Taulukko 31

WriteDataByIdentifier-palvelupyynnön annettavan kieltävän vastauksen sisältävä viesti

Tavun nro	Parametri	Arvo (Hex)	Muistikas
#1	Muototavu – fyysinen osoittaminen	80	FMT
#2	Kohteen osoitetavu	tt	TGT
#3	Lähteen osoitetavu	EE	SRC
#4	Pituutta osoittava lisätavu	03	LEN
#5	Palvelupyynnön annettavan kieltävän vastauksen tunniste	7F	NR
#6	WriteDataByIdentifier-palvelupyynnön tunniste	2E	WBDI
#7	ResponseCode = [requestOutOfRange incorrectMessageLength conditionsNotCorrect]	31 13 22	RC_ROOR RC_IML RC_CNC
#8	Tarkistussumma	00-FF	CS

6.2.3 Parametrien määrittely

Parametri recordDataIdentifier (RDI_) on määritelty taulukossa 28.

WriteDataByIdentifier-palvelupyynnön annettavan myöntävän vastauksen sisältävässä viestissä käytetään dataRecord (DREC_) -parametria hakemaan recordDataIdentifier-tunnisteen mukaisten tietueiden arvot palvelimelle (ajoneuvoyksikölle). Dataformaattit määritellään kohdassa 8.

7. TESTIPULSSIEN OHJAUS – TULO-/LÄHTÖSIGNAALIEN OHJAUKSEN TOIMINTAYKSIKKÖ

Käytettävissä olevat palvelut on esitetty seuraavassa taulukossa:

Taulukko 32

tulo-/lähtösignaalien ohjauksen toimintayksikkö

Palvelu	Kuvaus
InputOutputControlByIdentifier	Asiakas pyytää saada ohjata palvelinkohtaista tulo-/lähtösignaalia

7.1 InputOutputControlByIdentifier-palvelu**7.1.1 Viestin kuvaus**

Laitteen etukannessa olevan liittimen johtimen kautta voidaan testipulsseja ohjata tai seurata tarkoitukseen sopivan testauslaitteen avulla.

CPR_058 Tämän kalibroinnin tulo-/lähtösignaalijohtimen asetukset voidaan määrittellä InputOutputControlByIdentifier-palvelun avulla annetulla K-johdinta koskevalla komennolla, jolloin johtimelle otetaan käyttöön valittu tulo- tai lähtösignaalitoiminto. Johtimen tilat ovat:

- ei käytössä,
- speedSignalInput, jossa kalibroinnin tulo-/lähtösignaalijohdinta käytetään syötettäessä nopeussignaalia (testisignaalia), joka korvaa liikeanturin nopeussignaalin,
- realTimeSpeedSignalOutputSensor, jossa kalibroinnin tulo-/lähtösignaalijohdinta käytetään tulostettaessa liikeanturin nopeussignaalia,
- RTCOutput, jossa kalibroinnin tulo-/lähtösignaalijohdinta käytetään tulostettaessa UTC-kellosignaalia.

CPR_059 Ajoneuvoyksiköllä on oltava käynnissä säätöjakso ja sen tulee olla CALIBRATION-toimintatilassa, jotta johtimen tilaa koskeva asetus voidaan määrittää. Säätöjakson tai CALIBRATION-toimintatilan päättyessä ajoneuvoyksikön on varmistettava, että kalibroinnin tulo-/lähtösignaalijohdin palautetaan 'ei käytössä' -tilaan (oletusarvoinen tila).

CPR_060 Jos ajoneuvoyksikön liikepulsseja tosiasjassa vastaanottavaan tulojohtimeen saapuu liikepulsseja, kun kalibroinnin tulo-/lähtösignaalijohdin on asetettu vastaanottamaan pulsseja, on kalibroinnin tulo-/lähtösignaalijohdin asetettava lähetystilaan tai palautettava ei käytössä -tilaan.

CPR_061 Kommentisarjaan on kuuluttava seuraavat toimet:

- luodaan viestintäyhteys StartCommunication-palvelun avulla,
- siirrytään säätöjaksoon StartDiagnosticSession-palvelun avulla ja asetetaan laite CALIBRATION-toimintatilaan (nämä kaksi tointa voidaan suorittaa kummassa järjestyksessä hyvänsä)
- vaihdetaan lähtösignaalitila tulosignaalitylaksi InputOutputControlByIdentifier-palvelun avulla.

7.1.2 Viestin muoto

CPR_062 InputOutputControlByIdentifier-perusalkioiden viestien muodot on esitetty seuraavassa taulukossa.

Taulukko 33

InputOutputControlByIdentifier-palvelupyynnön sisältävä viesti

Tavun nro	Parametri	Arvo (Hex)	Muistikas
#1	Muototavu – fyysinen osoittaminen	80	FMT
#2	Kohteen osoitetavu	EE	TGT
#3	Lähteen osoitetavu	tt	SRC
#4	Pituutta osoittava lisätavu	xx	LEN
#5	inputOutputControlByIdentifier-palvelupyynnön tunniste	2F	IOCBI
#6–#7	InputOutputIdentifier = [CalibrationInputOutput]	F960	IOI_CIO
#8 tai #8–#9	ControlOptionRecord = [inputOutputControlParameter – arvo taulukosta 36 controlState – arvo taulukosta 37 (ks. huomautus)]	xx xx	COR_... IOCP_... CS_...
#9 tai #10	Tarkistussumma	00-FF	CS

Huomautus: controlState-parametria käytetään vain tietyissä tapauksissa (ks. 7.1.3).

Taulukko 34

InputOutputControlByIdentifier-palvelupyntöön annettavan myöntävän vastauksen sisältävä viesti

Tavun nro	Parametri	Arvo (Hex)	Muistikas
#1	Muototavu – fyysinen osoittaminen	80	FMT
#2	Kohteen osoitetavu	tt	TGT
#3	Lähteen osoitetavu	EE	SRC
#4	Pituutta osoittava lisätavu	xx	LEN
#5	inputOutputControlByIdentifier-palvelupyntöön annettavan myöntävän vastauksen tunniste	6F	IOCBIPR
#6 to #7	inputOutputIdentifier = [CalibrationInputOutput]	F960	IOI_CIO
#7 to #8	controlStatus = [inputOutputControlParameter (sama arvo kuin tavulla 8, taulukko 33) controlState (sama arvo kuin tavulla 9, taulukko 33)] (tarvittaessa)	xx xx	CSR_ IOCP_ CS_...
#9 or #10	Tarkistussumma	00-FF	CS

Taulukko 35

InputOutputControlByIdentifier-palvelupyntöön annettavan kieltävän vastauksen sisältävä viesti

Tavun nro	Parametri	Arvo (Hex)	Muistikas
#1	Muototavu – fyysinen osoittaminen	80	FMT
#2	Kohteen osoitetavu	tt	TGT
#3	Lähteen osoitetavu	EE	SRC
#4	Pituutta osoittava lisätavu	03	LEN
#5	Palvelupyntöön annettavan kieltävän vastauksen tunniste	7F	NR
#6	inputOutputControlByIdentifier-palvelupyntöön tunniste	2F	IOCBI
#7	responseCode = [incorrectMessageLength conditionsNotCorrect requestOutOfRange deviceControlLimitsExceeded]	13 22 31 7A	RC_IML RC_CNC RC_ROOR RC_DCLE
#8	Tarkistussumma	00-FF	CS

7.1.3 Parametrien määrittely

CPR_064 inputOutputControlParameter (IOCP_) -parametri on määritelty seuraavassa taulukossa.

Taulukko 36

inputOutputControlParameter-parametrin arvojen määritelmät

Hex	Kuvaus	Muistikas
00	ReturnControlToECU Tämä arvo osoittaa palvelimelle (ajoneuvoyksikkö), että testauslaite ei enää ohjaa kalibroinnin tulo-/lähtösignaalijohdinta.	RCTECU
01	ResetToDefault Tämä arvo osoittaa palvelimelle (ajoneuvoyksikölle), että sitä pyydetään asettamaan kalibroinnin tulo-/lähtösignaalijohdin oletusarvoiseen tilaansa.	RTD
03	ShortTermAdjustment Tämä arvo osoittaa palvelimelle (ajoneuvoyksikölle), että sitä pyydetään asettamaan kalibroinnin tulo-/lähtösignaalijohdin controlState-parametrin sisältämän arvon mukaiseksi.	STA

CPR_065 ControlState-parametria käytetään vain, kun inputOutputControlParameter-parametri on asetettu arvoon ShortTermAdjustment, ja se on määritelty seuraavassa taulukossa:

Taulukko 37

controlState-parametrin arvojen määritelmät

Tila	Arvo (Hex)	Kuvaus
Ei käytössä	00	Tulo-/lähtösignaalijohdin ei käytössä (oletusarvo)
Käytössä	01	Kalibroinnin tulo-/lähtösignaalijohdin käytössä tilassa speedSignalInput
Käytössä	02	Kalibroinnin tulo-/lähtösignaalijohdin käytössä tilassa realTimeSpeedSignalOutputSensor
Käytössä	03	Kalibroinnin tulo-/lähtösignaalijohdin käytössä tilassa RTCOutput

8. DATATIETUEIDEN MUOTO

Tämä kohta sisältää:

- yleissäännöt, joita on sovellettava ajoneuvoyksikön testauslaitteelle lähetettäviin parametriervoihin,
- formaatit, joita kohdassa 6. kuvattujen tiedonsiirtopalvelujen kautta siirretyn datan on noudatettava.

CPR_067 Ajoneuvoyksikön on tuettava kaikkia yksilöityjä parametrejä.

CPR_068 Ajoneuvoyksikön testauslaitteelle vastauksena pyyntöön lähetettävän datan on oltava mitattua tyyppiä (eli vastattava ajoneuvoyksikön mittaamaa tai toteamaan pyydetyn parametrin arvoa).

8.1 Lähetettävät parametriervot

CPR_069 Taulukossa 38 – dataRecords-parametrien arvoalueet määritellään alueet, joiden perusteella lähetetyn parametrin kelpoisuus määritellään.

CPR_070 Alueella 'error indicator' olevien arvojen avulla ajoneuvoyksikkö voi heti ilmoittaa, että oikeaa parametritietoja ei kyseisellä hetkellä ole saatavissa tallennuslaitteen virheen vuoksi.

CPR_071 Alueella 'not available' olevien arvojen avulla ajoneuvoyksikkö voi lähettää viestin, joka sisältää sellaisen parametrin, jota ei ole saatavilla tai jota ei tueta kyseisessä laitteessa. Alueella 'not requested' olevien arvojen avulla laite voi lähettää kommentiviestin ja osoittaa ne parametrit, joihin ei odoteta vastausta vastaanottavalta laitteelta.

CPR_072 Jos komponenttinvirhe estää parametriä koskevan oikean tiedon lähettämisen, parametrin tiedon sijasta olisi käytettävä virhekoodia taulukossa 38 kuvatulla tavalla. Jos mitattu tai laskettu data on kuitenkin tuottanut arvon, joka on periaatteessa kelvollinen, mutta asetetun arvoalueen ulkopuolella, virhekoodia ei tulisi käyttää. Data olisi lähetettävä käyttäen parametrin asianmukaista vähimmäis- tai enimmäisarvoa.

Taulukko 38

dataRecords-parametrien arvoalueet

Alueen nimi	1 tavu Arvo (Hex)	2 tavua Arvo (Hex)	4 tavua Arvo (Hex)	ASCII
Kelvollinen signaali	00-FA	0000-FAFF	00000000-FAFFFFFF	1-254
Parametrikohtainen osoitin	FB	FB00-FBFF	FB000000-FBFFFFFF	ei ole
Tuleville osoitinbiteille varattu alue	FC-FD	FC00-FDFF	FC000000-FDFFFFFF	ei ole
Virhekoodi	FE	FE00-FEFF	FE000000-FEFFFFFF	0
Ei saatavilla tai ei pyydetty	FF	FF00-FFFF	FF000000-FFFFFF	FF

CPR_073 ASCII-koodattujen parametrien erottimeksi varataan ASCII-merkki '*'.

8.2 Datatietueiden muoto

Alla taulukoissa 39-42 kuvataan muodot, joita on käytettävä ReadDataByIdentifier- ja WriteDataByIdentifier- palveluissa.

CPR_074 Taulukossa 39 ilmoitetaan recordDataIdentifier-tunnisteen ilmoittamien parametrien pituus, tarkkuus ja käyttöalue.

Taulukko 39

Datatietueiden muoto

Parametri	Datan pituus (tavua)	Tarkkuus	Käyttöalue
TimeDate	8	Ks. tiedot taulukossa 40	
HighResolutionTotalVehicleDistance	4	5 m/bit, lähtöarvo 0 m	0- + 21 055 406 km
Kfactor	2	0,001 pulssia/m /bit, lähtöarvo 0	0-64 255 pulssia/m
LfactorTyreCircumference	2	0,125 10 ⁻³ m/bit, lähtöarvo 0	0-8 031 m
WvehicleCharacteristicFactor	2	0,001 pulssia/m /bit, lähtöarvo 0	0-64,255 pulssia/m
TyreSize	15	ASCII	ASCII
NextCalibrationDate	3	Ks. tiedot taulukossa 41	
SpeedAuthorised	2	1/256 km/h/bit, lähtöarvo 0	0-250 996 km/h
RegisteringMemberState	3	ASCII	ASCII
VehicleRegistrationNumber	14	Ks. tiedot taulukossa 42	
VIN	17	ASCII	ASCII

CPR_075 Taulukossa 40 kuvataan TimeDate-parametrin tavujen muoto:

Taulukko 40

TimeDate-parametrin muoto (recordDataIdentifier-parametri arvo F00B)

Tavu	Parametrien määrittely	Tarkkuus	Käyttöalue
1	sekunnit	0,25 s/bit, lähtöarvo 0 s	0–59,75 s
2	minuutit	1 min/bit, lähtöarvo 0 min	0–59 min
3	tunnit	1 h/bit, lähtöarvo 0 h	0–23 h
4	kuukausi	1 kk/bit, lähtöarvo 0 kk	1–12 kuukautta
5	päivä	0,25 päivää/bit, lähtöarvo 0 päivää (ks. huomautus, taulukko 41)	0,25–31,75 päivää
6	vuosi	1 vuosi/bit, lähtöarvo vuosi 1985 (ks. huomautus, taulukko 41)	1985–2235 vuosi
7	paikallinen minuutti-poikkeama	1 min/bit, – 125 min	– 59– 59 min
8	paikallinen tunti-poikkeama	1 h/bit, – 125 h	– 23– + 23 h

CPR_076 Taulukossa 41 kuvataan NextCalibrationDate-parametrin tavujen muoto:

Taulukko 41

NextCalibrationDate-parametrin muoto (recordDataIdentifier-parametrin arvo F022)

Tavu	Parametrien määrittely	Tarkkuus	Käyttöalue
1	kuukausi	1 kk/bit, lähtöarvo 0 kk	1–12 kuukautta
2	päivä	0,25 päivää/bit, lähtöarvo 0 päivää (ks. huomautus)	0,25–31,75 päivää
3	vuosi	1 vuosi/bit, lähtöarvo vuosi 1985 (ks. huomautus)	1985–2235 (vuosi)

Huomautus päiväparametrin käytöstä:

- 0 päivämäärän arvona merkitsee tyhjää. Arvoja 1, 2, 3 ja 4 käytetään ilmaisemaan kuukauden ensimmäistä päivää, arvoja 5, 6, 7 ja 8 ilmaisemaan kuukauden toista päivää jne.
- Tämä parametri ei vaikuta tuntiparametriin.

Huomautus vuosiparametrin käytöstä:

0 vuoden arvona merkitsee vuotta 1985, arvo 1 merkitsee vuotta 1986 jne.

CPR_078 Taulukossa 42 kuvataan VehicleRegistrationNumber-parametrin tavujen muoto:

Taulukko 42

VehicleRegistrationNumber-parametrin muoto (recordDataIdentifier-parametrin arvo F07E)

Tavu	Parametrien määrittely	Tarkkuus	Käyttöalue
1	Koodisto (Code Page, lisäyksen 1 mukaisesti)	ASCII	01–0A
2–14	Ajoneuvon rekisterinumero (lisäyksen 1 mukaisesti)	ASCII	ASCII

Lisäys 9

TYYPPIHYVÄKSYNTÄ — LUETTELO VÄHIMMISTÄ VAADITTAVISTA TESTEISTÄ

SISÄLLYSLUETTELO

1.	Johdanto	191
1.1	Tyypiphyväksyntä	191
1.2	Viitetiedot	191
2.	Ajoneuvoyksikön toiminnalliset testit	192
3.	Liiketunnistimen toiminnalliset testit	195
4.	Ajopiirturikorttien toiminnalliset testit	197
5.	Yhteentoimivuustestit	198

1. JOHDANTO

1.1 Tyyppihyväksyntä

Valvontalaitteen (tai sen osan) ETY-tyyppihyväksyntä perustuu seuraaviin sertifiointeihin:

- tietoturvasertifiointi, jonka tekee ITSEC-valtuutettu (Information Technology Security Evaluation Criteria, EU:n komission suositus yleisistä tietotekniikan turvallisuuden arviointiperusteista) viranomaisen käyttäen vertailukohtana tietoturvatavoitetta, joka on täysin tämän liitteen lisäyksen 10 mukainen,
- toiminnallinen sertifiointi, jonka tekee jäsenvaltion viranomaisen antamalla todistuksen siitä, että koestettu laite täyttää tämän lisäyksen vaatimukset, jotka koskevat suoritettuja toimintoja, mittaustarkkuutta ja ympäristönsuojeluun liittyviä ominaisuuksia,
- yhteentoimivuuden sertifiointi, jonka tekee toimivaltainen elin antamalla todistuksen siitä, että valvontalaite (tai ajo-ajopiirturikortti) on täysin yhteentoimiva vaadittavien ajo-ajopiirturikorttimallien (tai valvontalaitemallien) kanssa (ks. tämän lisäyksen VIII luku).

Tässä lisäyksessä määritellään ne testit, jotka jäsenvaltion viranomaisen on vähintään tehtävä toiminnallisuutta koestettaessa, ja testit, jotka toimivaltaisen elimen on vähintään suoritettava yhteentoimivuutta koestettaessa. Testejä tehtäessä käytettäviä menettelyjä ei ole määritelty tätä yksityiskohtaisemmin.

Tässä lisäyksessä ei käsitellä tietoturvasertifiointiin liittyviä asioita. Jos jotkut tyyppihyväksyntää varten tarvittavat testit tehdään tietoturva-arvioinnin ja -sertifioinnin yhteydessä, niitä ei tarvitse tehdä uudelleen. Tässä tapauksessa riittää, että tarkastetaan kyseisten tietoturvatestien tulokset. Yleisenä ohjeena voidaan sanoa, että ne vaatimukset, joiden täyttämistä voidaan olettaa testattavan (tai jotka läheisesti liittyvät testeihin, jotka voidaan olettaa tehtäväksi) tietoturvatestien yhteydessä, on tässä liitteessä merkitty tähdellä (*).

Tässä lisäyksessä käsitellään liiketunnistimen ja ajoneuvoyksikön tyyppihyväksyntää erikseen valvontalaitteen osina. Kaikkien liiketunnistimien ja kaikkien ajoneuvoyksikkömallien välistä yhteentoimivuutta ei vaadita, joten liiketunnistimen tyyppihyväksyntä voidaan myöntää vain ajoneuvoyksikön tyyppihyväksynnän kanssa ja päinvastoin.

1.2 Viitetiedot

Tässä lisäyksessä käytetään seuraavia viitteitä:

- | | |
|---------------|--|
| IEC 68-2-1 | Environmental testing – Part 2: Tests – Tests A: Cold. 1990 + Amendment 2: 1994. (Ympäristötestaus. Osa 2: Testit. Testit A: Kylmätestit. 1990, toinen muutos: 1994) |
| IEC 68-2-2 | Environmental testing – Part 2: Tests – Tests B: Dry heat. 1974 + Amendment 2: 1994. (Ympäristötestaus. Osa 2: Testit. Testit B: Testit kuivassa lämmössä. 1974, toinen muutos: 1994) |
| IEC 68-2-6 | Basic environmental testing procedures – Test methods – Test Fc and guidance: Vibration (sinusoidal). 6 edition: 1985. (Ympäristötestauksen perusmenetelmät. Testimenetelmät. Testi Fc ohjeineen: Tärinä (sinimuotoinen). Kuudes painos: 1985) |
| IEC 68-2-14 | Basic environmental testing procedures – Test methods – Test N: Change of temperature. Modification 1: 1986. (Ympäristötestauksen perusmenetelmät. Testimenetelmät. Testi N: Lämpötilamuutokset. Ensimmäinen muutos: 1986) |
| IEC 68-2-27 | Basic environmental testing procedures – Test methods – Test Ea and guidance: Shock. Edition 3: 1987. (Ympäristötestauksen perusmenetelmät. Testimenetelmät. Testi Ea ohjeineen: Iskut. Kolmas painos: 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. (Ympäristötestauksen perusmenetelmät. Testimenetelmät. Testi Db ohjeineen: Testit kosteassa lämmössä toistettavien jaksoin (jakso 12 + 12 tuntia). Ensimmäinen muutos: 1985) |
| IEC 68-2-35 | Basic environmental testing procedure – Test methods – Test Fda: Random vibration wide band – Reproducibility High. Modification 1: 1983. (Ympäristötestauksen perusmenetelmät. Testimenetelmät. Testi Fda : Laajakaistainen satunnaisesti muuttuva tärinä. Hyvä toistettavuus. Ensimmäinen muutos: 1983) |
| IEC 529 | Degrees of protection provided by enclosures (IP code). Edition 2: 1989. (Koteloinnin suojausluokat (IP-luokat). Toinen painos: 1989) |
| IEC 61000-4-2 | Electromagnetic Compatibility (EMC) – Testing and measurement techniques – Electrostatic discharge immunity test: 1995 / Amendment 1: 1998 (Sähkömagneettinen yhteensopivuus (EMC). Testaus- ja mittausten menetelmät. Staattisen sähkön purkauksien sietotesti. 1995, ensimmäinen lisäys: 1998) |
| ISO 7637-1 | 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. (Tieliikenteessä käytettävät ajoneuvot. Johtumisesta ja kytkemisestä aiheutuvat sähköiset häiriöt. Osa 1: Henkilöautot ja ammattimaisessa liikenteessä käytettävät kevyet ajoneuvot, joissa on 12 V:n jännite. Jännitepiikkien johtuminen pelkästään virtajohtoja myöden. Toinen painos: 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. (Tieliikenteessä käytettävät ajoneuvot. Johtumisesta ja kytkemisestä aiheutuvat sähköiset häiriöt. Osa 2: Ammattimaisessa liikenteessä käytettävät ajoneuvot, joissa on 24 V:n jännite. Jännitepiikkien johtuminen pelkästään virtajohtoja myöden. Ensimmäinen painos: 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. (Tieliikenteessä käytettävät ajoneuvot. Johtumisesta ja kytkemisestä aiheutuvat sähköiset häiriöt. Osa 3: Ajoneuvot, joissa on 12 tai 24 V:n jännite. Jännitepiikkien kapasitiivinen ja induktiivinen johtuminen muilla tavoin kuin virtajohtoja myöden. Ensimmäinen painos: 1995, ensimmäinen korjaus: 1995)
- ISO/IEC 7816-1 Identification cards – Integrated circuit(s) cards with contacts – Part 1: Physical characteristics. First edition: 1998. (Henkilökortit. Integroidulla piirillä varustetut kontaktilliset kortit. Osa 1: Fysiset ominaisuudet. Ensimmäinen painos: 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. (Tietotekniikka. Henkilökortit. Integroidulla piirillä varustetut kontaktilliset kortit. Osa 2: Mitat ja liittimien paikat. Ensimmäinen painos: 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. (Tietotekniikka. Henkilökortit. Integroidulla piirillä varustetut kontaktilliset kortit. Osa 3: Sähköiset signaalit ja siirtoprotokollat. Toinen painos: 1997)
- ISO/IEC 10373 Identification cards – Test methods. First edition: 1993. (Henkilökortit. Testausmenetelmät. Ensimmäinen painos: 1993)

