

32002R1360

2002 8 5

EUROPOS BENDRIJŲ OFICIALUSIS LEIDINYS

L 207/1

KOMISIJOS REGLAMENTAS (EB) Nr. 1360/2002**2002 m. birželio 13 d.****septintąjį kartą derinantis su technikos pažanga Tarybos reglamentą (EEB) Nr. 3821/85 dėl kelių transporto priemonėse naudojamų tachografų****(tekstas svarbus EEE)**

EUROPOS BENDRIJŲ KOMISIJA,

atsižvelgdama į Europos bendrijos steigimo sutartį,

atsižvelgdama į 1985 m. gruodžio 20 d. Tarybos reglamentą (EEB) Nr. 3821/85 dėl kelių transporto priemonėse naudojamų tachografų ⁽¹⁾ su paskutiniais pakeitimais, padarytais Reglamentu (EB) Nr. 2135/98 ⁽²⁾, ypač į jo 17 ir 18 straipsnius,

kadangi:

- (1) Reglamento (EEB) Nr. 3821/85 I priedo B dalies technines sąlygas reikia suderinti su technikos pažanga, ypač atkreipiant dėmesį į bendrą sistemos saugumą ir tachografų bei vairuotojo asmens kortelių suderinamumą.
- (2) Suderinant įrangą reikia suderinti ir Reglamento (EEB) Nr. 3821/85 II priedą, kuriame nustatyti patvirtinimo ženklas ir pažymėjimas.
- (3) Reglamento (EEB) Nr. 3821/85 18 straipsniu įkurtas komitetas nepareišė savo nuomonės dėl pasiūlyme pateiktų priemonių, todėl Komisija Tarybai pateikė pasiūlymą dėl šių priemonių.
- (4) Per Reglamento (EEB) Nr. 3821/85 18 straipsnio 5 dalies b punkte nustatytą laikotarpį Taryba nepriėmė jokio sprendimo, todėl priemonės turi patvirtinti Komisija,

PRIĖMĖ ŠĮ REGLAMENTĄ:

1 straipsnis

Reglamento (EEB) Nr. 2135/98 priedas pakeičiamas šio reglamento priedu.

2 straipsnis

Reglamento (EEB) Nr. 3821/85 II priedas iš dalies keičiamas taip:

1. I skyriaus, 1 dalies pirmoji pastraipa iš dalies keičiama taip:
 - Graikijos sutartinis ženklas „GR“ pakeičiamas „23“,
 - Airijos sutartinis ženklas „IRL“ pakeičiamas „24“,
 - įrašomas Austrijos sutartinis ženklas „12“,
 - įrašomas Suomijos sutartinis ženklas „17“,
 - įrašomas Švedijos sutartinis ženklas „5“.
2. I skyriaus, 1 dalies antroji pastraipa iš dalies keičiama taip:
 - po žodžių „registracijos lapo“ įrašomi žodžiai „arba tachografo kortelės“.
3. I skyriaus, 2 dalis iš dalies keičiama taip:
 - po žodžių „registracijos lapo“ įrašomi žodžiai „ir ant kiekvienos tachografo kortelės“.
4. II skyriuje prieš pavadinimo žodžius įrašomi žodžiai „I PRIEDO REIKALAVIMUS ATITINKANČIŲ GAMINIŲ“.

⁽¹⁾ OL L 370, 1985 12 31, p. 8.⁽²⁾ OL L 274, 1998 10 9, p. 1.

5. Pridedamas toks III skyrius:

„III. „I PRIEDO B DALIES REIKALAVIMUS ATITINKANČIŲ GAMINIŲ PATVIRTINIMO SERTIFIKATAS“

Patvirtinusi įrangą, valstybė išduoda pareiškėjui patvirtinimo sertifikatą, kurio pavyzdys yra pateikiamas toliau. Pranešdama kitoms valstybėms narėms apie patvirtinimą arba, jei taip atsitiktų, patvirtinimo panaikinimą, valstybė narė naudoja to sertifikato nuorašais.

I PRIEDO B DALIES REIKALAVIMUS ATITINKANČIŲ GAMINIŲ PATVIRTINIMO SERTIFIKATAS

Kompetentingos institucijos pavadinimas

Pranešimas dėl ⁽³⁾:

- ☐ tipo patvirtinimo
- ☐ tipo patvirtinimo panaikinimo
- ☐ tachografo modelio
- ☐ tachografo komponento ⁽⁴⁾
- ☐ vairuotojo asmens kortelės
- ☐ dirbtuvių kortelės
- ☐ įmonės kortelės
- ☐ kontrolieriaus kortelės

Patvirtinimo Nr.