2. AJONEUVOYKSIKÖN TOIMINNALLISET TESTIT

Nro	Testi	Selite	Vaatimukset, joihin testi liittyy
1.	Hallinnollinen tarkastus		
1.1	Kirjallinen aineisto	Kirjallisen aineiston oikeellisuus	
1.2	Valmistajan testitulokset	Valmistajan kokoonpanovaiheessa suorittaman testin tulokset. Kirjalliset todisteet	070, 071, 073
2.	Silmämääräinen tarkastus		
2.1	Yhtäpitävyys kirjallisen aineiston kanssa		
2.2	Tunniste/merkinnät		168, 169
2.3	Materiaalit		163–167
2.4	Sinetöinti		251
2.5	Ulkoiset liitäntälaitteet		
3.	Toiminnalliset testit		
3.1	Laitteessa mukana olevat toiminnot		
3.2	Toimintatilat		006*, 007*, 008*, 009*, 106, 107
3.3	Toiminnot ja tietojen käyttöoikeudet		010*, 011*, 240, 246, 247
3.4	Korttien paikoilleen asettamisen ja poistamisen seuranta		013, 014, 015*, 016*, 106
3.5	Nopeuden ja matkan mittaus		017–026
3.6	Ajanmittaus (testi tehdään 20 °C:n lämpötilassa)		027–032
3.7	Kuljettajan toiminnan seuranta		033–043, 106
3.8	Ajoneuvon miehityksen seuranta		044, 045, 106
3.9	Tietojen syöttö käsin		046–050b
3.10	Yritysten tekemien lukitusten hallinta		051–055
3.11	Tarkastustoimien seuranta		056, 057
3.12	Tapausten ja/tai vikojen havaitseminen		059–069, 106

Nro	Testi	Selite	Vaatimukset, joihin testi liittyy
3.13	Laitteen tunnistetiedot		075*, 076*, 079
3.14	Kuljettajakortin paikoilleen asettamiseen ja poistamisen liittyvät tiedot		081*–083*
3.15	Kuljettajan toimintaan liittyvät tiedot		084*–086*
3.16	Paikkoihin liittyvät tiedot		087*–089*
3.17	Matkamittariin liittyvät tiedot		090*–092*
3.18	Nopeuteen liittyvät yksityiskohtaiset tiedot		093*
3.19	Tapauksiin liittyvät tiedot		094*, 095
3.20	Vikoihin liittyvät tiedot		096*
3.21	Kalibrointiin liittyvät tiedot		097*, 098*
3.22	Ajan asetukseen liittyvät tiedot		100*, 101*
3.23	Tarkastustoimiin liittyvät tiedot		102*, 103*
3.24	Yritysten tekemiin lukituksiin liittyvät tiedot		104*
3.25	Tietojen kopiointitapahtumiin liittyvät tiedot		105*
3.26	Erytisolosuhteisiin liittyvät tiedot		105a*, 105b*
3.27	Tietojen tallennus ja säilytys ajopiirturikorteilla		108, 109*, 109a*, 110*, 111, 112
3.28	Tietojen näyttö		072, 106, 113–128, PIC_001, DIS_001
3.29	Tulostus		072, 106, 129–138, PIC_001, PRT_001 – PRT_012
3.30	Varoitukset		106, 139–148, PIC_001
3.31	Tietojen kopiointi ulkoiselle tietovälineelle		072, 106, 149–151
3.32	Tietojen tulostus ulkoisille lisälaitteille		152, 153
3.33	Kalibrointi		154*, 155*, 156*, 245
3.34	Ajan asetukset		157*, 158*
3.35	Lisätoimintojen aiheuttamat häiriöt		003, 269

Nro	Testi	Selite	Vaatimukset, joihin testi liittyy
4.	Ympäristötestit		
4.1	Lämpötila	<p>Todennetaan laitteen toiminta seuraavissa oloissa:</p> <ul style="list-style-type: none"> — standardin IEC 68-2-1 testi Ad, testin kesto 72 tuntia alhaisimmassa lämpötilassa (– 20 °C), laite toiminnassa 1 tunnin ajan, ei toiminnassa 1 tunnin ajan, — standardin IEC 68-2-2 testi Bd, testin kesto 72 tuntia korkeimmassa lämpötilassa (+ 70 °C), laite toiminnassa 1 tunnin ajan, ei toiminnassa 1 tunnin ajan <p>Toistuvat lämpötilan vaihtelut: todennetaan, että ajoneuvoyksikkö sietää nopeita ulkoisen lämpötilan vaihteluja tekemällä standardin IEC 68-2-14 mukainen testi Na, 20 lämpötilan vaihtelujaksoa, joista jokaisessa lämpötila vaihtuu alhaisimmasta lämpötilasta (– 20 °C) korkeimpaan lämpötilaan (+ 70 °C) ja pysyy kaksi tuntia sekä alhaisimmassa että korkeimmassa lämpötilassa</p> <p>Alimmassa ja korkeimmassa lämpötilassa sekä lämpötilan muutosjaksojen aikana voidaan tehdä rajoitettu testisarja (joka sisältää tämän taulukon osassa 3 olevia testejä)</p>	159
4.2	Kosteus	<p>Todennetaan, että ajoneuvoyksikkö sietää jaksoittaista kosteutta (lämpötesti) tekemällä standardin IEC 68-2-30 mukainen testi Db, kuusi 24 tunnin jaksoa, joista jokaisessa lämpötila vaihtelee välillä + 25 °C – + 55 °C ja suhteellinen kosteus on 97 % lämpötilassa + 25 °C ja 93 % lämpötilassa + 55 °C</p>	160
4.3	Tärinä	<p>1. Sinimuotoinen tärinä:</p> <p>Todennetaan, että ajoneuvoyksikkö sietää sinimuotoista tärinää, jolla on seuraavat ominaisuudet:</p> <p>vakioamplitudi taajuusalueella 5–11 Hz: 10 mm huipusta huippuun mitattuna</p> <p>vakiokiihtyvyys taajuusalueella 11–300 Hz: 5 g</p> <p>Tämän vaatimuksen täyttäminen todennetaan tekemällä standardin IEC 68-2-6 mukainen testi Fc vähimmäiskestoltaan 3 x 12 tuntia (12 tuntia kutakin akselia kohden)</p> <p>2. Satunnaisesti muuttuva tärinä:</p> <p>Todennetaan, että ajoneuvoyksikkö sietää satunnaisesti muuttuvaa tärinää, jolla on seuraavat ominaisuudet:</p> <p>taajuus 5–150 Hz, taso 0,02 g²/Hz.</p> <p>Tämän vaatimuksen täyttäminen todennetaan tekemällä standardin IEC 68-2-35 mukainen testi Ffd vähimmäiskestoltaan 3 x 12 tuntia (12 tuntia kutakin akselia kohden), laite toiminnassa 1 tunnin ajan, ei toiminnassa 1 tunnin ajan</p> <p>Edellä kuvatut kaksi testiä tehdään kahdelle eri näytteelle, jotka edustavat testattavaa laitetyyppiä</p>	163
4.4	Suojaus vettä ja vieraita esineitä vastaan	<p>Todennetaan, että ajoneuvoyksikön standardin IEC 529 mukainen suojausluokka on vähintään IP 40, kun laite on asennettu ajoneuvoon käyttöolosuhteisiinsa</p>	164, 165
4.5	Ylijännitesuojaus	<p>Todennetaan, että ajoneuvoyksikkö sietää seuraavia käyttöjännitteitä:</p> <p>24 V:n mallit: 34 V lämpötilassa + 40 °C 1 tunnin ajan</p> <p>12 V:n mallit: 17 V lämpötilassa + 40 °C 1 tunnin ajan</p>	161
4.6	Suojaus väärää napaisuutta vastaan	<p>Todennetaan, että ajoneuvoyksikkö sietää virtalähteen napojen vaihtamisen toisin päin</p>	161

Nro	Testi	Selite	Vaatimukset, joihin testi liittyy
4.7	Oikosulku suojaus	Todennetaan, että laitteen tulo- ja lähtösignaalit on suojattu oikosululta käyttöjännitettä ja maata vastaan	161
5.	Sähkömagneettisen yhteensopivuuden (EMC) testaus		
5.1	Laitteen tuottama säteily ja magneettinen vastaanottavuus	Laitteen on täytettävä direktiivin 95/54/ETY vaatimukset	162
5.2	Staatista sähköpurkaukset	Laitteen on täytettävä standardin IEC 61000-4-2, ± 2 kV (taso 1) vaatimukset	162
5.3	Virtajohtimia pitkin tulevien jännitepiikkien sietokyky	<p>24 V:n mallit: laitteen on täytettävä standardin ISO 7637-2 vaatimukset:</p> <p>pulssi 1a: $V_s = -100$ V, $R_i = 10$ ohmia</p> <p>pulssi 2: $V_s = +100$ V, $R_i = 10$ ohmia</p> <p>pulssi 3a: $V_s = -100$ V, $R_i = 50$ ohmia</p> <p>pulssi 3b: $V_s = +100$ V, $R_i = 50$ ohmia</p> <p>pulssi 4: $V_s = -16$ V, $V_a = -12$ V, $t_6 = 100$ ms</p> <p>pulssi 5: $V_s = +120$ V, $R_i = 2,2$ ohmia, $t_d = 250$ ms</p> <p>12 V:n mallit: laitteen on täytettävä standardin ISO 7637-1 vaatimukset:</p> <p>pulssi 1: $V_s = -100$ V, $R_i = 10$ ohmia</p> <p>pulssi 2: $V_s = +100$ V, $R_i = 10$ ohmia</p> <p>pulssi 3a: $V_s = -100$ V, $R_i = 50$ ohmia</p> <p>pulssi 3b: $V_s = +100$ V, $R_i = 50$ ohmia</p> <p>pulssi 4: $V_s = -6$ V, $V_a = -5$ V, $t_6 = 15$ ms</p> <p>pulssi 5: $V_s = +65$ V, $R_i = 3$ ohmia, $t_d = 100$ ms</p> <p>Pulssin 5 sietokyky testataan vain ajoneuvoyksiköillä, jotka on tarkoitettu asennettavaksi ajoneuvoihin, joissa ei ole erillistä suojausta sähköisen kuormituksen äkillisen katkeamisen varalta</p>	162

3. LIIKETUNNISTIMEN TOIMINNALLISET TESTIT

Nro	Testi	Selite	Vaatimukset, joihin testi liittyy
1.	Hallinnollinen tarkastus		
1.1	Kirjallinen aineisto	Kirjallisen aineiston oikeellisuus	
2.	Silmämääräinen tarkastus		
2.1	Yhtäpitävyys kirjallisen aineiston kanssa		
2.2	Tunniste/merkinnät		169, 170
2.3	Materiaalit		163–167
2.4	Sinetöinti		251
3.	Toiminnalliset testit		
3.1	Liiketunnistimen tunnistetiedot		077*
3.2	Liiketunnistimen liittäminen ajoneuvoyksikköön		099*, 155
3.3	Liikkeen havaitseminen		
	Liikkeen mittaustarkkuus		022–026

Nro	Testi	Selite	Vaatimukset, joihin testi liittyy
4.	Ympäristötestit		
4.1	Käyttölämpötila	Todennetaan toiminnallisuus (niin kuin se on määritelty testin 3.3 kohdalla) lämpötila-alueella $[- 40\text{ °C} - + 135\text{ °C}]$ tekemällä: — standardin IEC 68-2-1 mukainen testi Ad kestoltaan 96 tuntia alimmassa lämpötilassa T_{min} — standardin IEC 68-2-2 mukainen testi Bd kestoltaan 96 tuntia ylimmässä lämpötilassa T_{max}	159
4.2	Lämpötilan jaksoittainen vaihtelu	Todennetaan toiminnallisuus (niin kuin se on määritelty testin 3.3 kohdalla) tekemällä standardin IEC 68-2-14 mukainen testi Na, 20 lämpötilan vaihtelujaksoa, joista jokaisessa lämpötila vaihtuu alhaisimmasta lämpötilasta ($- 40\text{ °C}$) korkeimpaan lämpötilaan ($+ 135\text{ °C}$) ja pysyy kaksi tuntia sekä alhaisimmassa että korkeimmassa lämpötilassa Alimmassa ja korkeimmassa lämpötilassa sekä lämpötilan muutosjaksojen aikana voidaan tehdä rajoitettu testisarja (joka sisältää kohdassa 3.3 määriteltyjä testejä)	159
4.3	Kosteuden jaksoittainen vaihtelu	Todennetaan toiminnallisuus (niin kuin se on määritelty testin 3.3 kohdalla) tekemällä standardin IEC 68-2-30 mukainen testi Db, kuusi 24 tunnin jaksoa, joista jokaisessa lämpötila vaihtelee välillä $+ 25\text{ °C} - + 55\text{ °C}$ ja suhteellinen kosteus on 97 % lämpötilassa $+ 25\text{ °C}$ ja 93 % lämpötilassa $+ 55\text{ °C}$	160
4.4	Tärinä	Todennetaan toiminnallisuus (niin kuin se on määritelty testin 3.3 kohdalla) tekemällä standardin IEC 68-2-6 mukainen testi Fc siten, että se sisältää 100 taajuuden muutosjaksoa: vakioamplitudi taajuusalueella 10–57 Hz: 1,5 mm huipusta huippuun mitattuna vakiokiikkyvyys taajuusalueella 57–500 Hz: 20 g	163
4.5	Iskut	Todennetaan toiminnallisuus (niin kuin se on määritelty testin 3.3 kohdalla) tekemällä standardin IEC 68-2-27 mukainen testi Ea antamalla 3 iskua molempiin suuntiin kunkin kolmen kohtisuoran akselin suunnassa	163
4.6	Suojaus vettä ja vieraita esineitä vastaan	Todennetaan, että liiketunnistimen standardin IEC 529 mukainen suojausluokka on vähintään IP 64, kun laite on asennettu ajoneuvoon käyttöolosuhteisiinsa	165
4.7	Suojaus vääriä napaisuutta vastaan	Todennetaan, että liiketunnistin sietää virtalähteen napojen vaihtamisen toisin päin	161
4.8	Oikosulkusuojaus	Todennetaan, että tulo- ja lähtösignaalit on suojattu oikosuulta käyttäjännitettä ja maata vastaan	161
5.	Sähkömagneettisen yhteensopivuuden (EMC) testaus		
5.1	Laitteen tuottama säteily ja magneettinen vastaanottavuus	Laitteen on täytettävä direktiivin 95/54/ETY vaatimukset	162
5.2	Staattisen sähkön purkaukset	Laitteen on täytettävä standardin IEC 61000-4-2, $\pm 2\text{ kV}$ (taso 1) vaatimukset	162
5.3	Datakaapeleita pitkin tulevien jännitepiikkien sietokyky	Laitteen on täytettävä standardin ISO7637-3 (taso III) vaatimukset	162

4. AJOPIIRTURIKORTTIEN TOIMINNALLISET TESTIT

Nro	Testi	Selite	Vaatumukset, joihin testi liittyy
1.	Hallinnollinen tarkastus		
1.1	Kirjallinen aineisto	Kirjallisen aineiston oikeellisuus	
2.	Silmämääräinen tarkastus		
2.1		Varmistetaan, että turvakuviointi ja näkyviksi tarkoitetut tiedot on painettu korttiin oikein ja vaatimusten mukaisesti	171-181
3.	Fyysiset testit		
3.1	Tarkastetaan kortin mitat ja koskettimien sijainti		184 ISO/IEC 7816-1 ISO/IEC 7816-2
4.	Tiedonsiirtoprotokolliin liittyvät testit		
4.1	ATR-signaali	Tarkastetaan, että ATR-signaali on vaatimusten mukainen	ISO/IEC 7816-3 TCS 304, 307, 308
4.2	T=0	Tarkastetaan, että T=0-protokolla on vaatimusten mukainen	ISO/IEC 7816-3 TCS 302, 303, 305
4.3	PTS-komento	Tarkastetaan, että PTS-komento on vaatimusten mukainen, vaihtamalla käytössä oleva protokolla T=0:sta T=1:ksi	ISO/IEC 7816-3 TCS 309-311
4.4	T=1	Tarkastetaan, että T=1-protokolla on vaatimusten mukainen	ISO/IEC 7816-3 TCS 303, / 306
5.	Kortin tiedostorakenne		
5.1		Testataan, että kortin tiedostorakenne on vaatimusten mukainen, tarkastamalla, että kortilla on vaadittavat tiedostot ja että niiden käyttöehdot ovat asianmukaiset	TCS 312 TCS 400*, 401, 402, 403*, 404, 405*, 406, 407, 408*, 409, 410*, 411, 412, 413*, 414, 415*, 416, 417, 418*, 419
6.	Toiminnalliset testit		
6.1	Normaali tietojenkäsittely	Testataan jokaisen komennon jokainen sallittu käyttötapa vähintään kertaalleen (esim. testataan UPDATE BINARY -komento luokkaa osoittavan CLA-tavun arvolla 00h ja arvolla 0Ch sekä käyttäen eri arvoja parametreissa P1, P2 ja Lc). Tarkastetaan, että komennon mukaiset toiminnot on todella suoritettu kortilla (esim. lukemalla sen tiedoston tiedot, jota komento koski)	TCS 313 to TCS 379
6.2	Virheilmoitukset	Testataan jokainen (lisäyksessä 2 määritelty) virheilmoitus vähintään kerran jokaisessa komennossa. Testataan jokainen yleinen virhe vähintään kerran (paitsi datan eheyteen liittyvät virheet, joiden vastauskoodi on '6400' ja jotka tarkastetaan tietoturvasertifioinnin yhteydessä)	
7.	Ympäristötestit		
7.1		Varmistetaan, että kortit toimivat standardin ISO/IEC 10373 mukaisesti määritellyissä olosuhteissa	185-188 ISO/IEC 7816-1

5. YHTEENTOIMIVUUSTESTIT

Nro	Testi	Selite
1.	Molemminpuolinen varmentaminen	Tarkastetaan, että ajoneuvoyksikön ja ajopiirturikortin välinen molemminpuolinen varmentaminen sujuu normaalisti
2.	Tietojen kirjoittamisen ja lukemisen testaus	Suoritetaan tyypillinen käyttötilannetta vastaava toiminto ajoneuvoyksikössä. Toiminto on valittava testattavan kortin tyyppin mukaan, ja sen on kirjoitettava tietoja mahdollisimman moneen kortilla olevaan EF-tiedostoon Todennetaan kopioimalla kortin tiedot, että kaikki asianmukaiset tallenteet on tehty oikein Todennetaan tulostamalla päivittäinen tuloste, että kaikki asianmukaiset tallenteet ovat luettavissa

Lisäys 10

YLEISET TIETOTURVATAVOITTEET

Tässä lisäyksessä määritellään liiketunnistimen, ajoneuvoyksikön ja ajopiirturikortin tietoturvatavoitteiden vähimmäisvaatimukset.

Luodakseen tietoturvatavoitteet, joiden mukaan voidaan hakea turvavarmennusta, valmistajien on tarpeen mukaan hiottava ja täydennettävä asiakirjoja ilman, että niissä olevien uhkien, tavoitteiden, menettelytapojen ja tietoturvan toteuttamistoimintojen erittelyjen osalta lisätään mitään tai poistetaan mitään.

SISÄLLYSLUETTELO

Liiketunnistimen yleiset tietoturvatavoitteet

1.	Johdanto	204
2.	Lyhenteet, määritelmät ja viitetiedot	204
2.1	Lyhenteet	204
2.2	Määritelmät	204
2.3	Viitetiedot	204
3.	Perusteet	205
3.1	Liiketunnistimen kuvaus ja käyttötapa	205
3.2	Liiketunnistimen elinkaari	206
3.3	Uhat	206
3.3.1	Käyttöoikeuksiin liittyvät uhat	206
3.3.2	Suunnitteluun ja raketeeseen liittyvät uhat	207
3.3.3	Käyttöön liittyvät uhat	207
3.4	Tietoturvatavoitteet	207
3.5	Tietotekniikan tietoturvatavoitteet	207
3.6	Fyysiset, henkilöstön tai menetelmien vaikutustavat	208
3.6.1	Laitteen suunnittelu ja rakenne	208
3.6.2	Laitteen toimittaminen	208
3.6.3	Tietoturvadatan luonti ja toimittaminen	208
3.6.4	Valvontalaitteen asennus, kalibrointi ja tarkastus	208
3.6.5	Lainvalvontaan liittyvät tarkastukset	208
3.6.6	Ohjelmistopäivitykset	208
4.	Tietoturvan toteuttamistoiminnot	208
4.1	Tunnistaminen ja todentaminen	208
4.2	Käyttöoikeuksien valvonta	209
4.2.1	Käyttöoikeuksien valvonnan toimintalinjat	209
4.2.2	Tietojen käyttöoikeudet	209
4.2.3	Tiedostorakenteet ja käyttöehdot	209
4.3	Selvitysvelvollisuus	209

4.4	Seuranta	210
4.5	Tarkkuus	210
4.5.1	Tiedonkulun ohjauksen toimintalinjat	210
4.5.2	Sisäiset tiedonsiirrot	210
4.5.3	Tallennettujen tietojen eheys	210
4.6	Luotettavuus käytössä	210
4.6.1	Testit	210
4.6.2	Ohjelmistot	211
4.6.3	Fyysinen suojaus	211
4.6.4	Keskeytykset virransyötössä	211
4.6.5	Alkutilaan asettamisen olosuhteet	211
4.6.6	Tietojen käytettävyys	211
4.6.7	Lisäsovellukset	211
4.7	Tiedonvaihto	211
4.8	Salauksen tuki	211
5.	Turvamekanismien määrittely	212
6.	Turvamekanismien vähimmäisvahvuus	212
7.	Varmuustaso	212
8.	SEF-toimintojen ajatus	212

Ajoneuvoyksikön yleiset tietoturvatavoitteet

1.	Johdanto	214
2.	Lyhenteet, määritelmät ja viitetiedot	214
2.1	Lyhenteet	214
2.2	Määritelmät	214
2.3	Viitetiedot	214
3.	Perusteet	214
3.1	Ajoneuvoyksikön kuvaus ja käyttötapa	214
3.2	Ajoneuvoyksikön elinkaari	216
3.3	Uhat	216
3.3.1	Tunnistukseen ja käyttöoikeuksien valvonnan toimintalinjoihin liittyvät uhat	216
3.3.2	Suunnitteluun ja rakenteeseen liittyvät uhat	217
3.3.3	Käyttöön liittyvät uhat	217
3.4	Tietoturvatavoitteet	217
3.5	Tietotekniikan tietoturvatavoitteet	218
3.6	Fyysiset, henkilöstön tai menetelmien vaikutustavat	218
3.6.1	Laitteen suunnittelu ja rakenne	218
3.6.2	Laitteen toimittaminen ja aktivointi	218

3.6.3	Tietoturvadatan luonti ja toimittaminen	218
3.6.4	Korttien toimittaminen	219
3.6.5	Valvontalaitteen asennus, kalibrointi ja tarkastus	219
3.6.6	Laitteiden käyttö	219
3.6.7	Lainvalvontaan liittyvät tarkastukset	219
3.6.8	Ohjelmistopäivitykset	219
4.	Tietoturvan toteuttamistoiminnot	219
4.1	Tunnistaminen ja todentaminen	219
4.1.1	Liiketunnistimen tunnistaminen ja todentaminen	219
4.1.2	Käyttäjän tunnistaminen ja todentaminen	220
4.1.3	Etäyhteyttä käyttävän yrityksen tunnistaminen ja todentaminen	221
4.1.4	Hallintalaitteiden tunnistaminen ja todentaminen	221
4.2	Käyttöoikeuksien valvonta	221
4.2.1	Käyttöoikeuksien valvonnan toimintalinjat	221
4.2.2	Toimintojen käyttöoikeudet	221
4.2.3	Tietojen käyttöoikeudet	221
4.2.4	Tiedostorakenteet ja käyttöehdot	222
4.3	Selvitysvelvollisuus	222
4.4	Seuranta	222
4.5	Tietojen uudelleenkäyttö	223
4.6	Tarkkuus	223
4.6.1	Tiedonkulun ohjauksen toimintalinjat	223
4.6.2	Sisäiset tiedonsiirrot	223
4.6.3	Tallennettujen tietojen eheys	223
4.7	Luotettavuus käytössä	223
4.7.1	Testit	223
4.7.2	Ohjelmistot	224
4.7.3	Fyysinen suojaus	224
4.7.4	Kerskeytykset virransyötössä	224
4.7.5	Alkutilaan asettamisen olosuhteet	224
4.7.6	Tietojen käytettävyys	224
4.7.7	Lisäsovellukset	224
4.8	Tiedonvaihto	224
4.8.1	Tiedonvaihto liiketunnistimen kanssa	224
4.8.2	Tiedonvaihto ajopiirturikorttien kanssa	225
4.8.3	Tiedonvaihto ulkoisten tallennusvälineiden kanssa (tietojen kopiointitoiminto)	225
4.9	Salauksen tuki	225

5.	Turvamekanismien määrittely	225
6.	Turvamekanismien vähimmäisvahvuus	225
7.	Varmuustaso	225
8.	SEF-toimintojen ajatus	226

Ajopiirturikortin yleiset tietoturvatavoitteet

1.	Johdanto	230
2.	Lyhenteet, määritelmät ja viitetiedot	230
2.1	Lyhenteet	230
2.2	Määritelmät	231
2.3	Viitetiedot	231
3.	Perusteet	231
3.1	Ajopiirturikortin kuvaus ja käyttötapa	231
3.2	Ajopiirturikortin elinkaari	231
3.3	Uhat	232
3.3.1	Päämäärät	232
3.3.2	Hyökkäysreitit	232
3.4	Tietoturvatavoitteet	232
3.5	Tietotekniikan tietoturvatavoitteet	232
3.6	Fyysiset, henkilöstön tai menetelmien vaikutustavat	232
4.	Tietoturvan toteuttamistoiminnot	233
4.1	Yhdenmukaisuus suojausprofiilien kanssa	233
4.2	Käyttäjän tunnistaminen ja todentaminen	233
4.2.1	Käyttäjän tunnistaminen	233
4.2.2	Käyttäjän todentaminen	233
4.2.3	Epäonnistuneet todentamiset	233
4.3	Käyttöoikeuksien valvonta	234
4.3.1	Käyttöoikeuksien valvonnan toimintalinjat	234
4.3.2	Käyttöoikeuksien valvontatoiminnot	234
4.4	Selvitysvollisuus	234
4.5	Seuranta	234
4.6	Tarkkuus	234
4.6.1	Tallennettujen tietojen eheys	234
4.6.2	Perustietojen todentaminen	234
4.7	Luotettavuus käytössä	235
4.7.1	Testit	235
4.7.2	Ohjelmistot	235
4.7.3	Virtalähde	235

4.7.4	Alkutilaan asettamisen olosuhteet	235
4.8	Tiedonvaihto	235
4.8.1	Tiedonvaihto ajoneuvoyksikön kanssa	235
4.8.2	Tiedonsiirto muulle kuin ajoneuvoyksikölle (tietojen kopiointitoiminto)	235
4.9	Salauksen tuki	235
5.	Turvamekanismien määrittely	235
6.	Turvamekanismien vähimmäisvahvuus	236
7.	Varmuustaso	236
8.	SEF-toimintojen ajatus	236

LIIKETUNNISTIMEN YLEISET TIETOTURVATAVOITTEET

1. Johdanto

Tässä asiakirjassa kuvataan liiketunnistin, uhat, jotka sen on torjuttava, sekä tietoturvatavoitteet, jotka sen on täytettävä. Asiakirjassa määritellään vaadittavat tietoturvan toteuttamistoiminnot. Edelleen asiakirjassa määritellään tietoturvamekanismien oletettu vähimmäisvahvuus sekä kehityksen ja arvioinnin vaatima varmuustaso.

Tässä asiakirjassa viitataan vaatimuksiin, jotka on esitetty varsinaisessa liitteessä I B. On huomattava, että varsinaisen liitteen I B vaatimuksien ja tietoturvatavoitteiden vaatimuksien kohdalla saattaa esiintyä päällekkäisyyksiä. Mikäli suhde jonkin tietoturvatavoitteen vaatimuksen ja sen varsinaisen liitteen I B vaatimuksen, johon tämän tietoturvatavoitteen vaatimus viittaa, välillä on epäselvä, on varsinaisen liitteen I B vaatimus määräävä.

Sellaisiin varsinaisen liitteen I B vaatimuksiin, joihin ei viitata tietoturvatavoitteissa, ei kohdisteta tietoturvan toteuttamistoimintoja.

Uhille, tavoitteille, menettelytavoille ja tietoturvan toteuttamistoimintojen erittelyille on annettu yksilölliset nimet, jotta ne olisivat jäljitettävissä kehitys- ja arviointiasiakirjoissa.

2. Lyhenteet, määritelmät ja viitetiedot**2.1 Lyhenteet**

ROM (Read only memory) ROM-muisti; muisti, josta tietoja voidaan lukea, mutta johon ei voi kirjoittaa

SEF (Security enforcing function) SEF-toiminto; tietoturvan toteuttamistoiminto

TBD (To be defined) Määritellään erikseen (myöhemmin)

TOE (Target of evaluation) Arviointikohde

VU (Vehicle unit) Ajoneuvoyksikkö

2.2 Määritelmät

Digitaalinen ajopiirturi	Valvontalaite
Laitekokonaisuus	Liiketunnistimeen kytketty laite
Liikedata	Ajoneuvoyksikön kanssa vaihdettavat tiedot, jotka koskevat nopeutta ja kuljettavaa matkaa
Fyysisesti erilliset osat	Liiketunnistimen fyysiset osat, jotka on sijoitettu eri puolille ajoneuvoa, erotuksena liiketunnistimen kuoren sisällä olevista fyysisistä osista
Tietoturvadata	Tietyt tiedot, joita tarvitaan tukemaan tietoturvan toteuttamistoimintoja (esim. sala- kirjoitusavaimet)
Järjestelmä	Laitteet, ihmiset tai organisaatiot, jotka jollain tavoin liittyvät valvontalaitteeseen
Käyttäjä	Liiketunnistinta käyttävä henkilö (paitsi jos kyseessä on 'käyttäjätiedot')
Käyttäjätiedot	Kaikki muut kuin liikkeeseen ja tietoturvaan liittyvät liiketunnistimen tallentamat ja säilyttämät tiedot

2.3 Viitetiedot

ITSEC (Information Technology Security Evaluation Criteria) EU:n komission suositus yleisistä tietotekniikan turvallisuuden arviointiperusteista vuodelta 1991

3. Perusteet

3.1 Liiketunnistimen kuvaus ja käyttötapa

Liiketunnistin on tarkoitettu asennettavaksi tieliikenteessä käytettäviin kuljetusajoneuvoihin. Sen tarkoituksena on antaa ajoneuvoyksikölle turvattua liikedataa, joka kuvaa ajoneuvon nopeutta ja sen kulkemaa matkaa.

Liiketunnistin liitetään mekaanisesti ajoneuvon sellaiseen liikuvaan osaan, jonka liike osoittaa ajoneuvon nopeutta tai kuljettua matkaa. Se voidaan sijoittaa ajoneuvon vaihdelaatikkoon tai muuhun ajoneuvon osaan.

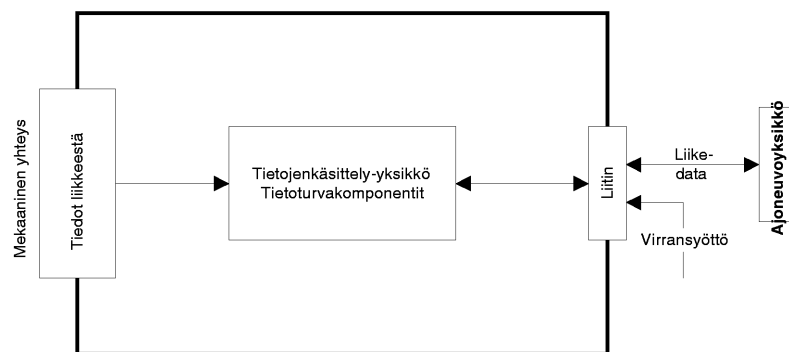
Käyttötilassaan liiketunnistin on oltava kytkettynä ajoneuvoyksikköön.

Se voidaan hallintatarkoituksessa myös kytkeä tiettyihin laitteisiin (*valmistajan määriteltävissä*).

Seuraavassa kuvassa on tyypillinen liiketunnistin:

Kuva 1

Tyypillinen liiketunnistin

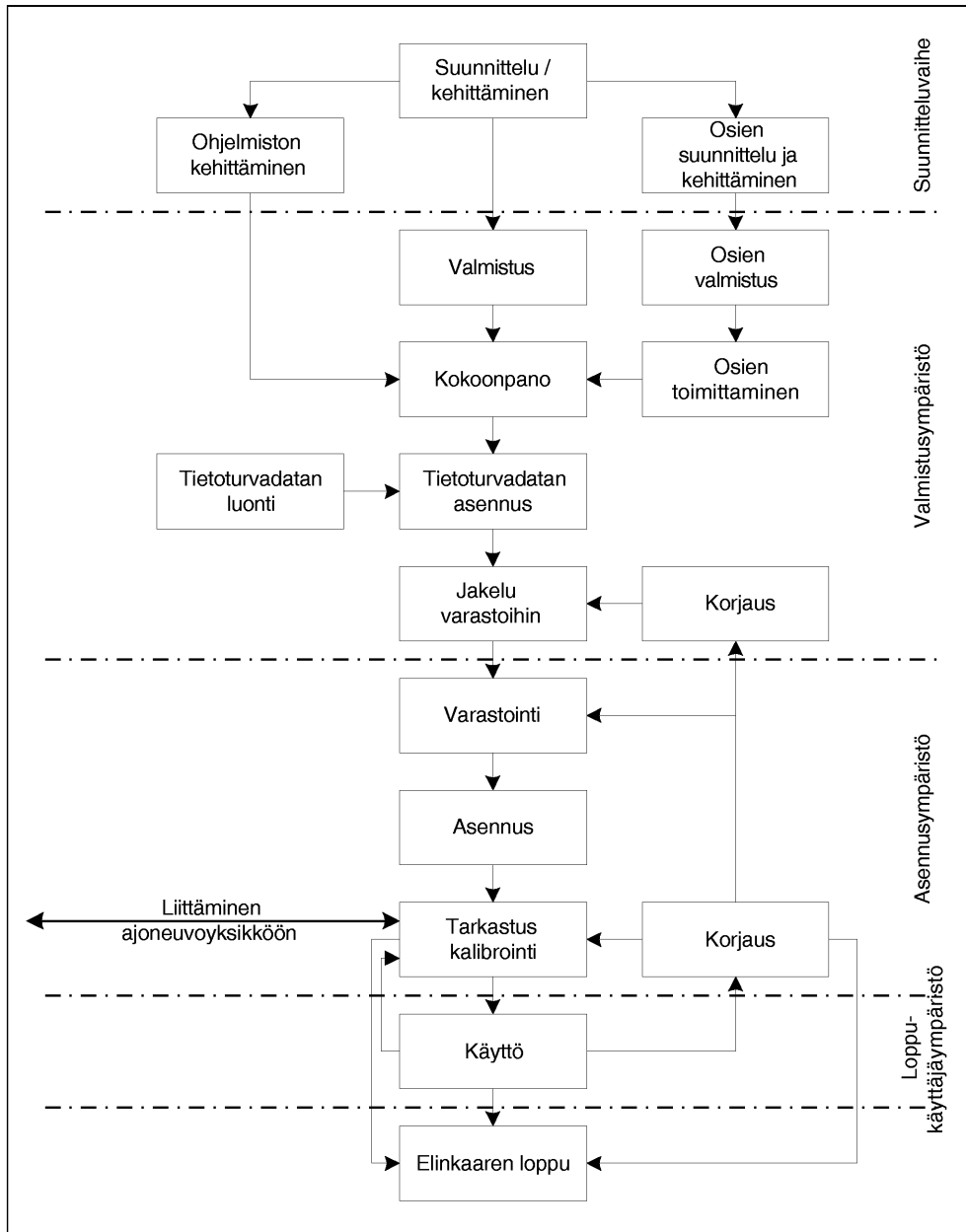


3.2 Liiketunnistimen elinkaari

Seuraavassa kuvassa on liiketunnistimen tyypillinen elinkaari:

Kuva 2

Liiketunnistimen tyypillinen elinkaari



3.3 Uhat

Tässä kohdassa kuvataan uhat, joiden kohteeksi liiketunnistin saattaa joutua.

3.3.1 Käyttöoikeuksiin liittyvät uhat

T.Access

Käyttäjät saattavat yrittää käyttää toimintoja, joihin heillä ei ole käyttöoikeuksia

3.3.2 Suunnitteluun ja rakenteeseen liittyvät uhat

T.Faults	Laitteiston, ohjelmiston tai viestintätapahtumien virheet saattavat asettaa liiketunnistimen vaikeasti ennakoitaviin olosuhteisiin, jotka vaarantavat sen tietoturvan
T.Tests	Käytöstä poistamatta jääneiden testaustoimintatilojen tai kiertoteiden käyttäminen saattaa vaarantaa liiketunnistimen tietoturvan
T.Design	Käyttäjät saattavat yrittää saada oikeudettomia tietoja laitteen rakenteesta joko valmistajan lähteistä (varkauden, lahjonnan tms. avulla) tai käänteissuunnittelun avulla

3.3.3 Käyttöön liittyvät uhat

T.Environment	Käyttäjät saattavat vaarantaa liiketunnistimen tietoturvan saattamalla laitteen alttiiksi ympäristön vaikutuksille (lämpövaikutukset, sähkömagneettiset, optiset, kemialliset, mekaaniset vaikutukset jne.)
T.Hardware	Käyttäjät saattavat yrittää tehdä muutoksia liiketunnistinlaitteisiin
T.Mechanical_Origin	Käyttäjät saattavat yrittää vaikuttaa liiketunnistimen tulosihtäviin (esim. irrottamalla tunnistimen vaihdelaatikosta jne.)
T.Motion_Data	Käyttäjät saattavat yrittää tehdä muutoksia ajoneuvon liiketietoihin (lisääminen, muuttaminen, poistaminen, signaalien toistaminen)
T.Power_Supply	Käyttäjät saattavat yrittää tehdä tyhjäksi liiketunnistimen tietoturvatavoitteet tekemällä muutoksia (katkaiseminen, alentaminen, lisääminen) sen virransyöttöön
T.Security_Data	Käyttäjät saattavat yrittää saada oikeudettomia tietoja tietoturvatavasta sitä luotaessa tai siirrettäessä tai laitteeseen asennettaessa
T.Software	Käyttäjät saattavat yrittää tehdä muutoksia liiketunnistimen ohjelmistoon
T.Stored_Data	Käyttäjät saattavat yrittää tehdä muutoksia tallennettuihin tietoihin (tietoturvatavataan tai käyttäjätietoihin)

3.4 Tietoturvatavoitteet

Digitaalisen ajopiirturijärjestelmän tärkein tietoturvatavoite on seuraava:

O.Main	Valvontaviranomaisten tarkastettavaksi tarkoitettujen tietojen on oltava käytettävissä ja niiden on täysin ja tarkasti kuvattava tarkastuksen kohteena olevia kuljettajia ja ajoneuvoja koskevat tapahtumat, jotka liittyvät ajo-, työ-, varallaolo- ja lepoaikoihin sekä ajoneuvon nopeuteen
--------	---

Järjestelmän kokonaistietoturvatavoitteeseen vaikuttava liiketunnistimen tietoturvatavoite on sen vuoksi seuraava:

O.Sensor_Main	Liiketunnistimen lähettämän datan on oltava ajoneuvoyksikön käytettävissä, jotta ajoneuvoyksikkö voi täysin ja tarkasti määrittää ajoneuvon nopeuden ja sen kulkeman matkan.
---------------	--

3.5 Tietotekniikan tietoturvatavoitteet

Liiketunnistimen tietotekniikkaan liittyvät tietoturvatavoitteet, jotka vaikuttavat sen tietoturvan päätavoitteeseen, ovat seuraavat:

O.Access	Liiketunnistimen on ohjattava siihen kytkettyjen laitekokonaisuuksien oikeuksia käyttäen toimintoja ja tietoja
O.Audit	Liiketunnistimen on seurattava yrityksiä murtaa sen tietoturva ja jäljitettävä yritykset niihin liittyviin laitekokonaisuuksiin
O.Authentication	Liiketunnistimen on todennettava siihen kytketyt laitekokonaisuudet

O.Processing	Liiketunnistimen on varmistettava, että tulosignaalin käsittely liikedatan saamiseksi on virheetöntä
O.Reliability	Liiketunnistimen on toimittava luotettavasti
O.Secured_Data_Exchange	Liiketunnistimen on suojattava tiedonvaihto ajoneuvoyksikön kanssa

3.6 *Fyysiset, henkilöstön tai menetelmien vaikutustavat*

Tässä kohdassa kuvataan fyysisiä, henkilöstöä ja menetelmiä koskevia vaatimuksia, jotka vaikuttavat liiketunnistimen tietoturvaan.

3.6.1 *Laitteen suunnittelu ja rakenne*

M.Development	Liiketunnistimien kehittäjien on varmistettava, että kehitystyön aikainen vastuunjako ei vaaranna tietotekniikkaan liittyvää tietoturvaa
M.Manufacturing	Liiketunnistimien valmistajien on varmistettava, että valmistuksen aikainen vastuunjako ei vaaranna tietotekniikkaan liittyvää tietoturvaa ja että liiketunnistin on valmistuksen aikana suojattu sellaisia fyysisiä toimenpiteitä vastaan, jotka saattaisivat vaarantaa tietotekniikkaan liittyvän tietoturvan

3.6.2 *Laitteen toimittaminen*

M.Delivery	Liiketunnistimien valmistajien, ajoneuvovalmistajien ja asentajien on varmistettava, että liiketunnistinta käsitellään tavalla, joka ei vaaranna tietotekniikkaan liittyvää tietoturvaa
------------	---

3.6.3 *Tietoturvadatan luonti ja toimittaminen*

M.Sec_Data_Generation	Tietoturvadatan luomisessa käytettävien algoritmien on oltava ainoastaan valtuutettujen ja luotettavien henkilöiden käytettävissä
M.Sec_Data_Transport	Tietoturvadata on luotava, siirrettävä ja asennettava liiketunnistimeen tavalla, joka säilyttää sen asianmukaisen luottamuksellisuuden ja eheyden

3.6.4 *Valvontalaitteen asennus, kalibrointi ja tarkastus*

M.Approved_Workshops	Valvontalaitteen asennuksen, kalibroinnin ja tarkastuksen saavat suorittaa vain luotettavat ja hyväksytyt asentajat tai korjaamot
M.Mechanical_Interface	Laitteessa on oltava varustus, joka paljastaa mekaanisen liitännän epäasianmukaisen käsittelyn (esim. sinetit)
M.Regular_Inspections	Valvontalaite on tarkastettava ja kalibroitava säännöllisesti

3.6.5 *Lainvalvontaan liittyvät tarkastukset*

M.Controls	Lainvalvontaan liittyviä tarkastuksia on suoritettava säännöllisesti ja satunnaisesti, ja niihin on sisällyttävä tietoturvan seuranta
------------	---

3.6.6 *Ohjelmistopäivitykset*

M.Software_Upgrade	Uusille ohjelmistoversioille on saatava turvavarmennus, ennen kuin niitä voidaan käyttää liiketunnistimessa
--------------------	---

4. **Tietoturvan toteuttamistoiminnot**

4.1 **Tunnistaminen ja todentaminen**

UIA_101 Liiketunnistimen on jokaisen vuorovaikutuksen yhteydessä voitava tunnistaa se laitekokonaisuus, johon se on kytketty.

UIA_102 Tunnistimeen kytketyn laitekokonaisuuden on koostuttava seuraavista osista:

- laitekokonaisuusryhmä:
 - ajoneuvoyksikkö,
 - hallintalaite,
 - muu laite,
- laitekokonaisuuden tunniste (koskee vain ajoneuvoyksikköä).

UIA_103 Tunnistimeen kytketyn ajoneuvoyksikön laitekokonaisuuden tunniste on sisällettävä ajoneuvoyksikön hyväksyntänumero ja ajoneuvoyksikön sarjanumero.

UIA_104 Liiketunnistimen on kyettävä todentamaan kaikki ajoneuvoyksiköt tai hallintalaitteet, joihin se on kytketty, kun

- laitekokonaisuus kytketään,
- käyttöjännite virtakatkoksen jälkeen palautuu.

UIA_105 Liiketunnistimen on kyettävä tietyin väliajoin uudelleen todentamaan ajoneuvoyksikkö, johon se on kytketty.

UIA_106 Liiketunnistimen on havaittava kopioitu todennusdata, jota yritetään käyttää uudelleen, ja estettävä sen käyttö.

UIA_107 Kun on tehty tietty määrä (joka on valmistajan määriteltävissä, mutta ei saa olla enemmän kuin 20) perättäisiä epäonnistuneita todennusyrityksiä, SEF-toiminnon on

- luotava tapausta koskeva seurantatietue,
- varoitettava laitekokonaisuutta,
- jatkettava liikedatan lähettämistä ei-suojatussa tilassa.

4.2 Käyttöoikeuksien valvonta

Käyttöoikeuksien valvonnalla on varmistettava, että arviointikohteen tietoja lukevat, luovat tai muuttavat vain ne, joilla on siihen valtuudet.

4.2.1 Käyttöoikeuksien valvonnan toimintalinjat

ACC_101 Liiketunnistimen on valvottava toimintojen ja tietojen käyttöoikeuksia.

4.2.2 Tietojen käyttöoikeudet

ACC_102 Liiketunnistimen on varmistettava, että liiketunnistimen tunnistetiedot voidaan kirjoittaa vain kerran (vaatimus 078).

ACC_103 Liiketunnistimen on hyväksyttävä ja/tai tallennettava käyttäjätietoja vain todennetuilta laitekokonaisuuksilta.

ACC_104 Liiketunnistimen on valvottava tietoturvadatan lukemiseen ja kirjoittamiseen oikeuttavien käyttöoikeuksien noudattamista.

4.2.3 Tiedostorakenteet ja käyttöehdot

ACC_105 Sovellus- ja datatiedostojen rakenne ja käyttöehdot on luotava valmistuksen aikana ja lukittava siten, ettei niitä voida myöhemmin muuttaa tai poistaa.

4.3 Selvitysvelvollisuus

ACT_101 Liiketunnistimen on säilytettävä muistissaan liiketunnistimen tunnistetiedot (vaatimus 077).

ACT_102 Liiketunnistimen on säilytettävä muistissaan asennukseen liittyvät tiedot (vaatimus 099).

ACT_103 Liiketunnistimen on kyettävä tulostamaan selvitysvelvollisuuden nojalla annettavia tietoja (selvitystietoja) todennetuille laitekokonaisuuksille niiden pyynnöstä.

4.4 *Seuranta*

AUD_101 Liiketunnistimen on luotava sen tietoturvaa vaarantavista tapauksista niitä koskeva seurantatietue.

AUD_102 Seuraavat tapaukset vaarantavat liiketunnistimen tietoturvan:

- tietoturvan murtoyritykset:
 - todennuksen epäonnistuminen,
 - virhe tallennettujen tietojen eheydessä,
 - virhe sisäisessä tiedonsiirrossa,
 - laitteen kannen luvaton avaaminen,
 - laitteen tahallinen vahingoittaminen,
- vika liiketunnistimessa.

AUD_103 Seurantatietueiden on sisällettävä seuraavat tiedot:

- päivämäärä ja aika, jolloin tapaus sattui,
- tapaustyyppi,
- tunnistimeen kytketyn laitekokonaisuuden tunniste.

Kun vaadittavia tietoja ei ole käytettävissä, on annettava asianmukainen oletusarvoinen tieto (valmistajan määriteltävissä).

AUD_104 Liiketunnistimen on lähetettävä syntyneet seurantatietueet ajoneuvoyksikölle heti, kun ne on luotu. Tunnistin saa tallentaa ne myös omaan muistiinsa.

AUD_105 Jos liiketunnistin säilyttää seurantatietueita, sen on varmistettava, että säilytettynä on 20 seurantatietuetta riippumatta siitä, onko seurantatietueille varattu säilytystila riittävä, ja sen on kyettävä pyydettäessä tulostamaan säilytetyt seurantatietueet todennetuille laitekokonaisuuksille.