1. Prekės ženklas ar pavadinimas
2. Modelio pavadinimas
3. Gamintojo pavadinimas
4. Gamintojo adresas
5. Pateikimo patvirtinti data
6. Laboratorija
7. Bandymo (-ų) data ir skaičius
8. Patvirtinimo data
9. Patvirtinimo panaikinimo data
10. Tachografo komponento (-ų), su kuriuo (su kuriais) numatyta komponentą naudoti
11. Vieta
12. Data
13. Pridėti aprašų dokumentai
14. Pastabos (ir antspaudų vieta, jei jie dedami)

(Parašas)

⁽³⁾ Pažymėti reikiamus langelius.

⁽⁴⁾ Nurodyti komponentą, apie kurį pranešama.“

3 straipsnis

Šis reglamentas įsigalioja dvidešimtą dieną po jo paskelbimo *Europos Bendrijų oficialiajame leidinyje*.

Šis reglamentas yra privalomas visas ir tiesiogiai taikomas visose valstybėse narėse.

Priimta Briuselyje, 2002 m. birželio 13 d.

Komisijos vardu
Loyola DE PALACIO
Pirmininko pavaduotoja

PRIEDAS

„I B PRIEDAS

GAMYBOS, BANDYMO, MONTAVIMO IR PATIKROS REIKALAVIMAI

TURINYS

I.	APIBRĖŽIMAI	286
II.	BENDROS TACHOGRAFO CHARAKTERISTIKOS IR FUNKCIJOS	290
1.	Bendrosios ypatybės	290
2.	Funkcijos	290
3.	Darbo režimai	291
4.	Apsauga	292
III.	TACHOGRAFO GAMINIMO IR JO VEIKIMO REIKALAVIMAI	292
1.	Kortelių įkišimo ir ištraukimo veiksmų stebėseną	292
2.	Greičio ir atstumo matavimas	292
2.1.	Nuvažiuto atstumo matavimas	293
2.2.	Greičio matavimas	293
3.	Laiko matavimas	293
4.	Vairuotojo veiklos stebėseną	294
5.	Važiavimo būsenos stebėseną	294
6.	Vairuotojo rankomis įvedami duomenys	294
6.1.	Vietų, kuriose prasideda ir (arba) baigiasi dienos darbo laikotarpiai, žymenų įvedimas	294
6.2.	Duomenų apie vairuotojo veiklą įvedamas rankomis	294
6.3.	Informacijos apie ypatingas būsenas įvedimas	296
7.	Įmonės užraktų valdymas	296
8.	Kontrolės veiklos stebėseną	296
9.	Įvykių ir (arba) gedimų aptikimas	296
9.1.	„Negaliojančios kortelės įkišimo“ įvykis	296
9.2.	„Kortelių nesuderinamumo“ įvykis	297
9.3.	„Dalinio laiko sutapimo“ įvykis	297
9.4.	„Važiavimo be tinkamos kortelės“ įvykis	297
9.5.	„Kortelės įkišimo važiuojant“ įvykis	297
9.6.	„Paskutinės kortelės panaudos netinkamo užbaigimo“ įvykis	297
9.7.	„Greičio viršijimo“ įvykis	297

9.8.	„Maitinimo nutrūkimo“ įvykis	298
9.9.	„Duomenų apie judėjimą klaidos“ įvykis	298
9.10.	„Duomenų apie judėjimą klaidos“ įvykis	298
9.11.	„Mėginimo pažeisti apsaugą“ įvykis	298
9.12.	„Tachografo“ gedimas	298
10.	Savidiagnostika ir savitikra	298
11.	Savidiagnostika ir savitikra	298
12.	Informacijos įrašymas ir laikymas duomenų atmintyje	299
12.1.	Įrangos identifikacijos duomenys	299
12.1.1.	Transporto priemonės bloko identifikacijos duomenys	299
12.1.2.	Judesio jutiklio identifikacijos duomenys	299
12.2.	Apsaugos elementai	300
12.3.	Duomenys apie vairuotojo kortelės įkišimą ir ištraukimą	300
12.4.	Duomenys apie vairuotojo veiklą	301
12.5.	Vietos, kur prasideda ir (arba) baigiasi dienos darbo laikotarpiai	301
12.6.	Hodometro duomenys	301
12.7.	Išsamūs duomenys apie greitį	301
12.8.	Duomenys apie įvykius	301
12.9.	Duomenys apie gedimus	303
12.10.	Duomenys apie kalibravimą	304
12.11.	Duomenys apie laiko koregavimą	304
12.12.	Duomenys apie kontrolės veiklą	304
12.13.	Duomenys apie įmonės užraktus	305
12.14.	Duomenys apie duomenų perkėlimo veiklą	305
12.15.	Duomenys apie ypatingas būsenas	305
13.	Tachografo kortelėse įrašytos informacijos nuskaitymas	305
14.	Informacijos įrašymas į tachografo korteles ir laikymas	305
15.	Rodymas ekrane	306
15.1.	Numatytasis rodinys	306
15.2.	Perspėjamasis rodinys	307
15.3.	Naudojimasis meniu	307
15.4.	Kiti rodiniai	307
16.	Spausdinimas	307
17.	Perspėjimai	308
18.	Duomenų perkėlimas į išorines laikmenas	309
19.	Duomenų persiuntimas į papildomus išorinius įtaisus	309
20.	Kalibravimas	310
21.	Laiko koregavimas	310