4.5 *Tarkkuus*

4.5.1 *Tiedonkulun ohjauksen toimintalinjat*

ACR_101 Liiketunnistimen on varmistettava, että liikedata on voitu saada vain käsittelemällä tunnistimen mekaaniseen tulosignaaliin perustuvia tietoja ja niistä johtamalla.

4.5.2 *Sisäiset tiedonsiirrot*

Tämän kohdan vaatimukset koskevat vain liiketunnistimia, joissa on fyysisesti erillisiä osia.

ACR_102 Jos tietoja siirretään liiketunnistimen fyysisesti erillisten osien välillä, tiedot on suojattava niiden muuttamista vastaan.

ACR_103 Jos havaitaan sisäisen tiedonsiirron aikana tapahtunut tiedonsiirtovirhe, siirto on uusittava ja SEF-toiminnon on luotava tapausta koskeva seurantatietue.

4.5.3 *Tallennettujen tietojen eheys*

ACR_104 Liiketunnistimen on tarkastettava, että sen muistiin tallennetut käyttäjätiedot ovat eheät.

ACR_105 Jos havaitaan virhe tallennettujen käyttäjätietojen eheydessä, SEF-toiminnon on luotava seurantatietue.

4.6 *Luotettavuus käytössä*

4.6.1 *Testit*

RLB_101 Kaikki pelkästään valmistusvaiheessa käytettävät komennot, toiminnot tai koestuspisteet on tehtävä toimintakyvyttö-
miksi tai poistettava ennen valmistusvaiheen päättymistä. Ne eivät saa olla myöhemmin palautettavissa käyttöön.

RLB_102 Liiketunnistimen on itse suoritettava testejä sitä ensi kertaa käynnistettäessä sekä normaalin käytön aikana sen virheettömyyden toiminnan todentamiseksi. Liiketunnistimen itse suorittamiin testeihin on sisällyttävä tietoturvadatan eheyden todentaminen sekä tallennettujen suoritettavien ohjelmakoodien eheyden todentaminen (ellei niitä ole tallennettu ROM-muistiin).

RLB_103 Jos laitteen itse suorittaman testin aikana havaitaan virhe, SEF-toiminnon on luotava seurantatietue (vika liiketunnistimessa).

4.6.2 Ohjelmistot

RLB_104 Liiketunnistimen ohjelmistojen käyttöolosuhteissa tapahtuvan analysoinnin tai korjailun on oltava mahdotonta.

RLB_105 Ulkopuolelta syötettyä dataa ei saa hyväksyä suoritettavaksi ohjelmakoodiksi.

4.6.3 Fyysinen suojaus

RLB_106 Jos liiketunnistimen rakenne mahdollistaa sen avaamisen, liiketunnistimen on havaittava kaikki sen kotelon avaamista-paukset myös ilman ulkoista virtalähdettä vähintään kuuden kuukauden ajan. Näissä tapauksissa SEF-toiminnon on luotava tapausta koskeva seurantatietue. (Riittää, että seurantatietue luodaan ja tallennetaan vasta, kun virta jälleen kytetään laitteeseen.)

Jos liiketunnistinta ei rakenteensa vuoksi ole mahdollista avata, sen rakenteen on oltava sellainen, että yritykset käsitellä sitä epäasianmukaisesti ovat helposti havaittavissa (esim. tarkastamalla silmämääräisesti).

RLB_107 Liiketunnistimen on havaittava laitteen tietyntyyppinen tahallinen vahingoittaminen (valmistajan määriteltävissä).

RLB_108 Edellä kuvatussa tapauksessa SEF-toiminnon on luotava seurantatietue ja liiketunnistimen on (valmistajan määriteltävissä).

4.6.4 Keskeytykset virransyötössä

RLB_109 Virransyötön keskeytyessä tai jännitteen vaihdella liiketunnistimen on siirryttävä suojattuun toimintatilaan.

4.6.5 Alkutilaan asettamisen olosuhteet

RLB_110 Jos virransyöttö keskeytyy tai jokin toimenpide keskeytyy ennen kuin se on saatettu loppuun tai muissa alkutilaan asettamista edellyttävissä olosuhteissa, liiketunnistimen on tultava asetetuksi alkutilaansa virheettömästi.

4.6.6 Tietojen käytettävyys

RLB_111 Liiketunnistimen on varmistettava, että tiedot ja toiminnot ovat tarvittaessa käytettävissä ja että tietoja ja toimintoja ei pyydetä tai niiden käyttöön antamisesta pidättäydytä tarpeettomasti.

4.6.7 Lisäsovellukset

RLB_112 Jos liiketunnistimessa on käytettävissä muita sovelluksia kuin ajopiirturisolvellus, kaikki sovellukset on pidettävä fyysisesti ja/tai loogisesti erillään toisistaan. Nämä sovellukset eivät saa käyttää tietoturvadataa. Kerrallaan saa käynnissä olla vain yksi toiminto.

4.7 Tiedonvaihto

DEX_101 Liiketunnistimen on lähetettävä ajoneuvoyksikölle liikedataa, joka on varustettu asianmukaisin tietoturvamäärittein, jotta ajoneuvoyksikkö voi todentaa sen eheyden ja aitouden.

4.8 Salauksen tuki

Tämän kohdan vaatimuksia sovelletaan vain tarvittaessa, käytettävien turvamekanismien ja valmistajan ratkaisujen mukaan.

CSP_101 Kaikkien liiketunnistimen suorittamien salaukseen liittyvien toimien on oltava määritellyn algoritmin mukaisia ja noudatettava määriteltyjä avaimen pituuksia.

CSP_102 Jos liiketunnistin luo salausavaimia, sen on tapahduttava määriteltyjen salausavaimien luontialgoritmien mukaisesti ja noudattamalla määriteltyjä salausavaimen pituuksia.

CSP_103 Jos liiketunnistin jakelee salausavaimia, sen on tapahduttava määriteltyjen avaimen jakelumenetelmien mukaisesti.

CSP_104 Jos liiketunnistin käyttää salausavaimia, sen on tapahduttava avaimen käyttämiseen määriteltyjen menetelmien mukaisesti.

CSP_105 Jos liiketunnistin tuhoaa salausavaimia, sen on tapahduttava määriteltyjen avaimen tuhoamisen menetelmien mukaisesti.

5. Turvamekanismien määrittely

Liiketunnistimien valmistajat määrittelevät turvamekanismit, jotka täyttävät tietoturvan toteuttamistoimintojen vaatimukset.

6. Turvamekanismien vähimmäisvahvuus

Liiketunnistimen turvamekanismien vähimmäisvahvuus on ITSEC-viiteaineiston mukainen High (korkea).

7. Varmuustaso

Liiketunnistimen tavoitevarmuustaso on ITSEC-viiteaineiston mukainen E3.

8. SEF-toimintojen ajatus

Seuraavissa taulukoissa esitetään SEF-toimintojen ajatus näyttämällä,

— millä SEF-toiminnoilla tai keinoilla kukin uhka torjutaan,

— mikä SEF-toiminto täyttää kunkin tietoturvatavoitteen.

	Uhat											Tietotekniikan tavoitteet						
	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
Tietoturvan toteuttamistoiminnot (SEF-toiminnot)																		
Tunnistaminen ja todentaminen																		
Uia_101 Laitekokonaisuuksien tunnistaminen	x							x					x		x			x
Uia_102 Laitekokonaisuuksien tunniste	x												x		x			
Uia_103 Ajoneuvoyksikön tunniste														x				
Uia_104 Laitekokonaisuuksien todentaminen	x						x						x		x			x
Uia_105 Uudelleentodentaminen	x						x						x		x			x
Uia_106 Todentaminen, jota ei voida väärentää	x						x						x		x			
Uia_107 Epäonnistunut todentaminen							x							x			x	
Käyttöoikeuksien valvonta																		
Acc_101 Käyttöoikeuksien valvonnan toimintalinjat	x								x			x	x					
Acc_102 Liiketunnistimen tunniste												x	x					

AJONEUVOYKSIKÖN YLEISET TIETOTURVATAVOITTEET

1. Johdanto

Tässä asiakirjassa kuvataan ajoneuvoyksikkö, uhat, jotka sen on torjuttava, sekä tietoturvatavoitteet, jotka sen on täytettävä. Asiakirjassa määritellään vaadittavat tietoturvan toteuttamistoiminnot. Edelleen asiakirjassa määritellään tietoturvamekanismien oletettu vähimmäisvahvuus sekä kehityksen ja arvioinnin vaatima varmuustaso.

Tässä asiakirjassa viitataan vaatimuksiin, jotka on esitetty varsinaisessa liitteessä I B. On huomattava, että varsinaisen liitteen I B vaatimuksien ja tietoturvatavoitteiden vaatimuksien kohdalla saattaa esiintyä päällekkäisyyksiä. Mikäli suhde jonkin tietoturvatavoitteen vaatimuksen ja sen varsinaisen liitteen I B vaatimuksen, johon tämän tietoturvatavoitteen vaatimus viittaa, välillä on epäselvä, on varsinaisen liitteen I B vaatimus määräävä.

Sellaisiin varsinaisen liitteen I B vaatimuksiin, joihin ei viitata tietoturvatavoitteissa, ei kohdisteta tietoturvan toteuttamistoimintoja.

Uhille, tavoitteille, menettelytavoille ja tietoturvan toteuttamistoimintojen erittelyille on annettu yksilölliset nimet, jotta ne olisivat jäljitettävissä kehitys- ja arviointiasiakirjoissa.

2. Lyhenteet, määritelmät ja viitetiedot**2.1 Lyhenteet**

PIN	(Personal identification number) PIN-koodi; henkilökohtainen tunnusluku
ROM	(Read only memory) ROM-muisti; muisti, josta tietoja voidaan lukea, mutta johon ei voi kirjoittaa
SEF	(Security enforcing function) SEF-toiminto; tietoturvan toteuttamistoiminto
TBD	(To be defined) Määritellään erikseen (myöhemmin)
TOE	(Target of evaluation) Arviointikohde
VU	(Vehicle unit) Ajoneuvoyksikkö

2.2 Määritelmät

Digitaalinen ajopiirturi	Valvontalaite
Liikedata	Liiketunnistimen kanssa vaihdettavat tiedot, jotka koskevat nopeutta ja kuljettavaa matkaa
Fyysisesti erilliset osat	Ajoneuvoyksikön fyysiset osat, jotka on sijoitettu eri puolille ajoneuvoa, erotuksena ajoneuvoyksikön kuoren sisällä olevista fyysisistä osista
Tietoturvatadata	Tietyt tiedot, joita tarvitaan tukemaan tietoturvan toteuttamistoimintoja (esim. salakirjoitusavaimet)
Järjestelmä	Laitteet, ihmiset tai organisaatiot, jotka jollain tavoin liittyvät valvontalaitteeseen
Käyttäjä	Käyttäjillä tarkoitetaan laitteita käyttäviä henkilöitä. Ajoneuvoyksikön normaaleihin käyttäjiin kuuluvat kuljettajat, korjaamot ja yritykset
Käyttäjätiedot	Kaikki muut kuin liikkeeseen ja tietoturvaan liittyvät ajoneuvoyksikön tallentamat ja säilyttämät tiedot, joita koskevat vaatimukset on esitetty luvun III kohdassa 12

2.3 Viitetiedot

ITSEC (Information Technology Security Evaluation Criteria) EY:n komission suositus yleisistä tietotekniikan turvallisuuden arviointiperusteista vuodelta 1991

3. Perusteet**3.1 Ajoneuvoyksikön kuvaus ja käyttötapa**

Ajoneuvoyksikkö on tarkoitettu asennettavaksi tieliikenteessä käytettäviin kuljetusajoneuvoihin. Sen tarkoituksena on kirjata, tallentaa, näyttää, tulostaa ja antaa tietoja, jotka liittyvät kuljettajan toimintaan.

Se kytketään liiketunnistimeen, jonka kanssa se vaihtaa ajoneuvon liikedataa.

Käyttäjät osoittavat henkilöllisyytensä ajoneuvoyksikölle ajopiirturikorttien avulla.

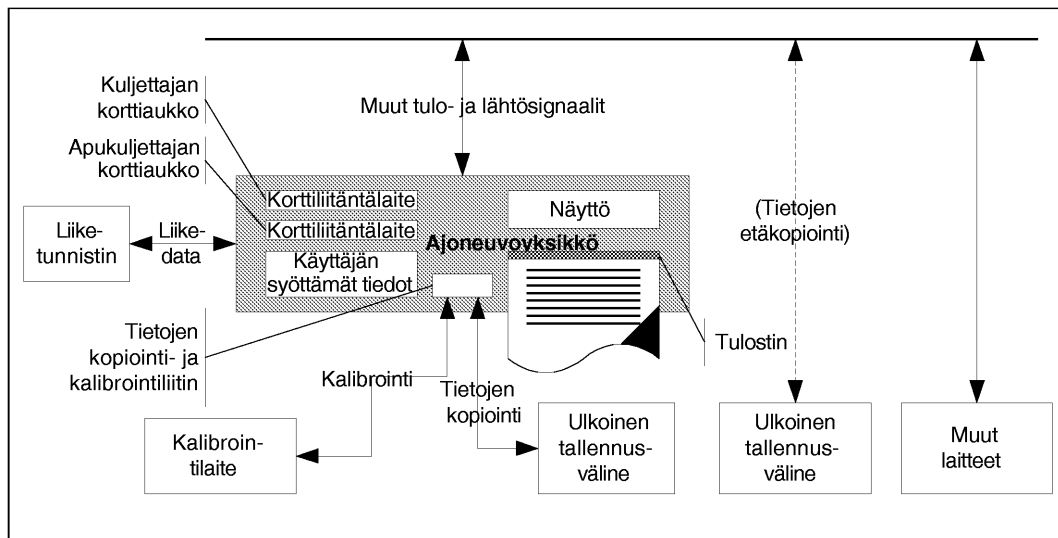
Ajoneuvoyksikkö kirjaa ja tallentaa kuljettajan toimintaan liittyviä tietoja datamuistiinsa sekä ajopiirturikortteille.

Ajoneuvoyksikkö tulostaa tietoja näytölle, tulostimelle ja ulkoisille laitteille.

Seuraavassa kuvassa on ajoneuvoon asennetun ajoneuvoyksikön käyttöympäristö:

Kuva 1

Ajoneuvoyksikön käyttöympäristö



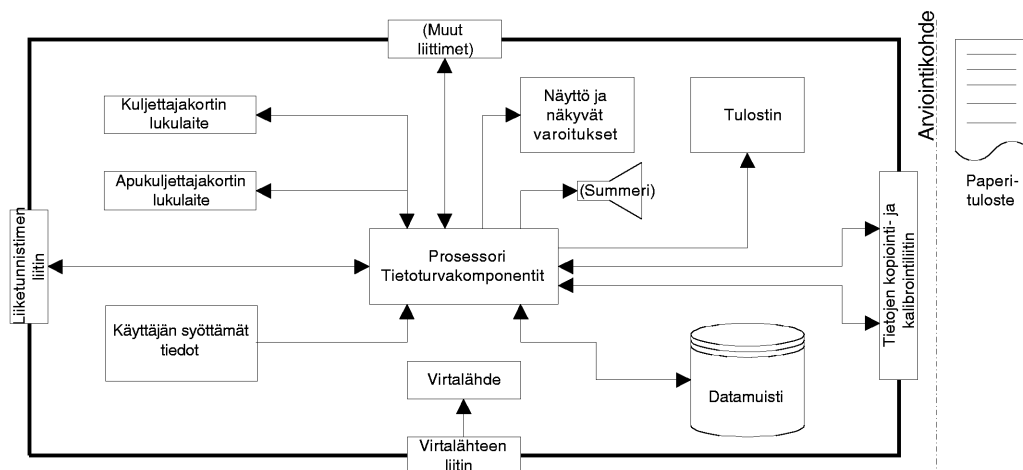
Ajoneuvoyksikön yleiset ominaisuudet, toiminnot ja toimintatilat on kuvattu liitteen I B luvussa II.

Ajoneuvoyksikön toiminnalliset vaatimukset on määritelty liitteen I B luvussa III.

Seuraavassa kuvassa on tyypillinen ajoneuvoyksikkö:

Kuva 2

Tyypillinen ajoneuvoyksikkö (...) valinnainen



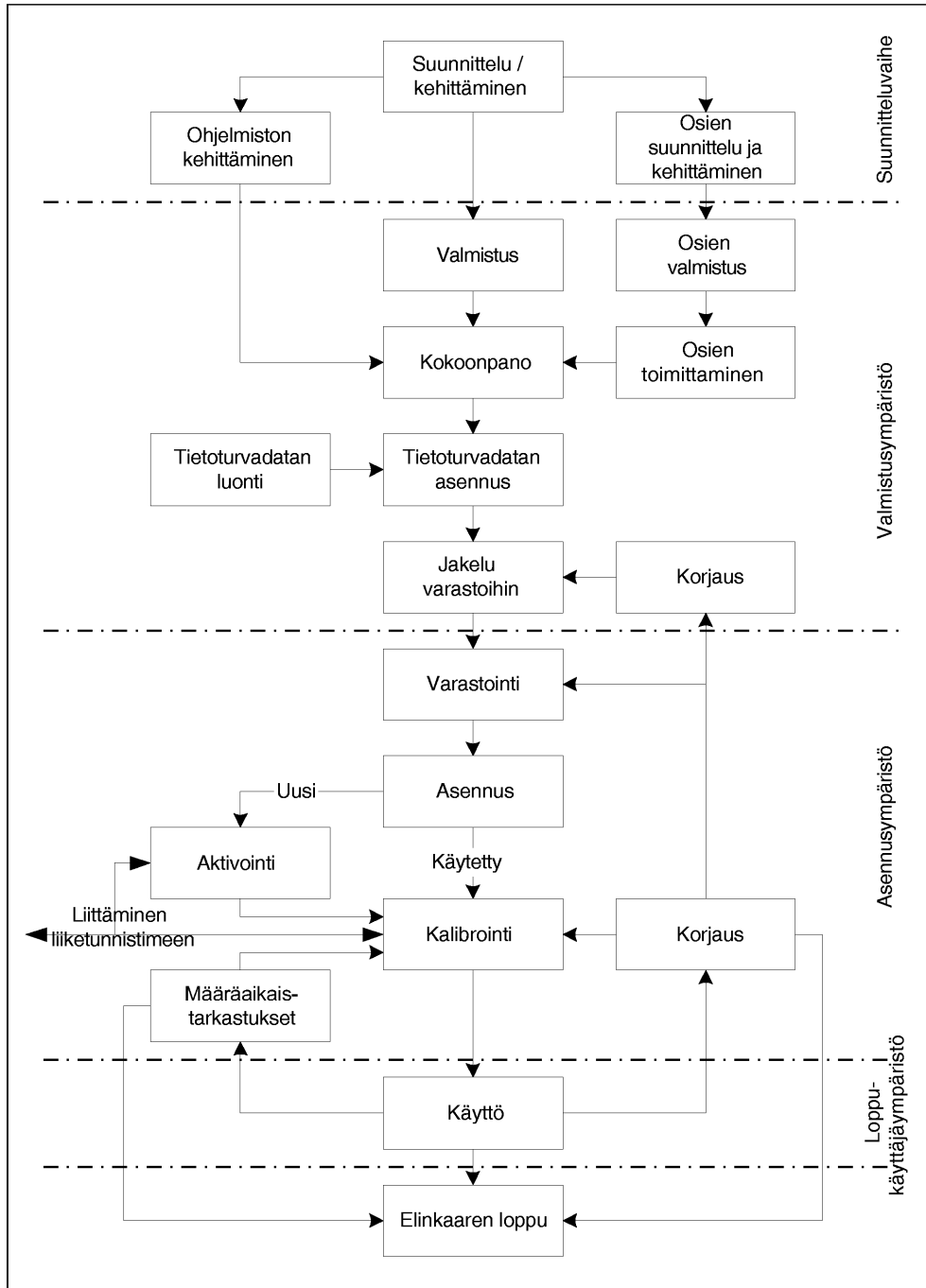
On huomattava, että vaikka tulostimen koneisto on osa arviointikohdetta, paperituloste ei ole.

3.2 Ajoneuvoyksikön elinkaari

Seuraavassa kuvassa on ajoneuvoyksikön tyypillinen elinkaari:

Kuva 3

Ajoneuvoyksikön tyypillinen elinkaari



3.3 Uhat

Tässä kohdassa kuvataan uhat, joiden kohteeksi ajoneuvoyksikkö saattaa joutua.

3.3.1 Tunnistukseen ja käyttöoikeuksien valvonnan toimintalinjoihin liittyvät uhat

T.Access

Käyttäjät saattavat yrittää käyttää toimintoja, joiden käyttämiseen heillä ei ole oikeutta (esim. kuljettajat käyttävät kalibrointitoimintoa)

T.Identification

Käyttäjät saattavat yrittää käyttää useita eri tunnisteita tai ei lainkaan tunnistetta

3.3.2 Suunnitteluun ja rakenteeseen liittyvät uhat

T.Faults	Laitteiston, ohjelmiston tai viestintätapahtumien virheet saattavat asettaa ajoneuvoyksikön vaikeasti ennakoitaviin olosuhteisiin, jotka vaarantavat sen tietoturvan
T.Tests	Käytöstä poistamatta jääneiden testaustoimintatilojen tai kiertoteiden käyttäminen saattaa vaarantaa ajoneuvoyksikön tietoturvan
T.Design	Käyttäjät saattavat yrittää saada oikeudettomia tietoja laitteen rakenteesta joko valmistajan lähteistä (varkauden, lahjonnan tms. avulla) tai käänteissuunnittelun avulla

3.3.3 Käyttöön liittyvät uhat

T.Calibration_Parameters	Käyttäjät saattavat yrittää käyttää väärin kalibroituja laitteita (muuttamalla kalibrointitietoja tai käyttämällä hyväksyen organisaation heikkouksia)
T.Card_Data_Exchange	Käyttäjät saattavat yrittää muuttaa tietoja, kun niitä vaihdetaan ajoneuvoyksikön ja ajopiirturikorttien välillä (tietojen lisääminen, muuttaminen, poistaminen, signaalin toistaminen)
T.Clock	Käyttäjät saattavat yrittää muuttaa sisäisen kellon asetuksia
T.Environment	Käyttäjät saattavat vaarantaa ajoneuvoyksikön tietoturvan saattamalla laitteen alttiiksi ympäristön vaikutuksille (lämpövaikutukset, sähkömagneettiset, optiset, kemialliset, mekaaniset vaikutukset jne.)
T.Fake_Devices	Käyttäjät saattavat yrittää kytkeä ajoneuvoyksikköön valelaitteita (liiketunnistin, älykortit)
T.Hardware	Käyttäjät saattavat yrittää tehdä muutoksia ajoneuvoyksikkölaitteisiin
T.Motion_Data	Käyttäjät saattavat yrittää tehdä muutoksia ajoneuvon liikedataan (lisääminen, muuttaminen, poistaminen, signaalin toistaminen)
T.Non_Activated	Käyttäjät saattavat käyttää laitetta, jota ei ole aktivoitu
T.Output_Data	Käyttäjät saattavat yrittää muuttaa tulostettavia tietoja (tulostamisen, näyttämisen tai kopioinnin yhteydessä)
T.Power_Supply	Käyttäjät saattavat yrittää tehdä tyhjiksi ajoneuvoyksikön tietoturvatavoitteet tekemällä muutoksia (katkaiseminen, alentaminen, lisääminen) sen virransyöttöön
T.Security_Data	Käyttäjät saattavat yrittää saada oikeudettomia tietoja tietoturvadatasta sitä luotaessa tai siirrettäessä tai laitteeseen asennettaessa
T.Software	Käyttäjät saattavat yrittää tehdä muutoksia ajoneuvoyksikön ohjelmistoon
T.Stored_Data	Käyttäjät saattavat yrittää tehdä muutoksia tallennettuihin tietoihin (tietoturvadataan tai käyttäjätietoihin)

3.4 Tietoturvatavoitteet

Digitaalisen ajopiirturijärjestelmän tärkein tietoturvatavoite on seuraava:

O.Main	Valvontaviranomaisten tarkastettavaksi tarkoitettujen tietojen on oltava käytettävissä ja niiden on täysin ja tarkasti kuvattava tarkastuksen kohteena olevia kuljettajia ja ajoneuvoja koskevat tapahtumat, jotka liittyvät ajo-, työ-, varallaolo- ja lepoaikoihin sekä ajoneuvon nopeuteen
--------	---

Järjestelmän kokonaistietoturvatavoitteeseen vaikuttavat ajoneuvoyksikön tietoturvatavoitteet ovat sen vuoksi seuraavat:

O.VU_Main	Mitattavaksi ja tallennettavaksi ja sen jälkeen viranomaisten tarkastettavaksi tarkoitettujen tietojen on oltava käytettävissä ja niiden on tarkasti kuvattava tarkastuksen kohteena olevien kuljettajien ja ajoneuvojen toimintaa, joka liittyy ajo-, työ-, varallaolo- ja lepoaikoihin sekä ajoneuvon nopeuteen
O.VU_Export	Ajoneuvoyksikön on kyettävä siirtämään tietoja ulkoiselle tallennusvälineelle siten, että niiden eheys ja aitous voidaan todentaa

3.5 Tietotekniikan tietoturvatavoitteet

Ajoneuvoyksikön tietotekniikkaan liittyvät tietoturvatavoitteet, jotka vaikuttavat sen tietoturvan päätavoitteisiin, ovat seuraavat:

O.Access	Ajoneuvoyksikön on ohjattava toimintojen ja tietojen käyttöoikeuksia
O.Accountability	Ajoneuvoyksikön on kerättävä tarkkoja selvitystietoja
O.Audit	Ajoneuvoyksikön on seurattava yrityksiä murtaa sen tietoturva ja jäljitettävä yritykset niihin liittyviin käyttäjiin.
O.Authentication	Ajoneuvoyksikön on todennettava käyttäjät ja siihen kytketyt laitekokonaisuudet (kun laitekokonaisuuksien välille tulee luoda turvallinen siirtotie (trusted path))
O.Integrity	Ajoneuvoyksikön on säilytettävä tallennettujen tietojen eheys
O.Output	Ajoneuvoyksikön on varmistettava, että lähetettävä data kuvaa tarkasti mitattuja tai tallennettuja tietoja
O.Processing	Ajoneuvoyksikön on varmistettava, että tulossignaalin käsittely käyttäjätietojen saamiseksi on virheetöntä
O.Reliability	Ajoneuvoyksikön on toimittava luotettavasti
O.Secured_Data_Exchange	Ajoneuvoyksikön on suojattava tiedonvaihto liiketunnistimen ja ajopiirturikorttien kanssa

3.6 Fyysiset, henkilöstön tai menetelmien vaikutustavat

Tässä kohdassa kuvataan fyysisiä, henkilöstöä ja menetelmiä koskevia vaatimuksia, jotka vaikuttavat ajoneuvoyksikön tietoturvaan.

3.6.1 Laitteen suunnittelu ja rakenne

M.Development	Ajoneuvoyksikköjen kehittäjien on varmistettava, että kehitystyön aikainen vastuunjako ei vaaranna tietotekniikkaan liittyvää tietoturvaa
M.Manufacturing	Ajoneuvoyksikköjen valmistajien on varmistettava, että valmistuksen aikainen vastuunjako ei vaaranna tietotekniikkaan liittyvää tietoturvaa ja että ajoneuvoyksikkö on valmistuksen aikana suojattu sellaisia fyysisiä toimenpiteitä vastaan, jotka saattaisivat vaarantaa tietotekniikkaan liittyvän tietoturvan

3.6.2 Laitteen toimittaminen ja aktivointi

M.Delivery	Ajoneuvoyksikköjen valmistajien, ajoneuvovalmistajien ja asentajien tai korjaamojen on varmistettava, että aktiivoimattomia ajoneuvoyksikköjä käsitellään tavalla, joka ei vaaranna ajoneuvoyksikköjen tietoturvaa
M.Activation	Ajoneuvovalmistajien ja asentajien tai korjaamojen on aktivoitava ajoneuvoyksikkö sen asennuksen jälkeen ennen kuin ajoneuvo poistuu tiloista, joissa asennus tehtiin

3.6.3 Tietoturvadatan luonti ja toimittaminen

M.Sec_Data_Generation	Tietoturvadatan luomisessa käytettävien algoritmien on oltava ainoastaan valtuutettujen ja luotettavien henkilöiden käytettävissä
M.Sec_Data_Transport	Tietoturvadata on luotava, siirrettävä ja asennettava ajoneuvoyksikköön tavalla, joka säilyttää sen asianmukaisen luottamuksellisuuden ja eheyden

3.6.4 Korttien toimittaminen

M.Card_Availability	Ajopiirturikortteja saadaan antaa ja toimittaa vain valtuutetuille henkilöille
M.Driver_Card_Uniqueness	Kuljettajilla saa kerrallaan olla vain yksi voimassa oleva kuljettajakortti
M.Card_Traceability	Korttien toimituksen on oltava jäljitettävissä (valkoiset listat, mustat listat), ja mustia listoja on käytettävä turvaseurannassa

3.6.5 Valvontalaitteen asennus, kalibrointi ja tarkastus

M.Approved_Workshops	Valvontalaitteen asennuksen, kalibroinnin ja tarkastuksen saavat suorittaa vain luotettavat ja hyväksytyt asentajat tai korjaamot
M.Regular_Inspections	Valvontalaite on tarkastettava ja kalibroitava säännöllisesti
M.Faithful_Calibration	Hyväksytyjen asentajien ja korjaamojen on asetettava valvontalaitteeseen oikeat ajoneuvoparametrit kalibroinnin aikana

3.6.6 Laitteiden käyttö

M.Faithful_Drivers	Kuljettajien on noudatettava annettuja sääntöjä ja käytäydyttävä vastuuntuntoisesti (kuten käytettävä kuljettajakorttejaan, valittava oikeat toimintatiedot tietoja käsin syötettäessä jne.)
--------------------	--

3.6.7 Lainvalvontaan liittyvät tarkastukset

M.Controls	Lainvalvontaan liittyviä tarkastuksia on suoritettava säännöllisesti ja satunnaisesti, ja niihin on sisällyttävä tietoturvan seuranta
------------	---

4. Tietoturvan toteuttamistoiminnot

4.1 Tunnistaminen ja todentaminen

4.1.1 Liiketunnistimen tunnistaminen ja todentaminen

UIA_201 Ajoneuvoyksikön on jokaisen vuorovaikutuksen yhteydessä voitava tunnistaa se liiketunnistin, johon se on kytketty.

UIA_202 Liiketunnistimen tunnistetietoihin on sisällyttävä tunnistimen hyväksyntänumero ja tunnistimen sarjanumero.

UIA_203 Ajoneuvoyksikön on todennettava liiketunnistin, johon se on kytketty,

- kun liiketunnistin kytketään,
- jokaisen valvontalaitteen kalibroinnin yhteydessä,
- kun käyttöjännite virtakatkoksen jälkeen palautuu.

Todentamisen on oltava molemminpuolinen ja ajoneuvoyksikön alulle panema.

UIA_204 Ajoneuvoyksikön on tietyin väliajoin (aikaväli on valmistajan määriteltävissä, mutta sen on oltava lyhyempi kuin yksi tunti) uudelleen tunnistettava ja todennettava liiketunnistin, johon se on kytketty, sekä varmistettava, että valvontalaitteen edellisen kalibroinnin yhteydessä tunnistettua liiketunnistinta ei ole vaihdettu.

UIA_205 Ajoneuvoyksikön on havaittava kopioitu todennusdata, jota yritetään käyttää uudelleen, ja estettävä sen käyttö.

UIA_206 Kun on havaittu tietty määrä (joka on valmistajan määriteltävissä, mutta ei saa olla enemmän kuin 20) perättäisiä epäonnistuneita todennusyrityksiä ja/tai havaittu, että liiketunnistin on vaihdettu luvattomasti (ts. muulloin kuin valvontalaitteen kalibroinnin aikana), SEF-toiminnon on

- luotava tapausta koskeva seurantatietue,
- varoitettava käyttäjää,
- jatkettava liiketunnistimen lähettämän ei-suojatun liikedatan vastaanottamista ja käyttämistä.

4.1.2 Käyttäjän tunnistaminen ja todentaminen

UIA_207 Ajoneuvoyksikön on jatkuvasti ja yksilöidysti seurattava kahden käyttäjän henkilöllisyyttä valvomalla ajopiirturikortteja, jotka on asetettu laitteen kuljettaja- ja apukuljettajakortille tarkoitettuihin korttiaukkoihin.

UIA_208 Käyttäjän tunnistetietojen on sisällettävä seuraavat tiedot:

- käyttäjäryhmä:
 - DRIVER (kuljettajakortti),
 - CONTROLLER (valvontakortti),
 - WORKSHOP (korjaamokortti),
 - COMPANY (yrityskortti),
 - UNKNOWN (laitteessa ei ole korttia),
- käyttäjän tunniste, joka muodostuu seuraavista tiedoista:
 - kortin myöntäneen jäsenvaltion tunnus ja kortin numero,
 - UNKNOWN-tieto, jos käyttäjäryhmä on UNKNOWN.

UNKNOWN-ryhmään kuuluvien käyttäjien henkilöllisyys voi olla automaattisesti tiedossa tai annettu.

UIA_209 Ajoneuvoyksikön on todennettava käyttäjät, kun kortti asetetaan paikoilleen.

UIA_210 Ajoneuvoyksikön on uudelleen todennettava käyttäjät,

- kun käyttöjännite virtakatkoksen jälkeen palautuu,
- tietyin väliajoin tai tiettyjen tapausten jälkeen (valmistajan määriteltävissä, mutta useammin kuin kerran päivässä).

UIA_211 Todentaminen on tehtävä todistamalla, että korttiaukkoon asetettu kortti on voimassa oleva ajopiirturikortti, jolla on oikeasta järjestelmästä peräisin olevaa tietoturvadataa. Todentamisen on oltava molemminpuolinen ja ajoneuvoyksikön alulle panema.

UIA_212 Edellä mainitun lisäksi korjaamoilta on vaadittava oikein annetun PIN-koodin avulla tehtävä tunnistaminen. PIN-koodien on oltava vähintään 4 merkin pituisia.

Huomautus: Jos PIN-koodi on siirretty ajoneuvoyksikköön sen lähellä olevasta ulkoisesta laitteesta, ei PIN-koodia tarvitse pitää salassa siirron aikana.

UIA_213 Ajoneuvoyksikön on havaittava kopioitu todennusdata, jota yritetään käyttää uudelleen, ja estettävä sen käyttö.

UIA_214 Kun viisi perättäistä todennusyritystä on epäonnistunut, SEF-toiminnon on

- luotava tapausta koskeva seurantatietue,
- varoitettava käyttäjää,
- oletettava, että käyttäjä on tyyppiä UNKNOWN ja että kortti ei ole voimassa (määritelmä z) ja vaatimus 007.

4.1.3 Etäyhteyttä käyttävän yrityksen tunnistaminen ja todentaminen

Yrityksen mahdollisuus käyttää etäyhteyttä on valinnainen. Sen vuoksi tätä kohtaa sovelletaan vain, jos kyseinen toiminto on käytettävissä.

- UIA_215 Ajoneuvoyksikön on jokaisen etäyhteyttä käyttävän yrityksen kanssa tapahtuvan vuorovaikutuksen yhteydessä voitava tunnistaa kyseinen yritys.
- UIA_216 Etäyhteyttä käyttävän yrityksen tunnisteeseen tulee sisältää kortin myöntäneen jäsenvaltion tunniste ja yrityksen yrityskortin numero.
- UIA_217 Ajoneuvoyksikön on onnistuttava todentamaan etäyhteyttä käyttävä yritys, ennen kuin se sallii yritykselle lähetettävään mitään tietoja.
- UIA_218 Todentaminen on tehtävä todistamalla, että yrityksellä on voimassa oleva yrityskortti, jolla on oikeasta järjestelmästä peräisin olevaa tietoturvadataa.
- UIA_219 Ajoneuvoyksikön on havaittava kopioitu todennusdata, jota yritetään käyttää uudelleen, ja estettävä sen käyttö.
- UIA_220 Kun viisi perättäistä epäonnistunutta todennusyritystä on havaittu, ajoneuvoyksikön on
- varoitettava etäyhteyttä käyttävää yritystä.

4.1.4 Hallintalaitteiden tunnistaminen ja todentaminen

Ajoneuvoyksiköiden valmistajat saattavat nähdä tarpeelliseksi käyttää laitteita, jotka on tarkoitettu ajoneuvoyksikön hallinnassa käytettäviin lisätoimintoihin (esim. ohjelmistojen päivittämiseen, tietoturvadatan uudelleen syöttämiseen jne.). Sen vuoksi tätä kohtaa sovelletaan vain, jos kyseinen mahdollisuus on käytettävissä.

- UIA_221 Ajoneuvoyksikön on jokaisen hallintalaitteen kanssa tapahtuvan vuorovaikutuksen yhteydessä voitava tunnistaa kyseinen hallintalaitte.
- UIA_222 Ajoneuvoyksikön on onnistuttava todentamaan hallintalaitte, ennen kuin se sallii muita vuorovaikutuksia.
- UIA_223 Ajoneuvoyksikön on havaittava kopioitu todennusdata, jota yritetään käyttää uudelleen, ja estettävä sen käyttö.

4.2 Käyttöoikeuksien valvonta

Käyttöoikeuksien valvonnan avulla varmistetaan, että vain ne, joilla on siihen lupa, lukevat tietoja arviointikohteesta, luovat niitä siinä tai muuttavat niitä siihen.

On huomattava, että vaikkakin ajoneuvoyksikköön tallennetuilla käyttäjätiedoilla on yksityisyyteen tai kaupallisiin salaisuuksiin liittyviä piirteitä, ne eivät luonteeltaan ole salassa pidettäviä. Sen vuoksi tietojen lukemisen mahdollistaviin käyttöoikeuksiin liittyvä toiminnallinen vaatimus (vaatimus 011) ei ole SEF-toiminnon alainen.

4.2.1 Käyttöoikeuksien valvonnan toimintalinjat

- ACC_201 Ajoneuvoyksikön on hallittava ja tarkastettava toimintojen ja tietojen käyttöoikeuksia.

4.2.2 Toimintojen käyttöoikeudet

- ACC_202 Ajoneuvoyksikön on valvottava toimintatilan valintaa koskevien sääntöjen noudattamista (vaatimukset 006–009).
- ACC_203 Ajoneuvoyksikön on käytettävä toimintatiloja käyttöoikeuksien valvontasääntöjen noudattamisen valvonnassa (vaatimus 010).

4.2.3 Tietojen käyttöoikeudet

- ACC_204 Ajoneuvoyksikön on valvottava tunnistustietojen kirjoittamiseen liittyvien käyttöoikeussääntöjen noudattamista (vaatimus 076)
- ACC_205 Ajoneuvoyksikön on valvottava siihen liitetyn liiketunnistimen tunnistustietojen kirjoittamiseen liittyvien käyttöoikeussääntöjen noudattamista (vaatimukset 079 ja 155)
- ACC_206 Ajoneuvoyksikön aktivoinnin jälkeen sen on varmistettava, että kalibrointitietoja voidaan syöttää ajoneuvoyksikköön ja tallentaa sen datamuistiin vain sen ollessa kalibrointitilassa (vaatimukset 154 ja 156).
- ACC_207 Ajoneuvoyksikön aktivoinnin jälkeen sen on valvottava kalibrointitietojen kirjoittamiseen ja poistamiseen liittyvien käyttöoikeussääntöjen noudattamista (vaatimus 097).

- ACC_208 Ajoneuvoyksikön aktivoinnin jälkeen sen on varmistettava, että ajan asetukseen liittyviä tietoja voidaan syöttää ajoneuvoyksikköön ja tallentaa sen datamuistiin vain sen ollessa kalibrointitilassa (tämä vaatimus ei koske vaatimusten 157 ja 158 sallimia pieniä korjauksia ajan asetuksiin).
- ACC_209 Ajoneuvoyksikön aktivoinnin jälkeen sen on valvottava ajan asetustietojen kirjoittamiseen ja poistamiseen liittyvien käyttöoikeussääntöjen noudattamista (vaatimus 100).
- ACC_210 Ajoneuvoyksikön on valvottava asianmukaisten tietoturvadatan lukemiseen ja kirjoittamiseen liittyvien käyttöoikeuksien noudattamista (vaatimus 080).

4.2.4 Tiedostorakenteet ja käyttöehdot

- ACC_211 Sovellus- ja datatiedostojen rakenne ja käyttöehdot on luotava valmistuksen aikana ja lukittava siten, ettei niitä voida myöhemmin muuttaa tai poistaa.

4.3 Selvitysvelvollisuus

- ACT_201 Ajoneuvoyksikön on varmistettava, että kuljettajien toimintaa koskeva selvitysvelvollisuus toteutuu (vaatimukset 081, 084, 087, 105a, 105b, 109 ja 109a).
- ACT_202 Ajoneuvoyksikön on säilytettävä pysyviä tunnistustietoja (vaatimus 075).
- ACT_203 Ajoneuvoyksikön on varmistettava, että korjaamojen toimintaa koskeva selvitysvelvollisuus toteutuu (vaatimukset 098, 101 ja 109).
- ACT_204 Ajoneuvoyksikön on varmistettava, että tarkastuksia suorittavien toimintaa koskeva selvitysvelvollisuus toteutuu (vaatimukset 102, 103 ja 109).
- ACT_205 Ajoneuvoyksikön on tallennettava matkamittarin lukematietoja (vaatimus 090) ja yksityiskohtaisia tietoja nopeudesta (vaatimus 093).
- ACT_206 Ajoneuvoyksikön on varmistettava, että käyttäjätietoja, jotka liittyvät vaatimukseen 081–093 ja 102–105b, mainitut rajat mukaan lukien, ei muuteta niiden tallentamisen jälkeen, paitsi silloin, kun ne jäävät vanhimmiksi tiedoiksi, jotka korvataan uusilla tiedoilla.
- ACT_207 Ajoneuvoyksikön on varmistettava, ettei se muuta ajopiirturikortille valmiiksi tallennettuja tietoja (vaatimukset 109 ja 109a), paitsi silloin, kun ne jäävät vanhimmiksi tiedoiksi, jotka korvataan uusilla tiedoilla (vaatimus 110), tai lisäyksen 1 kohdan 2.1 huomautuksessa kuvatuissa tapauksissa.

4.4 Seuranta

Seurantaominaisuuksia tarvitaan vain sellaisissa tapauksissa, jotka saattavat olla merkinä määräysten vastaisesta käsittelystä tai tietoturvan murtoyrityksestä. Niitä ei tarvita normaalin käyttöoikeuksien käyttämisen yhteydessä, vaikka sillä olisikin merkitystä tietoturvan kannalta.

- AUD_201 Ajoneuvoyksikön tietoturvaa vaarantavien tapausten sattuessa sen on tallennettava tapausta koskevat ja siihen liittyvät tiedot (vaatimukset 094, 096 ja 109).
- AUD_202 Ajoneuvoyksikön tietoturvaa vaarantavat tapaukset ovat seuraavat:

- Tietoturvan murtoyritykset:
 - liiketunnistimen epäonnistunut todentaminen,
 - ajopiirturikortin epäonnistunut todentaminen,
 - liiketunnistimen luvaton vaihtaminen,
 - virhe kortille syötettävien tietojen eheydessä,
 - virhe tallennettujen käyttäjätietojen eheydessä,
 - virhe sisäisessä tiedonsiirrossa,
 - laitteen luvaton avaaminen,
 - laitteen tahallinen vahingoittaminen,

- Edellistä kortin käyttöjaksoa ei lopetettu oikein,
- Virhe liikedatassa -tapaus,
- Katkos virransyötössä -tapaus,
- Ajoneuvoyksikön sisäinen vika.

AUD_203 Ajoneuvoyksikön on valvottava seurantatietueiden tallennusta koskevien sääntöjen noudattamista (vaatimus 094 ja 096).

AUD_204 Ajoneuvoyksikön on tallennettava liiketunnistimen luomat seurantatietueet datamuistiinsa.

AUD_205 Seurantatietueita on voitava tulostaa, näyttää ja kopioida.

4.5 Tietojen uudelleenkäyttö

REU_201 Ajoneuvoyksikön on varmistettava, että tilapäisesti tallennettuja tietoja voidaan käyttää uudelleen ilman, että siihen liittyy luvaton tietovirtaa.

4.6 Tarkkuus

4.6.1 Tiedonkulun ohjauksen toimintalinjat

ACR_201 Ajoneuvoyksikön on varmistettava, että vaatimuksiin 081, 084, 087, 090, 093, 102, 104, 105, 105a ja 109 liittyviä käyttäjätietoja voidaan käsitellä vain, kun ne ovat peräisin oikeasta lähteestä. Näitä ovat:

- ajoneuvon liikedata,
- ajoneuvoyksikön tosiaikainen kello,
- valvontalaitteen kalibrointitiedot,
- ajopiirturikortit,
- käyttäjän syöttämät tiedot.

ACR_201a Ajoneuvoyksikön on varmistettava, että vaatimukseen 109a liittyviä käyttäjätietoja voidaan syöttää vain ajalta kortin viimeisestä poistamisesta sen nyt tapahtuneeseen paikalleen asettamiseen (vaatimus 050a).

4.6.2 Sisäiset tiedonsiirrot

Tämän kohdan vaatimukset koskevat vain ajoneuvoyksikköjä, joissa on fyysisesti erillisiä osia.

ACR_202 Jos tietoja siirretään ajoneuvoyksikön fyysisesti erillisten osien välillä, tiedot on suojattava niiden muuttamista vastaan

ACR_203 Jos havaitaan sisäisen tiedonsiirron aikana tapahtunut tiedonsiirtovirhe, siirto on uusittava ja SEF-toiminnon on luotava tapausta koskeva seurantatietue.

4.6.3 Tallennettujen tietojen eheys

ACR_204 Ajoneuvoyksikön on tarkastettava, että sen muistiin tallennetut käyttäjätiedot ovat eheät.

ACR_205 Jos tallennettujen käyttäjätietojen eheydessä havaitaan virhe, SEF-toiminnon on luotava seurantatietue.

4.7 Luotettavuus käytössä

4.7.1 Testit

RLB_201 Kaikki pelkästään ajoneuvoyksikön valmistusvaiheessa käytettävät komennot, toiminnot tai koestuspisteet on tehtävä toimintakyvyttömiksi tai poistettava ennen ajoneuvoyksikön aktivointia. Ne eivät saa olla myöhemmin palautettavissa käyttöön.

RLB_202 Ajoneuvoyksikön on itse suoritettava testejä sitä ensi kertaa käynnistettäessä sekä normaalin käytön aikana sen virheettömän toiminnan todentamiseksi. Ajoneuvoyksikön itse suorittamiin testeihin on sisällyttävä tietoturvadatan eheyden todentaminen sekä tallennettujen suoritettavien ohjelmakoodien eheyden todentaminen (ellei niitä ole tallennettu ROM-muistiin).

RLB_203 Jos laitteen itse suorittaman testin aikana havaitaan virhe, SEF-toiminnon on

- luotava seurantatietue (paitsi jos laite on kalibrointitilassa) (ajoneuvoyksikön sisäinen vika),
- säilytettävä tallennettujen tietojen eheys.

4.7.2 Ohjelmistot

RLB_204 Ohjelmistojen käyttöolosuhteissa tapahtuvan analysoinnin tai korjailun on oltava mahdotonta ajoneuvoyksikön aktivoinnin jälkeen.

RLB_205 Ulkopuolelta syötettyä dataa ei saa hyväksyä suoritettavaksi ohjelmakoodiksi.

4.7.3 Fyysinen suojaus

RLB_206 Jos ajoneuvoyksikön rakenne mahdollistaa sen avaamisen, liiketunnistimen on havaittava kaikki muut kuin kalibrointi-toimintatilassa tapahtuneet kotelon avaamiset myös ilman ulkoista virtalähdettä vähintään kuuden kuukauden ajan. Näissä tapauksissa SEF-toiminnon on luotava tapausta koskeva seurantatietue. (Riittää, että seurantatietue luodaan ja tallennetaan vasta, kun virta jälleen kytketään laitteeseen.)

Jos ajoneuvoyksikköä ei rakenteensa vuoksi ole mahdollista avata, sen rakenteen on oltava sellainen, että yritykset käsitellä sitä epäasianmukaisesti ovat helposti havaittavissa (esim. tarkastamalla silmämääräisesti).

RLB_207 Aktivoinnin jälkeen ajoneuvoyksikön on havaittava laitteen tietyntyyppinen tahallinen vahingoittaminen (valmistajan määriteltävissä).

RLB_208 Edellä kuvatussa tapauksessa SEF-toiminnon on luotava seurantatietue ja ajoneuvoyksikön on (valmistajan määriteltävissä).

4.7.4 Keskeytykset virransyötössä

RLB_209 Ajoneuvoyksikön on havaittava poikkeamat virransyötölle määritellyistä arvoista mukaan lukien virran katkeaminen.

RLB_210 Edellä kuvatussa tapauksessa SEF-toiminnon on

- luotava seurantatietue (paitsi jos laite on kalibrointitilassa),
- säilytettävä ajoneuvoyksikön suojattu toimintatila,
- ylläpidettävä vielä toiminnassa oleviin osiin tai prosesseihin liittyvät tietoturvatoinnot,
- säilytettävä tallennettujen tietojen eheys.

4.7.5 Alkutilaan asettamisen olosuhteet

RLB_211 Jos virransyöttö keskeytyy tai jokin toimenpide keskeytyy ennen kuin se on saatettu loppuun tai muissa alkutilaan asettamista edellyttävissä olosuhteissa, ajoneuvoyksikön on tultava asetetuksi alkutilaansa virheettömästi.

4.7.6 Tietojen käytettävyys

RLB_212 Ajoneuvoyksikön on varmistettava, että tiedot ja toiminnot ovat tarvittaessa käytettävissä ja että tietoja ja toimintoja ei pyydetä tai niiden käyttöön antamisesta pidättäydytä tarpeettomasti.

RLB_213 Ajoneuvoyksikön on varmistettava, että kortteja ei voida poistaa ennen kuin tarvittavat tiedot on tallennettu niille (vaatimukset 015 ja 016)

RLB_214 Edellä kuvatussa tapauksessa SEF-toiminnon on luotava tapausta koskeva seurantatietue.

4.7.7 Lisäsovellukset

RLB_215 Jos ajoneuvoyksikössä on käytettävissä muita sovelluksia kuin ajopiirturisovellus, kaikki sovellukset on pidettävä fyysisesti ja/tai loogisesti erillään toisistaan. Nämä sovellukset eivät saa käyttää tietoturvadataa. Kerrallaan saa käynnissä olla vain yksi toiminto.

4.8 Tiedonvaihto

Tässä kohdassa käsitellään tiedonvaihtoa ajoneuvoyksikön ja siihen kytkettyjen laitteiden välillä.

4.8.1 Tiedonvaihto liiketunnistimen kanssa

DEX_201 Ajoneuvoyksikön on todennettava liiketunnistimelta tuodun liikedatan eheys ja aitous.

DEX_202 Jos liikedatan eheydessä tai aitoudessa havaitaan virhe, SEF-toiminnon on

- luotava seurantatietue,
- jatkettava tuodun liikedatan käyttämistä.

4.8.2 Tiedonvaihto ajopiirturikorttien kanssa

DEX_203 Ajoneuvoyksikön on todennettava ajopiirturikorteilta tuotujen tietojen eheys ja aitous.

DEX_204 Jos kortin tietojen eheydessä tai aitoudessa havaitaan virhe, ajoneuvoyksikön on

- luotava seurantatietue,
- oltava käyttämättä tietoja.

DEX_205 Ajoneuvoyksikön on lähetettävä ajopiirturiälykorteille tietoja, jotka on varustettu asianmukaisin tietoturvamäärittein, jotta kortti voi todentaa niiden eheyden ja aitouden.

4.8.3 Tiedonvaihto ulkoisten tallennusvälineiden kanssa (tietojen kopiointitoiminto)

DEX_206 Ajoneuvoyksikön on annettava todisteet ulkoiselle tallennusvälineelle kopioitujen tietojen alkuperästä.

DEX_207 Ajoneuvoyksikön on kyettävä todentamaan kopioitujen tietojen alkuperä niiden vastaanottajalle.

DEX_208 Ajoneuvoyksikön on kopioitava ulkoisille tallennusvälineille tietoja, jotka on varustettu asianmukaisin tietoturvamäärittein, jotta niiden eheys ja aitous voidaan todentaa.

4.9 Salauksen tuki

Tämän kohdan vaatimuksia sovelletaan vain tarvittaessa, käytettävien turvamekanismien ja valmistajan ratkaisujen mukaan.

CSP_201 Kaikkien ajoneuvoyksikön suorittamien salaukseen liittyvien toimien on oltava määritellyn algoritmin mukaisia ja noudatettava määriteltyjä avaimen pituuksia.

CSP_202 Jos ajoneuvoyksikkö luo salausavaimia, sen on tapahduttava määriteltyjen salausavaimien luontialgoritmin mukaisesti ja noudattamalla määriteltyjä salausavaimen pituuksia.

CSP_203 Jos ajoneuvoyksikkö jakelee salausavaimia, sen on tapahduttava määriteltyjen avaimen jakelumenetelmien mukaisesti.

CSP_204 Jos ajoneuvoyksikkö käyttää salausavaimia, sen on tapahduttava avaimen käyttämiseen määriteltyjen menetelmien mukaisesti.

CSP_205 Jos ajoneuvoyksikkö tuhoaa salausavaimia, sen on tapahduttava määriteltyjen avaimen tuhoamisen menetelmien mukaisesti.

5. Turvamekanismien määrittely

Vaadittavat turvamekanismit on määritelty lisäyksessä 11.

Valmistajat määrittelevät kaikki muut turvamekanismit.

6. Turvamekanismien vähimmäisvahvuus

Ajoneuvoyksikön turvamekanismien vähimmäisvahvuus on ITSEC-viiteaineiston mukainen High (korkea).

7. Varmuustaso

Ajoneuvoyksikön tavoitevarmuustaso on ITSEC-viiteaineiston mukainen E3.

	Uhat																Tietotekniikan tavoitteet												
	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.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 Epäonnistunut todentaminen	x	x							x											x									
UIA_215 Etäkäyttäjän tunnistaminen	x	x																x		x							x		
UIA_216 Etäkäyttäjän tunniste	x	x																x		x									
UIA_217 Etäkäyttäjän todentaminen	x	x																x		x							x		
UIA_218 Todentamiskeino	x	x																x		x									
UIA_219 Todentaminen, jota ei voida väärentää	x	x																x		x									
UIA_220 Epäonnistunut todentaminen	x	x																											
UIA_221 Hallintalaitteen tunnistaminen	x	x																x		x									
UIA_222 Hallintalaitteen todentaminen	x	x																x		x									
UIA_223 Todentaminen, jota ei voida väärentää	x	x																x		x									
Käyttöoikeuksien valvonta																													
ACC_201 Käyttöoikeuksien valvonnan toimintalinjat	x					x	x										x	x	x										
ACC_202 Toimintojen käyttöoikeudet	x					x	x												x										
ACC_203 Toimintojen käyttöoikeudet	x					x	x												x										
ACC_204 Ajoneuvoyksikön tunniste																		x	x										
ACC_205 Liitetyn liiketunnistimen tunniste									x									x	x										
ACC_206 Kalibrointitiedot	x					x												x	x										
ACC_207 Kalibrointitiedot						x													x	x									
ACC_208 Ajan asetustiedot							x												x	x									
ACC_209 Ajan asetustiedot							x												x	x									
ACC_210 Tietoturvadata																		x	x	x									
ACC_211 Tiedostorakenteet ja käyttöehdot	x					x												x	x	x									
Selvitysvollisuus																													
ACT_201 Kuljettajan selvitysvollisuus																					x								
ACT_202 Ajoneuvoyksikön tunnistetiedot																				x	x								
ACT_203 Korjaamon selvitysvollisuus																					x								
ACT_204 Tarkastuksia suorittavan selvitysvollisuus																					x								
ACT_205 Ajoneuvon liikkeisiin liittyvä selvitysvollisuus																					x								
ACT_206 Selvitystietojen muuttaminen																		x				x						x	
ACT_207 Selvitystietojen muuttaminen																		x				x						x	

AJOPIIRTURIKORTIN YLEISET TIETOTURVATAVOITTEET

1. Johdanto

Tässä asiakirjassa kuvataan ajopiirturikortti, uhat, jotka sen on torjuttava, sekä tietoturvatavoitteet, jotka sen on täytettävä. Asiakirjassa määritellään vaadittavat tietoturvan toteuttamistoiminnot. Edelleen asiakirjassa määritellään tietoturva-mekanismien oletettu vähimmäisvahvuus sekä kehityksen ja arvioinnin vaatima varmuustaso.

Tässä asiakirjassa viitataan vaatimuksiin, jotka on esitetty varsinaisessa liitteessä I B. On huomattava, että varsinaisen liitteen I B vaatimuksien ja tietoturvatavoitteiden vaatimuksien kohdalla saattaa esiintyä päällekkäisyyksiä. Mikäli suhde jonkin tietoturvatavoitteen vaatimuksen ja sen varsinaisen liitteen I B vaatimuksen, johon tämän tietoturvatavoitteen vaatimus viittaa, välillä on epäselvä, on varsinaisen liitteen I B vaatimus määräävä.

Sellaisiin varsinaisen liitteen I B vaatimuksiin, joihin ei viitata tietoturvatavoitteissa, ei kohdisteta tietoturvan toteuttamistoimintoja.

Ajopiirturikortti on normaali älykortti, jolla on erityinen ajopiirturisovellus ja joka on uusimpien älykortteja koskevien toiminnallisten ja tietoturvan varmistamiseen liittyvien vaatimusten mukainen. Sen vuoksi tämä tietoturvatavoite sisältää vain ajopiirturisovelluksen vaatimat tietoturvaan liittyvät lisävaatimukset.

Uhille, tavoitteille, menettelytavoille ja tietoturvan toteuttamistoimintojen erittelyille on annettu yksilölliset nimet, jotta ne olisivat jäljitettävissä kehitys- ja arviointiasiakirjoissa.

2. Lyhenteet, määritelmät ja viitetiedot**2.1 Lyhenteet**

IC	(Integrated circuit) Integroitu piiri (elektroninen komponentti, joka on suunniteltu suorittamaan tietojenkäsittely- ja/tai muistinhallintatoimintoja)
OS	(Operating system) Käyttöjärjestelmä
PIN	(Personal identification number) PIN-koodi; henkilökohtainen tunnusluku
ROM	(Read only memory) ROM-muisti; muisti, josta tietoja voidaan lukea, mutta johon ei voi kirjoittaa
SFP	(Security functions policy) Tietoturvatavoitteiden toimintalinjat
TBD	(To be defined) Määritellään erikseen (myöhemmin)
TOE	(Target of evaluation) Arviointikohde
TSF	(TOE security function) Arviointikohteen tietoturvatavoite
VU	(Vehicle unit) Ajoneuvoyksikkö

2.2 Määritelmät

Digitaalinen ajopiirturi	Valvontalaite
Suojattavat tiedot	Ajopiirturikortin tallentamat tiedot, jotka on suojattava niiden eheyden säilyttämiseksi, luvattoman muuttamisen estämiseksi ja salassa pitämiseksi (kun kyse on tietoturvadatasta). Tietoturvadata ja käyttäjätiedot kuuluvat suojattaviin tietoihin
Tietoturvadata	Tietoturvan toteuttamistoimintojen tukemiseen tarvittavat tiedot (esim. salausavaimet)
Järjestelmä	Laitteet, henkilöt tai organisaatiot, jotka jollain tavoin liittyvät valvontalaitteeseen
Käyttäjä	Mikä hyvänsä arviointikohteen ulkopuolinen laitekokonaisuus (henkilökäyttäjä tai ulkoinen tietotekninen laitekokonaisuus), joka on vuorovaikutuksessa arviointikohteen kanssa (paitsi jos käyttäjä-sanaa käytetään ilmaisussa 'käyttäjätiedot')

Käyttäjätiedot	Ajopiirturikortille tallennetut muut suojattavat tiedot kuin tietoturvadata. Käyttäjätiedot sisältävät tunnistetiedot ja toimintaa koskevat tiedot
Tunnistetiedot	Tunnistetiedot sisältävät kortin tunnistetiedot ja kortin haltijan tunnistetiedot
Kortin tunnistetiedot	Kortin tunnistamiseen liittyvät käyttäjätiedot, jotka on määritelty vaatimuksissa 190, 191, 192, 194, 215, 231 ja 235
Kortin haltijan tunnistetiedot	Kortin haltijan tunnistamiseen liittyvät käyttäjätiedot, jotka on määritelty vaatimuksissa 195, 196, 216, 232 ja 236
Toimintaan liittyvät tiedot	Toimintaan liittyvät tiedot sisältävät kortin haltijan toimintaan liittyvät tiedot, tapauksiin ja vikoihin liittyvät tiedot sekä tarkastustoimiin liittyvät tiedot
Kortin haltijan toimintaan liittyvät tiedot	Kortin haltijan toimintaan liittyvät käyttäjätiedot, jotka on määritelty vaatimuksissa 197, 199, 202, 212, 212a, 217, 219, 221, 226, 227, 229, 230a, 233 ja 237
Tapauksiin ja vikoihin liittyvät tiedot	Tapauksiin ja vikoihin liittyvät käyttäjätiedot, jotka on määritelty vaatimuksissa 204, 205, 207, 208 ja 223
Tarkastustoimiin liittyvät tiedot	Lainvalvontaan liittyviä tarkastuksia koskevat käyttäjätiedot, jotka on määritelty vaatimuksissa 210 ja 225

2.3 Viitetiedot

ITSEC	(Information Technology Security Evaluation Criteria) EY:n komission suositus yleisistä tietotekniikan turvallisuuden arviointiperusteista vuodelta 1991
IC PP	Smartcard Integrated Circuit Protection Profile – version 2.0 – issue September 1998. (Älykorttien integroitujen piirien suojausprofiili, versio 2.0, julkaistu syyskuussa 1998.) Rekisteröity Ranskan sertifiointielimessä numerolla PP/9806
ES PP	Smart Card Integrated Circuit With Embedded Software Protection Profile – version 2.0 – issue June 99. (Älykorttien integroidut piirit, joissa on sulautetun ohjelmiston suojausprofiili, versio 2.0, julkaistu kesäkuussa 1999.) Rekisteröity Ranskan sertifiointielimessä numerolla PP/9911

3. Perusteet

3.1 Ajopiirturikortin kuvaus ja käyttötapa

Ajopiirturikortti on viitteissä IC PP ja ES PP kuvatun mukainen älykortti, jolla on sovellus kortin käyttämiseksi valvontalaitteessa.

Ajopiirturikortin perustoiminnot ovat seuraavat:

- kortin ja kortin haltijan tunnistetietojen tallentaminen. Ajoneuvoyksikkö käyttää näitä tietoja kortin haltijan tunnistamiseen, tunnistuksen mukaisten toimintojen ja käyttöoikeuksien antamiseen sekä varmistamaan, että kortin haltijan toimia koskeva selvitysvelvollisuus toteutuu,
- kortin haltijan toimintaa koskevien tietojen, sekä kortin haltijaa koskevien, tapauksiin ja vikoihin sekä tarkastustoimiin liittyvien tietojen tallentaminen.

Ajopiirturikortti on näin ollen tarkoitettu käytettäväksi ajoneuvoyksikön korttiliitäntälaitteessa. Sitä voidaan käyttää myös kaikissa kortinlukulaitteissa (esim. henkilökohtaisen tietokoneen yhteydessä olevassa), jolla on kaikkien käyttäjätietojen lukemiseen oikeuttavat käyttöoikeudet.

Ajopiirturikortin elinkaaren loppukäyttövaiheessa (viitteessä ES PP määritellyn elinkaaren vaihe 7) vain ajoneuvoyksiköt saavat kirjoittaa käyttäjätietoja kortille.

Ajopiirturikortin toiminnalliset vaatimukset on määritelty varsinaisessa liitteessä I B ja lisäyksessä 2.

3.2 Ajopiirturikortin elinkaari

Ajopiirturikortin elinkaari on viitteessä ES PP kuvatun älykortin elinkaaren mukainen.

3.3 Uhat

Viitteissä ES PP ja IC PP lueteltujen älykorttien yleisten uhkien lisäksi ajopiirturikorttiin voi kohdistua seuraavia uhkia:

3.3.1 Päämäärät

Tietoturvaa vastaan hyökkäävien päämäärä on arviointikohteeseen tallennettujen käyttäjätietojen muuttaminen.

T.Ident_Data	Jos arviointikohteeseen tallennettujen tunnistetietojen (kuten kortin tyypin tai viimeisen voimassaolopäivän tai kortin haltijan tunnistetietojen) muuttaminen onnistuu, mahdollistaa se kortin vilpillisen käytön ja muodostaa huomattavan uhan järjestelmän yleiselle tietoturvatavoitteelle.
T.Activity_Data	Jos arviointikohteeseen tallennettujen toimintaa koskevien tietojen muuttaminen onnistuu, se uhkaa arviointikohteen tietoturvaa.
T.Data_Exchange	Jos arviointikohteeseen tallennettujen toimintaa koskevien tietojen muuttaminen (lisääminen, poistaminen, muuttaminen) onnistuu tietoja tuotaessa tai vietäessä, se uhkaa arviointikohteen tietoturvaa.

3.3.2 Hyökkäysreitit

Arviointikohteen sisältöön voidaan kohdistaa hyökkäys seuraavilla tavoilla:

- yrittämällä saada oikeudetonta tietoa arviointikohteen laitteiston ja ohjelmiston rakenteesta ja erityisesti sen tietoturvatavoiminoista tai tietoturvadatasta. Oikeudetonta tietoa voidaan saada hyökkäyksellä suunnittelijan tai valmistajan aineistoihin (varkaus, lahjonta jne.) tai suoraan tutkimalla arviointikohdetta (fyysinen koestaminen, päättelyminen jne.).
- käyttämällä hyväksi arviointikohteen rakenteen tai toteutuksen heikkouksia (hyödyntämällä laitteiston virheitä, ohjelmiston virheitä, virheitä tiedonsiirrossa, ympäristövaikutuksien aikaansaatuja arviointikohteen virheitä, käyttämällä hyväksi tietoturvatavoimintojen, kuten todennusmenettelyjen, tietojen käyttöoikeuksien valvonnan, salaustoi-
mien jne. heikkouksia).
- tekemällä muutoksia arviointikohteeseen tai sen tietoturvatavoimintoihin suorittamalla fyysisiä, sähköisiä tai loogisia hyökkäyksiä tai näiden yhdistelmiä.

3.4 Tietoturvatavoitteet

Koko digitaalisen ajopiirturijärjestelmän tärkein tietoturvatavoite on seuraava:

O.Main	Valvontaviranomaisten tarkastettavaksi tarkoitettujen tietojen on oltava käytettävissä ja niiden on täysin ja tarkasti kuvattava tarkastuksen kohteena olevia kuljettajia ja ajoneuvoja koskevat tapahtumat, jotka liittyvät ajo-, työ-, varal- laolo- ja lepoaikoihin sekä ajoneuvon nopeuteen.
--------	---

Tähän kokonaistietoturvatavoitteeseen vaikuttavat arviointikohteen tietoturvatavoitteet ovat sen vuoksi seuraavat:

O.Card_Identification_Data	Arviointikohteen on säilytettävä henkilötietojen antamisvaiheessa tallennetut kortin tunnistetiedot ja kortin haltijan tunnistetiedot.
O.Card_Activity_Storage	Arviointikohteen on säilytettävä ajoneuvoyksikköjen kortille tallentamat käyttä- jätiedot.

3.5 Tietotekniikan tietoturvatavoitteet

Viitteissä ES PP ja IC PP lueteltujen älykorttien tietoturvatavoitteiden lisäksi seuraavat tietotekniset arviointikohteen tietoturvatavoitteet vaikuttavat sen tärkeimpiin tietoturvatavoitteisiin arviointikohteen elinkaaren loppukäyttövaiheessa:

O.Data_Access	Arviointikohteen on rajoitettava oikeus käyttäjätietojen kirjoittamiseen siten, että se on vain todennetuilla ajoneuvoyksiköillä.
O.Secure_Communications	Arviointikohteen on kyettävä tukemaan turvallisia viestintäprotokollia ja menettelyjä kortin ja korttiliitäntälaitteen välillä silloin, kun sovellus sitä edellyttää.

3.6 Fyysiset, henkilöstön tai menetelmien vaikutustavat

Arviointikohteen tietoturvasuuteen vaikuttavat fyysiset, henkilöstön tai menetelmien vaikutustavat on lueteltu viitteissä ES PP ja IC PP (ympäristön tietoturvatavoitteita käsittelevissä luvuissa).

4. Tietoturvan toteuttamistoiminnot

Tässä kohdassa määritellään yksityiskohtaisesti joitakin sallittuja toimia, kuten tehtäviä ja viitettä ES PP koskevia valintoja, ja esitetään SEF-toimintoja koskevia lisävaatimuksia.

4.1 Yhdenmukaisuus suojausprofiilien kanssa

CPP_301 Arviointikohteen on oltava viitteen IC PP mukainen.

CPP_302 Arviointikohteen on oltava viitteen ES PP mukainen siten kuin on yksityiskohtaisesti määritelty.

4.2 Käyttäjän tunnistaminen ja todentaminen

Kortin on tunnistettava laitekokoisuus, johon se on yhdistetty sekä tiedettävä, onko se todennettu ajoneuvoyksikkö vai ei. Kortti saa lähettää kaikkia käyttäjätietoja laitekokoisuudelle, johon se on liitetty, lukuun ottamatta valvontakorttia, joka saa lähettää kortin haltijan tunnistetietoja vain todennetuille ajoneuvoyksiköille (jotta tarkastuksen suorittaja voi vakuuttaa siitä, että ajoneuvoyksikkö on aito, kun hän näkee nimensä näytöllä tai tulosteissa).

4.2.1 Käyttäjän tunnistaminen

Tehtävä (FIA_UID.1.1) *Luettelo arviointikohteen tietoturvatoinnin mukaan sovitetuista toimista:* ei toimia.

Tehtävä (FIA_ATD.1.1) *Luettelo tietoturvamääreistä:*

- USER_GROUP: VEHICLE_UNIT, NON_VEHICLE_UNIT,
- USER_ID: Ajoneuvon rekisteritunnus (VRN) ja ajoneuvon rekisteröineen jäsenvaltion tunnus (USER_ID tunnetaan vain, kun USER_GROUP = VEHICLE_UNIT).

4.2.2 Käyttäjän todentaminen

Tehtävä (FIA_UAU.1.1) *Luettelo arviointikohteen tietoturvatoinnin mukaan sovitetuista toimista:*

- Kuljettaja- ja korjaamokortti: lähetetään käyttäjätiedot tietoturvamääritteiden kanssa (kortin tietojen kopiointitoiminto),
- Valvontakortti: lähetetään käyttäjätiedot ilman muita tietoturvamääritteitä kuin kortin haltijan tunnistetiedot.

UIA_301 Ajoneuvoyksikön todentaminen on tehtävä todistamalla, että sillä on hallussaan tietoturvadata, jonka vain järjestelmä on voinut sille toimittaa.

Valinta (FIA_UAU.3.1 ja FIA_UAU.3.2): estettävä.

Tehtävä (FIA_UAU.4.1) *Yksilöity (yksilöidyt) todennusmekanismi(t):* mikä tahansa todennusmekanismi.

UIA_302 Korjaamokortilla on oltava todennukseen tarkoitettu lisämekanismi, joka perustuu PIN-koodin tarkastamiseen. (Tämän mekanismin tarkoitus on, että ajoneuvoyksikkö voi tarkastaa kortin haltijan henkilöllisyyden; sitä ei ole tarkoitettu suojaamaan korjaamokortin sisältöä.)

4.2.3 Epäonnistuneet todentamiset

Seuraavat tehtävät kuvaavat kortin reaktiota jokaiseen yksittäiseen käyttäjän todentamisen epäonnistumiseen.

Tehtävä (FIA_AFL.1.1) *Numero: 1, luettelo todentamistapauksista:* korttiliitäntälaitteen todentaminen.

Tehtävä (FIA_AFL.1.2) *Luettelo toimista:*

- varoitetaan kytkettynä olevaa laitekokoisuutta,
- oletetaan, että käyttäjä on tyyppiä NON_VEHICLE_UNIT.

Seuraavat tehtävät kuvaavat kortin reaktiota, jos vaatimuksessa UIA_302 esitetty todentamisen lisämekanismi epäonnistuu.

Tehtävä (FIA_AFL.1.1) *Numero: 5, luettelo todentamistapauksista:* PIN-koodin tarkistus (korjaamokortti).

Tehtävä (FIA_AFL.1.2) *Luettelo toimista:*

- varoitetaan kytkettynä olevaa laitekokonaisuutta,
- lukitaan PIN-koodin tarkistusmenettely siten, että kaikki seuraavat yritykset tarkistaa PIN-koodi epäonnistuvat,
- varaudutaan kertomaan seuraaville käyttäjille lukitsemisen syy.

4.3 **Käyttöoikeuksien valvonta**

4.3.1 *Käyttöoikeuksien valvonnan toimintalinjat*

Elinkaarensa loppukäyttövaiheen aikana ajopiirturikortti on yksien ainoiden käyttöoikeuksien valvontaa koskevien tietoturvatointojen toimintalinjojen (SFP) alainen, nimittäin AC_SFP-toimintalinjojen.

Tehtävä (FDP_ACC.2.1) *Käyttöoikeuksien valvonta-SFP:* AC_SFP.

4.3.2 *Käyttöoikeuksien valvontatoiminnot*

Tehtävä (FDP_ACF.1.1) *Käyttöoikeuksien valvonta-SFP:* AC_SFP.

Tehtävä (FDP_ACF.1.1) *Nimetty turvamäärity ryhmä:* USER_GROUP.

Tehtävä (FDP_ACF.1.2) *Säännöt, jotka koskevat valvottujen käyttäjien ja kohteiden käyttöoikeuksia, joita käytetään tekemällä valvottuja toimia valvotuille kohteille:*

- GENERAL_READ: Kaikki käyttäjät voivat lukea käyttäjätietoja kaikista arviointikohteista, lukuun ottamatta kortin haltijan tunnistetietoja, joita voi korjaamokortilta lukea vain käyttäjä tyyppiä VEHICLE_UNIT.
- IDENTIF_WRITE: Tunnistetiedot saadaan kirjoittaa vain kerran, ennen kortin elinkaaren kuudennen vaiheen päättymistä. Kukaan käyttäjä ei saa kirjoittaa tai muuttaa tunnistetietoja kortin elinkaaren loppukäyttövaiheen aikana.
- ACTIVITY_WRITE: Toimintaa koskevia tietoja saa arviointikohteeseen kirjoittaa vain VEHICLE_UNIT-käyttäjä.
- SOFT_UPGRADE: Kukaan käyttäjä ei saa päivittää arviointikohteen ohjelmistoja.
- FILE_STRUCTURE: Tiedostorakenteet ja käyttöehdot on luotava ennen arviointikohteen elinkaaren kuudennen vaiheen päättymistä ja lukittava sen jälkeen siten, ettei kukaan käyttäjä voi jälkepäin muuttaa tai poistaa niitä.

4.4 **Selvitysvelvollisuus**

ACT_301 Arviointikohteen on säilytettävä pysyvät tunnistetiedot.

ACT_302 Tietoihin on sisällyttävä tieto päivämäärästä ja ajasta, jolloin arviointikohteelle annettiin haltijan henkilötiedot. Näiden tietojen on säilyttävä muuttumattomina.

4.5 **Seuranta**

Arviointikohteen on seurattava tapauksia, jotka ovat merkinä sen tietoturvan mahdollisesta loukkaamisesta.

Tehtävä (FAU_SAA.1.2) *Määriteltujen seurattavien tapausten alaryhmä:*

- kortin haltijan epäonnistunut todentaminen (5 perättäistä epäonnistunutta PIN-koodin tarkastusta),
- laitteen itse suorittaman testin aikana ilmennyt virhe,
- virhe tallennettujen tietojen eheydessä,
- virhe toimintaa koskevien syötettävien tietojen eheydessä.

4.6 **Tarkkuus**

4.6.1 *Tallennettujen tietojen eheys*

Tehtävä (FDP_SDI.2.2) *Tehtävät toimet:* varoitetaan kytkettynä olevaa laitekokonaisuutta.

4.6.2 *Perustietojen todentaminen*

Tehtävä (FDP_DAU.1.1) *Luettelo kohteista tai tietojen tyypistä:* Toimintaa koskevat tiedot.

Tehtävä (FDP_DAU.1.2) *Luettelo käyttäjistä:* Mikä tahansa.

4.7 Luotettavuus käytössä

4.7.1 Testit

Valinta (FPT_TST.1.1): ensi kertaa käynnistettäessä, määrääjain normaalin käytön aikana.

Huomautus: 'ensi kertaa käynnistettäessä' tarkoittaa ennen kuin ohjelmakoodia on suoritettu (eikä välttämättä ATR-toiminnon aikana).

RLB_301 Arviointikohteen itse suorittamiin testeihin on sisällyttävä kaikkien muiden kuin ROM-muistiin tallennettujen ohjelmistokoodien eheyden todentaminen.

RLB_302 Jos havaitaan virhe itse suoritettussa testissä, arviointikohteen tietoturvatoinnoin on varoitettava kytkettynä olevaa laitekokonaisuutta.

RLB_303 Kun käyttöjärjestelmän testaus on suoritettu, kaikki testaukseen liittyvät komennot ja toiminnot on tehtävä toimintakyvyttömiksi tai poistettava. Näiden valvontatoimien kumoaminen ja mainittujen kommentojen ja toimintojen uudelleenkäyttöön otto ei saa olla mahdollista. Kommentoa, joka liittyy yksinomaan tiettyyn linkkaaren vaiheeseen, ei saa käyttää muiden vaiheiden aikana.

4.7.2 Ohjelmistot

RLB_304 Arviointikohteen ohjelmistojen käyttöolosuhteissa tapahtuvan analysoinnin tai korjailun on oltava mahdotonta.

RLB_305 Ulkopuolelta syötettyä dataa ei saa hyväksyä suoritettavaksi ohjelmakoodiksi.

4.7.3 Virtalähde

RLB_306 Arviointikohteen on säilytettävä suojattu toimintatila virtakatkoksen tai jännitevaihteluiden aikana.

4.7.4 Alkutilaan asettamisen olosuhteet

RLB_307 Jos arviointikohteen virransyöttö keskeytyy (tai jännite vaihtelee) tai jokin toimenpide keskeytyy ennen kuin se on saatettu loppuun tai muissa alkutilaan asettamista edellyttävissä olosuhteissa, arviointikohteen on tultava asetetuksi alkutilaansa virheettömästi.

4.8 Tiedonvaihto

4.8.1 Tiedonvaihto ajoneuvoyksikön kanssa

DEX_301 Arviointikohteen on todennettava ajoneuvoyksiköltä tuotujen tietojen eheys ja aitous.

DEX_302 Jos havaitaan virhe tuotujen tietojen eheydessä, arviointikohteen on

- varoitettava tietoja lähettävää laitekokonaisuutta,
- oltava käyttämättä tietoja.

DEX_303 Arviointikohteen on lähetettävä ajoneuvoyksikölle käyttäjätietoja, jotka on varustettu asianmukaisin tietoturvamäärittein, jotta ajoneuvoyksikkö voi todentaa vastaanotettujen tietojen eheyden ja aitouden.

4.8.2 Tiedonsiirto muulle kuin ajoneuvoyksikölle (tietojen kopiointitoiminto)

DEX_304 Arviointikohteen on annettava todisteet ulkoiselle tallennusvälineelle kopioitujen tietojen alkuperästä.

DEX_305 Arviointikohteen on kyettävä todentamaan kopioitujen tietojen alkuperä niiden vastaanottajalle.

DEX_306 Arviointikohteen on kopioitava ulkoisille tallennusvälineille tietoja, jotka on varustettu asianmukaisin tietoturvamäärittein, jotta niiden eheys ja aitous voidaan todentaa.

4.9 Salauksen tuki

CSP_301 Jos arviointikohteen tietoturvatoinnointo luo salausavaimia, sen on tapahduttava määriteltyjen salausavaimien luontialgoritmien mukaisesti ja noudattamalla määriteltyjä salausavaimen pituuksia. Luotujen tilapäisten avainten käyttökerrat on rajoitettava (valmistajan määriteltävissä, mutta ei enempää kuin 240 kertaa).

CSP_302 Jos arviointikohteen tietoturvatoinnointo jakelee salausavaimia, sen on tapahduttava määriteltyjen avaimen jakelumenetelmien mukaisesti.

5. Turvamekanismien määrittely

Vaadittavat turvamekanismit on määritelty lisäyksessä 11.

Arviointikohteiden valmistajat määrittelevät kaikki muut turvamekanismit.

Lisäys 11

YHTEISET TURVAMEKANISMIT

SISÄLLYSLUETTELO

1.	Yleistä	238
1.1	Viitetiedot	238
1.2	Merkintätavat ja lyhenteet	239
2.	Salausjärjestelmät ja -algoritmit	240
2.1	Salausjärjestelmät	240
2.2	Salausalgoritmit	240
2.2.1	RSA-algoritmi	240
2.2.2	Hajautus (Hash) -algoritmi	240
2.2.3	DES-salausalgoritmi	240
3.	Avaimet ja varmenteet	240
3.1	Avainten luonti ja jakelu	240
3.1.1	RSA-salausavainten luonti ja jakelu	240
3.1.2	RSA-testausavaimet	242
3.1.3	Liikkeentunnistinavaimet	242
3.1.4	Kolminkertaisessa DES-salauksessa käytettävien avainten luonti ja jakelu	242
3.2	Avaimet	242
3.3	Varmenteet	243
3.3.1	Varmenteiden sisältö	243
3.3.2	Annetut varmenteet	244
3.3.3	Varmenteen todentaminen ja purkaminen	245
4.	Molemminpuolinen todennusmekanismi	245
5.	Ajoneuvoyksikön ja kortin välisen tiedonsiirron salassapidon, eheyden turvaamisen ja todennuksen mekanismit	248
5.1	Salattu sanomanvälitys	248
5.2	Salatun sanomanvälityksen virheiden käsittely	249
5.3	Algoritmi salauksen tarkistussumman laskemiseksi	250
5.4	Algoritmi salattavien dataobjektien kryptogrammien laskemiseksi	250
6.	Tietojen kopioinnissa käytettävät digitaaliset allekirjoitusmekanismit	251
6.1	Allekirjoituksen luominen	251
6.2	Allekirjoituksen todentaminen	251

1. YLEISTÄ

Tässä lisäyksessä määritellään turvamekanismit, joiden avulla varmistetaan

- ajoneuvoyksikköjen ja ajopiirturikorttien molemminpuolinen todentaminen, mukaan lukien tilapäisavaimen liittyvä sopimus,
- ajoneuvoyksikköjen ja ajopiirturikorttien välillä siirrettävien tietojen salassapito, eheys ja todentaminen,
- ajoneuvoyksiköistä ulkoisille tietovälineille kopioitujen tietojen eheys ja todentaminen,
- I ajopiirturikorteilta ulkoisille tietovälineille kopioitujen tietojen eheys ja todentaminen.

1.1 Viitetiedot

Tässä lisäyksessä käytetään seuraavia viitetietoja:

SHA-1	National Institute of Standards and Technology (NIST). FIPS Publication 180-1: Secure Hash Standard. April 1995. (Turvallinen hajautusalgoritmistandardi. Huhtikuu 1995)
PKCS1	RSA Laboratories. PKCS # 1: RSA Encryption Standard. Version 2.0. October 1998. (RSA-salausstandardi. Versio 2.0. Lokakuu 1998)
TDES	National Institute of Standards and Technology (NIST). FIPS Publication 46-3: Data Encryption Standard. Draft 1999. (Tietojen salausstandardi. Luonnos 1999)
TDES-OP	ANSI X9.52, Triple Data Encryption Algorithm Modes of Operation. 1998. (Kolminkertaisten salausalgoritmien toimintatavat. 1998)
ISO/IEC 7816-4	Information Technology – Identification cards – Integrated circuit(s) cards with contacts – Part 4: Interindustry commands for interexchange. First edition: 1995 + Amendment 1: 1997. (Tietotekniikka. Henkilökortit. Integroidulla piirillä varustetut kontaktilliset kortit. Osa 4: Yleiset siirtokomennot. Ensimmäinen painos: 1995, ensimmäinen muutos: 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. (Tietotekniikka. Henkilökortit. Integroidulla piirillä varustetut kontaktilliset kortit. Osa 6: Yleiset dataelementit. Ensimmäinen painos: 1996, ensimmäinen korjaus: 1998)
ISO/IEC 7816-8	Information Technology – Identification cards – Integrated circuit(s) cards with contacts – Part 8: Security related interindustry commands. First edition 1999 (Tietotekniikka. Henkilökortit. Integroidulla piirillä varustetut kontaktilliset kortit. Osa 8: Yleiset turvakomennot. Ensimmäinen painos: 1999)
ISO/IEC 9796-2	Information Technology – Security techniques – Digital signature schemes giving message recovery – Part 2: Mechanisms using a hash function. First edition: 1997 (Tietotekniikka. Tietoturvatekniikat. Digitaaliset allekirjoitusjärjestelmät, joiden avulla alkuperäinen viesti voidaan palauttaa. Osa 2: Hajautusalgoritmia käyttävät mekanismit. Ensimmäinen painos: 1997)
ISO/IEC 9798-3	Information Technology – Security techniques – Entity authentication mechanisms – Part 3: Entity authentication using a public key algorithm. Second edition 1998. (Tietotekniikka. Tietoturvatekniikat. Laitekokonaisuuksien todennusmekanismit. Osa 3: Laitekokonaisuuden todentaminen julkisen avaimen algoritmia käyttäen. Toinen painos 1998)
ISO 16844-3	Road vehicles – Tachograph systems – Part 3: Motion sensor interface (Tieliikenteessä käytettävät ajoneuvot. Ajopiirturijärjestelmät. Osa 3: Liiketunnistimen rajapinta)

1.2 Merkitävat ja lyhenteet

Tässä lisäyksessä käytetään seuraavia merkitäviä ja lyhenteitä:

(K_a, K_b, K_c)	Avainnippu, jota kolminkertainen salausalgoritmi käyttää
CA	(Certification authority) Varmenneviranomaisen
CAR	(Certification authority reference) Varmenneviranomaisen viite
CC	(Cryptographic checksum) Salauksen tarkistussumma
CG	(Cryptogram) Kryptogrammi
CH	(Command header) Komennon ylätunniste
CHA	(Certificate holder authorisation) Varmenteen haltijan valtuutus
CHR	(Certificate holder reference) Varmenteen haltijan viite
D()	Salauksen avaaminen DES-algoritilla
DE	(Data element) Dataelementti
DO	(Data object) Dataobjekti
d	RSA-salauksessa käytettävä yksityinen avain eli yksityinen eksponentti
e	RSA-salauksessa käytettävä julkinen avain eli julkinen eksponentti
E()	Salaaminen DES-algoritilla
EQT	(Equipment) Laitteet
Hash()	Hash-hajautusalgoritilla laskettu tulos
Hash	Hajautusalgoritmi
KID	Avaimen tunnistus
Km	TDES-avain. ISO 16844-3-standardissa määritelty pääavain
Km_{VU}	Ajoneuvoyksikköön asetettava TDES-avain
Km_{WC}	Korjaamokorttiin asetettava TDES-avain
m	Viestiä edustava luku, kokonaisluku välillä 0- $n-1$
n	RSA-avaimien yhteinen osa, (kongruenssi)moduuli
PB	(Padding bytes) Täyttötavut
PI	(Padding indicator byte) Täyttämistä ilmaiseva tavu (käytetään salatun datan kryptogrammissa)
PV	(Plain value) Koodaamaton datan arvo
s	Allekirjoitusta edustava luku, kokonaisluku välillä 0- $n-1$
SSC	(Send Sequence counter) Lähetysvaihelaskuri
SM	Salattu sanomanvälitys
TCBC	(TDEA cipher block chaining mode of operation) TDEA-salauksen salauslohkoja ketjuttava käyttötila
TDEA	Kolminkertainen tiedonsalausalgoritmi
TLV	(Tag length value) TLV-koodaustapa; tuntomerkki-pituus-sisältö-koodaustapa
VU	Ajoneuvoyksikkö
X.C	Varmenneviranomaisen antama käyttäjä X:n varmenne
X.CA	Käyttäjä X:n varmenneviranomaisen
X.CA.PK ₀ .X.C	Toimenpide, jolla varmenne avataan sen sisältämän julkisen avaimen saamiseksi. Kyseessä on operandien väliin tuleva operaattori, jonka vasemmanpuoleinen kohdemuuttuja (operandi) on varmenneviranomaisen julkinen avain ja oikeanpuoleinen kohdemuuttuja on tämän varmenneviranomaisen antama varmenne. Tulos on sen käyttäjä X:n julkinen avain, jonka varmenne on oikeanpuoleisena kohdemuuttujana

X.PK	Käyttäjä X:n julkinen RSA-avain
X.PK[I]	Käyttäjä X:n julkista avainta käyttäen tehty tiedon I RSA-salaus
X.SK	Käyttäjä X:n yksityinen RSA-avain
X.SK[I]	Käyttäjä X:n yksityistä avainta käyttäen tehty tiedon I RSA-salaus
'xx'	Heksadesimaalilukuna ilmaistu arvo
	Ketjutusmerkki

2. SALAUSJÄRJESTELMÄT JA -ALGORITMIT

2.1 Salausjärjestelmät

CSM_001 Ajoneuvoyksikköjen ja ajopiirturikorttien on käytettävä klassista julkiseen avaimeen perustuvaa RSA-salausjärjestelmää luomaan seuraavat tietoturvamekanismit:

- ajoneuvoyksikköjen ja korttien välinen todentaminen,
- kolminkertaisessa DES-salauksessa käytettävien avainten siirtäminen ajoneuvoyksikköjen ja ajopiirturikorttien välillä,
- ajoneuvoyksiköistä tai ajopiirturikorteilta ulkoisille tallennusvälineille kopioitujen tietojen digitaalinen allekirjoitus.

CSM_002 Ajoneuvoyksikköjen ja ajopiirturikorttien on käytettävä kolminkertaista symmetristä DES-salausjärjestelmää luomaan mekanismi, jolla taataan tietojen eheys vaihdettaessa käyttäjätietoja ajoneuvoyksikköjen ja ajopiirturikorttien välillä, sekä tarvittaessa käytettävä sitä salaamaan ajoneuvoyksikköjen ja ajopiirturikorttien välillä vaihdettavat tiedot.

2.2 Salausalgoritmit

2.2.1 RSA-algoritmi

CSM_003 Seuraavat riippuvuudet määrittelevät täysin RSA-algoritmin:

$$\begin{aligned} X.SK[m] &= s = m^d \bmod n \\ X.PK[s] &= m = s^e \bmod n \end{aligned}$$

RSA-funktio on kuvattu yksityiskohtaisesti viitteessä PKCS1. RSA-laskelmissa käytettävä julkinen eksponentti e on kaikissa luoduissa RSA-avaimissa muu kuin 2.

2.2.2 Hajautus (Hash) -algoritmi

CSM_004 Digitaalisten allekirjoitusmekanismien on käytettävä viitteessä SHA-1 määriteltyä SHA-1-hajautusalgoritmia.

2.2.3 DES-salausalgoritmi

CSM_005 DES-perustaisia algoritmeja on käytettävä ketjuttaen salattavat lohkot.

3. AVAIMET JA VARMENTEET

3.1 Avainten luonti ja jakelu

3.1.1 RSA-salausavainten luonti ja jakelu

CSM_006 RSA-avaimet on luotava kolmella toiminnallisesti hierarkkisella tasolla:

- eurooppalaisella tasolla,
- jäsenvaltiotasolla,
- laitetasolla.

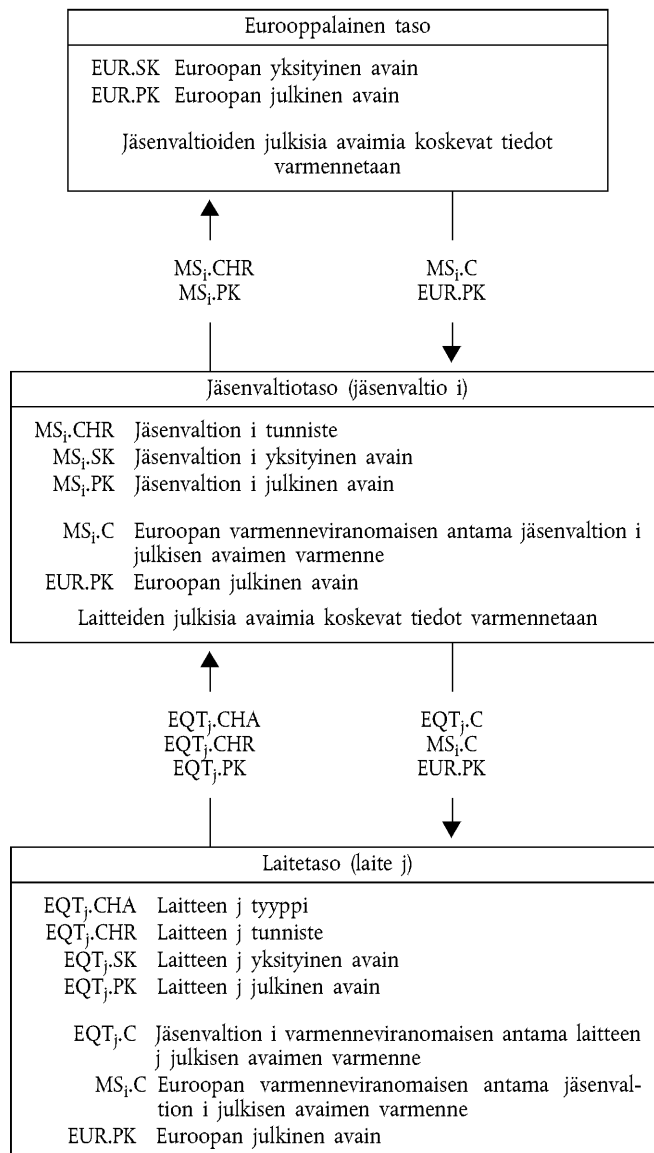
CSM_007 Eurooppalaisella tasolla on luotava yksi eurooppalainen avainpari (EUR.SK ja EUR.PK). Eurooppalaista yksityistä avainta on käytettävä varmentamaan jäsenvaltioiden julkiset avaimet. Kaikista varmennetuista avaimista on pidettävä rekisteriä. Euroopan varmenneviranomaisen on hoidettava nämä tehtävät Euroopan komission valtuuttamana ja vastuulla.

CSM_008 Jäsenvaltiotasolla on luotava jäsenvaltion avainpari (MS.SK ja MS.PK). Euroopan varmenneviranomaisen on varmennettava jäsenvaltioiden julkiset avaimet. Jäsenvaltioiden yksityistä avainta on käytettävä varmentamaan laitteisiin (ajoneuvo-yksikköön tai ajopiirturikortteille) asennetut julkiset avaimet. Kaikista varmennetuista julkisista avaimista on pidettävä rekisteriä, jossa on kunkin avaimen osalta sen laitteen tunnistus, johon avain on tarkoitettu. Jäsenvaltion varmenneviranomaisen on hoidettava nämä tehtävät. Jäsenvaltio saa vaihtaa avainpariaan säännöllisesti.

CSM_009 Laitetasolla on jokaiselle laitteelle luotava ja siihen lisättävä yksi avainpari (EQT.SK ja EQT.PK). Jäsenvaltion varmenneviranomaisen on varmennettava laitteiden julkinen avain. Nämä tehtävät voi hoitaa laitteen valmistaja, se, joka syöttää laitteeseen haltijan henkilötiedot, tai jäsenvaltion viranomaisen. Tätä avainparia käytetään todennuksessa, digitaalisessa allekirjoituksessa ja salauksessa.

CSM_010 Yksityiset avaimet on pidettävä salassa niitä luotaessa, siirrettäessä (jos niitä siirretään) ja säilytettäessä.

Seuraavassa kuvassa on tämän prosessin tietovirran yhteenveto:



3.1.2 RSA-testausavaimet

CSM_011 Laitteiden testausta varten (mukaan lukien yhteentoimivuustestit) Euroopan varmenneviranomaisen on luotava yksi erillinen Euroopan testausavainpari ja vähintään kaksi jäsenvaltioiden testausavainparia, joiden julkiset avaimet on varmennettava Euroopan yksityisellä testausavaimella. Laitteiden valmistajien on asennettava tyyppihyväksyntää varten testattaviin laitteisiin jollain näistä jäsenvaltioiden testausavaimista varmennettu testausavain.

3.1.3 Liikkeen tunnistinavaimet

Alla kuvatut kolme TDES-avainta on pidettävä asianmukaisesti salassa luonnin, (mahdollisen) siirron ja säilytyksen aikana.

ISO 16844 -standardin mukaisten tallennuslaitteiden tukemiseksi Euroopan varmenneviranomaisen ja jäsenvaltioiden varmenneviranomaisten on lisäksi toimittava seuraavasti:

CSM_036 Euroopan varmenneviranomaisen on luotava kaksi itsenäistä ja ainutkertaista TDES-avainta ($K_{m_{VU}}$ ja $K_{m_{WC}}$) ja luotava K_m seuraavasti:

$$K_m = K_{m_{VU}} \text{ XOR } K_{m_{WC}}$$

Euroopan varmenneviranomaisen on toimitettava nämä avaimet tarvittavin turvatoimin pyynnöstä jäsenvaltioiden varmenneviranomaisille.

CSM_037 Jäsenvaltioiden varmenneviranomaisten on:

- käytettävä K_m :ää salatessaan liikkeen tunnistinvalmistajien pyytämät liikkeen tunnistintiedot (K_m :llä salattavat tiedot määritellään ISO 16844-3-standardissa),
- toimitettava tarvittavin turvatoimin $K_{m_{VU}}$ ajoneuvoyksiköiden valmistajille asennettavaksi ajoneuvoyksiköihin,
- varmistettava, että $K_{m_{WC}}$ asennetaan kaikkiin korjaamokortteihin (`SensorInstallationSecData` tiedostossa `Sensor_Installation_Data`) kortin asiakaskohtaisia asetuksia tehtäessä.

3.1.4 Kolminkertaisessa DES-salauksessa käytettävien avainten luonti ja jakelu

CSM_012 Ajoneuvoyksikköjen ja ajopiirturikorttien on osana molemminpuoleista todennusprosessia luotava ja vaihdettava tarvittavat tiedot yhteisen kolminkertaisen DES-salauksen avaimen luomiseksi. Tämä tiedonvaihto on salattava RSA-salausmekanismia käyttäen.

CSM_013 Tätä avainta on käytettävä kaikkiin myöhempiin salaustoimiin, joissa käytetään salattua sanomanvälitystä. Sen voimassaolo päättyy kortin käyttöjakson päättyessä (kun kortti poistetaan tai asetetaan alkutilaansa) ja/tai 240 käyttökerran jälkeen (yksi avaimen käyttökerta = yksi salattua sanomanvälitystä käyttäen kortille lähetetty komento ja siihen liittyvä vastaus).

3.2 Avaimet

CSM_014 RSA-avaimen pituuden (kaikilla tasoilla) on oltava seuraava: moduuli n 1 024 bittiä, julkinen eksponentti e enintään 64 bittiä, yksityinen eksponentti d 1 024 bittiä.

CSM_015 Kolminkertaisen DES-salauksen avainten on oltava muotoa (K_a, K_b, K_a) , missä K_a ja K_b ovat toisistaan riippumattomia 64 bitin pituisia avaimia. Pariteettibittejä ei aseteta.

3.3. Varmenteet

CSM_016 Julkisten RSA-avainten varmenteiden on oltava heterologisia (non self descriptive) kortin avulla todennettavia (card verifiable) varmenteita (Viite.: ISO/IEC 7816-8)

3.3.1. **Varmenteiden sisältö**

CSM_017 Julkisten RSA-avainten varmenteet koostuvat seuraavista tiedoista seuraavassa järjestyksessä:

Data	Muoto	Tavuja	Selite
CPI	INTEGER	1	Varmenteen profiilin tunniste (tässä versiossa '01')
CAR	OCTET STRING	8	Varmenneviranomaisen viite
CHA	OCTET STRING	7	Varmenteen haltijan valtuutus
EOV	TimeReal	4	Varmenteen viimeinen voimassaoloaika. Valinnainen, täytetään tavuilla 'FF', jos ei käytössä.
CHR	OCTET STRING	8	Varmenteen haltijan viite
<i>n</i>	OCTET STRING	128	Julkinen avain (moduuli)
<i>e</i>	OCTET STRING	8	Julkinen avain (julkinen eksponentti)
		164	

Huomautuksia:

1. Varmenteen profiilin tunniste (CPI) kuvaa todennusvarmenteen tarkan rakenteen. Sitä voidaan käyttää laitteen sisäisesti yksilöimään tietty ylätunnisteluettelo, joka kuvaa varmenteessa olevien dataelementtien ketjutuksen.

Tämän varmenteen sisältöön liittyvä ylätunnisteluettelo on seuraava:

	'4D'	'16'	'5F 29'	'01'	'42'	'08'	'5F 4B'	'07'	'5F 24'	'04'	'5F 20'	'08'	'7F 49'	'05'	'81'	'81 80'	'82'	'08'
Pidennetyt ylätunnisteluettelon tunnisteet																		
Ylätunnisteluettelon pituus																		
CPI:n tunniste																		
CAR:n tunniste																		
CHA:n tunniste																		
EOV:n tunniste																		
CHR:n tunniste																		
Julkinen avaimen tunniste (koottu)																		
Seuraavien dataobjektien pituus																		
Moduulin tunniste																		
Moduulin pituus																		
Julkinen eksponentin tunniste																		
Julkinen eksponentin pituus																		

2. Varmenneviranomaisen viitteen (CAR) avulla tunnistetaan varmenteen antanut varmenneviranomaisen siten, että dataelementtiä voidaan käyttää samanaikaisesti viranomaisen avaimen tunnisteiden kanssa löytämään varmenneviranomaisen julkinen avain (koodaus on selitetty jäljempänä avaimen tunnistetta käsittelevässä kohdassa).
3. Varmenteen haltijan valtuutusta (CHA) käytetään yksilöimään varmenteen haltijan oikeudet. Se koostuu ajopiirturi-sovelluksen tunnisteesta ja sen laitteen tyypistä, johon varmenne on tarkoitettu *EquipmentType*-dataelementin mukaisesti; jäsenvaltiota vastaava arvo on 00).
4. Varmenteen haltijan viitteen (CHR) avulla yksilöidään varmenteen haltija siten, että dataelementtiä voidaan käyttää samanaikaisesti kyseisen avaimen tunnisteiden kanssa löytämään varmenteen haltijan julkinen avain.
5. Avaimen tunnisteet yksilöivät varmenteen haltijan tai varmenneviranomaisen. Ne koodataan seuraavasti:

5.1. Laite (Ajoneuvoyksikkö tai kortti):

Data	Laitteen sarjanumero	Päivämäärä	Tyyppi	Valmistaja
Pituus	4 tavua	2 tavua	1 tavu	1 tavu
Arvo	Kokonaisluku	kk vv BCD-koodatuna	Valmistajan mukaan	Valmistajan koodi

Varmennetta pyytäessään ajoneuvoyksikön valmistaja joko tietää tai ei tiedä sen laitteen tunnistetta, johon avaimet tullaan asentamaan.

Ensin mainitussa tapauksessa valmistaja lähettää laitteen tunnisteen julkisen avaimen kanssa jäsenvaltionsa viranomaiselle saadakseen varmenteen. Varmenne sisältää tällöin laitteen tunnisteen ja valmistajan on varmistettava, että avain ja varmenne asennetaan aiottuun laitteeseen. Avaimen tunniste on jäljempänä esitetyn muotoinen.

Jälkimmäisessä tapauksessa valmistajan on yksilöitävä jokainen varmennepyyntö ja lähetettävä tämä tunniste julkisen avaimen kanssa jäsenvaltionsa viranomaiselle saadakseen varmenteen. Varmenne sisältää pyynnön tunnisteen. Kun avain on asennettu johonkin laitteeseen, valmistajan on annettava jäsenvaltion viranomaiselle tieto siitä, mihin laitteeseen se asennettiin (ts. pyynnön tunniste, laitteen tunniste). Avaimen tunniste on seuraavan muotoinen:

Data	Varmennepyynnön järjestysnumero	Päivämäärä	Tyyppi	Valmistaja
Pituus	4 tavua	2 tavua	1 tavu	1 tavu
Arvo	BCD-koodattu	kk vv BCD-koodattuna	'FF'	Valmistajan koodi

5.2. Varmenneviranomaisen:

Data	Viranomaisen tunniste	Avaimen järjestysnumero	Lisätiedot	Tunniste
Pituus	4 tavua	1 tavu	2 tavua	1 tavu
Arvo	1 tavu: valtion numerotunnus 3 tavua: valtion aakkosnumeerinen tunnus	Kokonaisluku	Koodatut lisätiedot (CA:n mukaan) 'FF FF', jos ei käytössä	'01'

Avaimen järjestysnumeroa käytetään erottamaan toisistaan jäsenvaltion eri avaimet tapauksissa, joissa avain vaihdetaan.

6. Varmenteiden todentajien on saatava tieto siitä, että varmennettu julkinen avain on RSA-avain, jota käytetään todentamiseen, digitaaliseen allekirjoitukseen ja salaukseen (varmenne ei sisällä tunnistetta, joka kertoisi sen).

3.3.2 Annetut varmenteet

CSM_018 Annettu varmenne on digitaalinen allekirjoitus, joka sisältää varmenteen sisällön osittaisen palautuksen ISO/IEC 9796-2 -standardin mukaisesti ja johon on liitetty varmenneviranomaisen viite.

$$X.C = X.CA.SK['6A' || C_r || Hash(Cc) || 'BC'] || C_n || X.CAR$$

Varmenteen sisällön ollessa $= C_c =$ C_r || C_n
106 tavua || 58 tavua

Huomautuksia:

1. Tämä varmenne on 194 tavun pituinen.
2. Allekirjoituksella peitetty varmenneviranomaisen viite (CAR) liitetään myös allekirjoitukseen, jotta varmenteen todentamiseksi voidaan valita varmenneviranomaisen julkinen avain.
3. Varmenteen todentajan on automaattisesti tunnettava algoritmi, jota varmenneviranomaisen on käyttänyt allekirjoittaessaan varmenteen.

5. AJONEUVOYKSIKÖN JA KORTIN VÄLISEN TIEDONSIIRRON SALASSAPIDON, EHEYDEN TURVAAMISEN JA TODENNUKSEN MEKANISMIT

5.1 Salattu sanomanvälitys

- CSM_021 Ajoneuvoyksikön ja kortin välisen tiedonsiirron eheys on turvattava käyttämällä salattua sanomanvälitystä viitteiden ISO/IEC 7816-4 ja ISO/IEC 7816-8 mukaisesti.
- CSM_022 Kun tiedot on suojattava siirron ajaksi, on komennon tai sen vastauksen mukana lähetettäviin dataobjekteihin liitettävä salauksen tarkistussumman sisältävä dataobjekti. Vastaanottajan on todennettava salauksen tarkistussumma.
- CSM_023 Komennon mukana lähetettyyn tietojen salauksen tarkistussummaan on laskettava mukaan komennon ylätunniste ja kaikki lähetetyt dataobjektit (= > CLA = '0C', ja kaikki dataobjektit on ympäröitävä tunnusmerkeillä, joissa b1 = 1).
- CSM_024 Vastauksen tilaa osoittavat tavut on suojattava salauksen tarkistussummalla, kun vastauksessa ei ole datakenttää.
- CSM_025 Salauksen tarkistussummien on oltava neljän tavun pituisia.

Salattua sanomanvälitystä käytettäessä komentojen rakenne on sen vuoksi seuraava:

Käytetyt dataobjektit ovat osa ISO/IEC 7816-4 -standardissa kuvatuista salatussa sanomanvälityksessä käytettävistä dataobjekteista:

Tuntemerkki	Muistikas	Merkitys
'81'	T _{PV}	Koodaamaton data, jota ei ole BER-TLV-koodattu (suojataan CC:llä)
'97'	T _{LE}	Le:n arvo suojaamattomassa komennossa (suojataan CC:llä)
'99'	T _{SW}	Status info (suojataan CC:llä)
'8E'	T _{CC}	Salauksen tarkistussumma CC
'87'	T _{PI CG}	Täyttämistä osoittava tavu Kryptogrammi (koodaamaton data, jota ei ole BER-TLV-koodattu)

Kun suojaamaton komento-vastauspari on:

Komennon ylätunniste	Varsinainen komento
CLA INS P1 P2	[L _c -kenttä] [Datakenttä] [L _c -kenttä]
neljä tavua	L tavua merkittynä B ₁ bis B _L

Varsinainen vastaus	Vastauksen lopuke
[Datakenttä]	SW1 SW2
L _r datatavua	kaksi tavua

Niin vastaava suojattu komento-vastauspari on:

Suojattu komento:

Komennon ylätunniste (CH)	Varsinainen komento										
CLA INS P1 P2	[Uusi L _c -kenttä]	[Uusi datakenttä]									[Uusi L _c -kenttä]
'0C'	Uuden datakentän pituus	T _{PV}	L _{PV}	PV	T _{LE}	L _{LE}	L _e	T _{CC}	L _{CC}	CC	'00'
		'81'	L _c	Data-kenttä	'97'	'01'	L _e	'8E'	'04'	CC	

Tarkistussummaan laskettava data = CH || PB || T_{PV} || L_{PV} || PV || T_{LE} || L_{LE} || L_e || PB

PB = Täyttötavut (80..00) standardin ISO-IEC 7816-4 ja ISO 9797 menetelmän 2 mukaisesti.

PV- ja LE-dataobjektit ovat mukana vain, jos suojaamattomassa komennoissa on vastaavaa dataa.

Suojattu vastaus:

1. Tapaus, jossa vastauksen datakenttä ei ole tyhjä mutta sitä ei tarvitse pitää salassa:

Varsinainen vastaus						Vastauksen lopuke
[Uusi datakenttä]						Uusi SW1 SW2
T _{PV}	L _{PV}	PV	T _{CC}	L _{CC}	CC	
'81'	L _r	Data-kenttä	'8E'	'04'	CC	

Tarkistussummaan laskettava data = T_{PV} || L_{PV} || PV || PB

2. Tapaus, jossa vastauksen datakenttä ei ole tyhjä ja se on pidettävä salassa:

Varsinainen vastaus						Vastauksen lopuke
[Uusi datakenttä]						Uusi SW1 SW2
T _{PI CG}	L _{PI CG}	PI CG	T _{CC}	L _{CC}	CC	
'87'		PI CG	'8E'	'04'	CC	

CG-kryptogrammin sisältämä data: data ilman BER-TLV-koodausta ja täyttötavut.

Tarkistussummaan laskettava data = T_{PI CG} || L_{PI CG} || PI CG || PB

3. Tapaus, jossa vastauksen datakenttä on tyhjä:

Varsinainen vastaus						Vastauksen lopuke
[Uusi datakenttä]						Uusi SW1 SW2
T _{SW}	L _{SW}	SW	T _{CC}	L _{CC}	CC	
'99'	'02'	SW1 SW2 Uusi	'8E'	'04'	CC	

Tarkistussummaan laskettava data = T_{SW} || L_{SW} || SW || PB

5.2 Salatun sanomanvälityksen virheiden käsittely

CSM_026 Kun ajopiirturikortti komentoa tulkitessaan havaitsee virheen salatussa sanomanvälityksessä, on tilaa osoittavat tavut lähetettävä takaisin ilman salattua sanomanvälitystä. ISO/IEC 7816-4 -standardin mukaisesti seuraavat tilaa osoittavat tavut on määritelty osoittamaan virheitä salatussa sanomanvälityksessä:

'66 88': Salauksen tarkistussumman todennus epäonnistui,

'69 87': Odotettuja salatun sanomanvälityksen dataobjekteja puuttuu,

'69 88': Salatun sanomanvälityksen dataobjektit virheellisiä.

CSM_027 Kun ajopiirturikortti lähettää takaisin tavuja ilman salatun sanomanvälityksen dataobjekteja tai virheellisen salatun sanomanvälityksen dataobjektin kanssa, ajoneuvoyksikön on lopetettava tiedonvaihtojakso.

5.3 Algoritmi salauksen tarkistussumman laskemiseksi

CSM_028 Salauksen tarkistussummat kootaan käyttäen ANSI X9.19 -standardin mukaisia retail MAC -tyyppisiä viestin todennuksen tarkistussummia ja DES-salausta:

- ensimmäinen vaihe: ensimmäinen tarkistuslohko y_0 on $E(K_a, SSC)$,
 - seuraavat vaiheet: tarkistuslohkot y_1 - y_n lasketaan K_a -avainta käyttäen,
 - viimeinen vaihe: salauksen tarkistussumma lasketaan viimeisestä tarkistuslohkosta y_n seuraavasti: $E(K_a, D(K_b, y_n))$,
- missä $E()$ tarkoittaa salaamista DES-algoritmillä ja $D()$ tarkoittaa salauksen avaamista DES-algoritmillä.

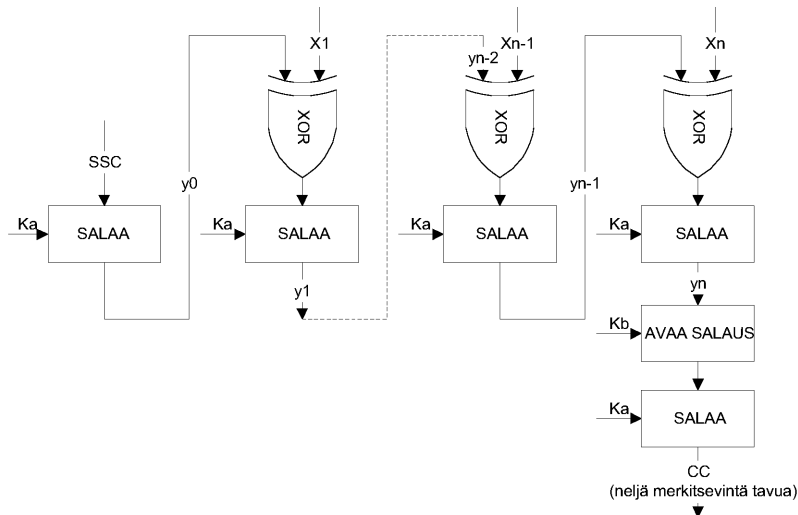
Salauksen tarkistussumman neljä merkitsevintä tavua lähetetään.

CSM_029 Lähetysvaihelaskuri (SSC) on avaimesta sopimismenettelyn aluksi asetettava tilaan:

SSC:n alkutila: Rnd3 (4 vähiten merkitsevää tavua) || Rnd1 (4 vähiten merkitsevää tavua).

CSM_030 Lähetysvaihelaskurin arvo on lisättävä yhdellä joka kerran ennen viestin todennuksen tarkistussumman (MAC) laskemista (ts. SSC:n arvo ensimmäiselle komennolle on SSC:n alkutila +1 ja SSC:n arvo ensimmäiselle vastaukselle on SSC:n alkutila + 2).

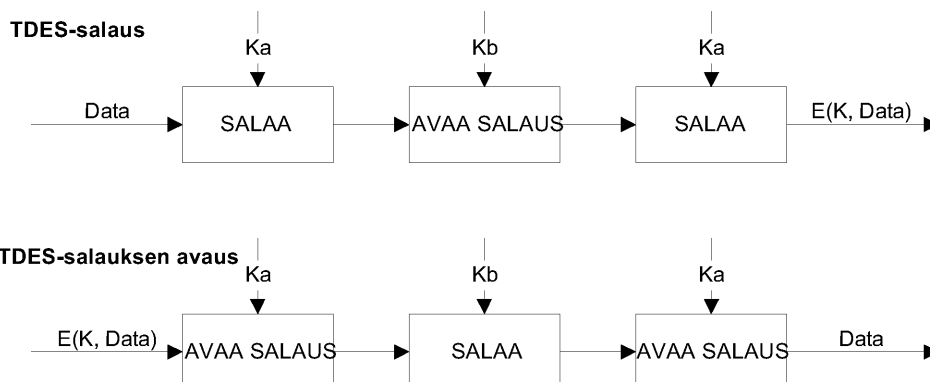
Seuraava kuva esittää retail MAC -tyyppisen viestin todennuksen tarkistussumman laskemista:



5.4 Algoritmi salattavien dataobjektien kryptogrammien laskemiseksi

CSM_031 Kryptogrammit lasketaan käyttäen viitteiden TDES ja TDES-OP mukaisesti kolminkertaista salausalgoritmia (TDEA) tilassa, jossa salauslohkot ketjutetaan (TCBC), ja siten, että ensimmäistä arvolohkoa edustaa nollavektori.

Seuraava kuva esittää avainten käyttöä TDES-salauksessa:



6. TIETOJEN KOPIOINNISSA KÄYTETTÄVÄT DIGITAALISET ALLEKIRJOITUSMEKANISMIT

CSM_032 Tietojen kopioimiseen ulkoisille tietovälineille tarkoitettu älykäs laite (IDE-laite) tallentaa laitteelta (ajoneuvoyksiköltä tai kortilta) yhden kopiointijakson aikana saadut tiedot yhteen fyysiseen tiedostoon. Tämän tiedoston on sisällettävä varmenteet MS₂C ja EQT.C. Tiedosto sisältää datalohkojen digitaaliset allekirjoitukset siten kuin lisäyksessä 7 (Tietojen kopiointiprotokollat) on määritelty.

CSM_033 Kopioitujen tietojen digitaalisissa allekirjoituksissa on noudatettava sellaista lisäyksellä täydennettyä digitaalisen allekirjoituksen muodostamistapaa, joka sallii tietojen lukemisen haluttaessa ilman salauksen avaamista.

6.1 Allekirjoituksen luominen

CSM_034 Tietojen allekirjoituksen luomisessa on noudatettava viitteessä PKCS1 määriteltyä liitteellä täydennettyä SHA-1 hajautusfunktiota käyttävää allekirjoituksen muodostamiskaaviota:

$$\text{Allekirjoitus} = \text{EQT.SK}[\text{'00' || '01' || PS || '00' || DER(SHA-1(Data))}]$$

PS = Arvoltaan 'FF' olevista tavuista muodostuva täyttömerkkijono, jolla pituus täydennetään 128 tavuksi.

DER(SHA-1(M)) on algoritmin tunnusteen koodaus Hash-hajautusfunktiota varten ja hajautusfunktion tuloksen koodaus ASN.1-standardin DigestInfo-datatyypin mukaiseksi (peruskoodaussäännöistä johdetut tiukemmat koodaussäännöt (DER, distinguished encoding rules)):

$$\text{'30' || '21' || '30' || '09' || '06' || '05' || '2B' || '0E' || '03' || '02' || '1A' || '05' || '00' || '04' || '14' || Hash-tulos.}$$

6.2 Allekirjoituksen todentaminen

CSM_035 Kopioitujen tietojen allekirjoituksen todentamisessa on noudatettava viitteessä PKCS1 määriteltyä liitteellä täydennettyä SHA-1-hajautusfunktiota käyttävää allekirjoituksen muodostamiskaaviota.

Todennuksen tekijän on erikseen tiedettävä Euroopan julkinen avain EUR.PK (ja luotettava siihen).

Seuraava kaavio kuvaa protokollaa, jota IDE-laite, johon on asetettu valvontakortti, voi noudattaa todentaakseen ulkoiselle tietovälineelle (ESM) tallennettujen tietojen eheyden. Valvontakorttia on käytetty purkamaan digitaalisten allekirjoitusten salaus. Tässä tapauksessa tätä toimintoa ei saa suorittaa IDE-laitteessa.

Analysoitavaa laitetta, josta tiedot on kopioitu ja joka on ne allekirjoittanut, kutsutaan lyhenteellä EQT.