22.	Eksplotacinės savybės	310
23.	Medžiagos	310
24.	Ženklaai	311
IV.	TACHOGRAFO KORTELIŲ KONSTRUKCIJOS IR FUNKCINIAI REIKALAVIMAI	311
1.	Regimieji duomenys	311
2.	Apsauga	314
3.	Standartai	314
4.	Aplinkos ir elektros specifikacijos	314
5.	Duomenų laikymas	314
5.1.	Kortelės identifikacijos ir apsaugos duomenys	315
5.1.1.	Taikomosios programos identifikacija	315
5.1.2.	Mikroschemos identifikacija	315
5.1.3.	IC kortelės identifikacija	315
5.1.4.	Apsaugos elementai	315
5.2.	Vairuotojo kortelė	315
5.2.1.	Kortelės identifikacija	315
5.2.2.	Kortelės turėtojo identifikacija	316
5.2.3.	Informacija apie vairuotojo pažymėjimą	316
5.2.4.	Duomenys apie naudotas transporto priemones	316
5.2.5.	Duomenys apie vairuotojo veiklą	316
5.2.6.	Vietos, kur prasideda ir (arba) baigiasi dienos darbo laikotarpiai	317
5.2.7.	Duomenys apie įvykius	317
5.2.8.	Duomenys apie gedimus	318
5.2.9.	Duomenys apie kontrolės veiklą	318
5.2.10.	Duomenys apie kortelės panaudą	318
5.2.11.	Duomenys apie ypatingas būsenas	318
5.3.	Dirbtuvių kortelė	319
5.3.1.	Apsaugos elementai	319
5.3.2.	Kortelės identifikacija	319
5.3.3.	Kortelės turėtojo identifikacija	319
5.3.4.	Duomenys apie panaudotas transporto priemones	319
5.3.5.	Duomenys apie vairuotojo veiklą	319
5.3.6.	Vietos, kur prasideda ir (arba) baigiasi dienos darbo laikotarpiai	319
5.3.7.	Duomenys apie įvykius ir gedimus	319
5.3.8.	Duomenys apie kontrolės veiklą	319
5.3.9.	Duomenys apie kalibravimą ir laiko koregavimą	320
5.3.10.	Duomenys apie ypatingas būsenas	320
5.4.	Kontrolės kortelė.	320

5.4.1.	Kortelės identifikacija	320
5.4.2.	Kortelės turėtojo identifikacija	320
5.4.3.	Duomenys apie kontrolės veiklą	320
5.5.	Duomenys apie kontrolės veiklą	321
5.5.1.	Kortelės identifikacija	321
5.5.2.	Kortelės turėtojo identifikacija	321
5.5.3.	Duomenys apie įmonės veiklą	321
V.	TACHOGRAFO ĮRENGIMAS	321
1.	Įrengimas	321
2.	Įrengimo plokštelė	322
3.	Plombavimas	322
VI.	TIKRINIMAI, PATIKROS IR REMONTAS	323
1.	Montuotojų arba dirbtuvių patvirtinimas	323
2.	Naujų arba suremontuotų prietaisų patikrinimas	323
3.	Įrengimo patikra	323
4.	Periodinės patikros	323
5.	Paklaidų matavimas	324
6.	Remontas	324
VII.	KORTELĖS IŠDAVIMAS	324
VIII.	TACHOGRAFŲ IR TACHOGRAFO KORTELIŲ TIPO PATVIRTINIMAS	324
1.	Pagrindinės nuostatos	324
2.	Apsaugos pažymėjimas	325
3.	Veikimo pažymėjimas	325
4.	Funkcinio suderinamumo pažymėjimas	325
5.	Tipo patvirtinimo sertifikatas	326
6.	Išskirtinė tvarka: pirmieji funkcinio suderinamumo pažymėjimai	326
1 priedėlis.	Duomenų žodynėlis	
2 priedėlis.	Tachografo kortelių specifikacija	
3 priedėlis.	Piktogramos	
4 priedėlis.	Spaudiniai	
5 priedėlis.	Ekranas	
6 priedėlis.	Išorinės sąsajos	
7 priedėlis.	Duomenų perkėlimo protokolai	
8 priedėlis.	Kalibravimo protokolai	
9 priedėlis.	TIPO PATVIRTINIMAS. BŪTINIAUSIŲ BANDYMŲ SĄRAŠAS	
10 priedėlis.	BENDRIEJI APSAUGOS TIKSLAI	
11 priedėlis.	BENDRIEJI APSAUGOS MECHANIZMAI	

I. APIBRĖŽIMAI

Šiame priede:

a) „aktyvavimas“

tai etapas, kuriuo tachografas ima visiškai veikti ir atlieka visas funkcijas, įskaitant ir apsaugos;

tachografą galima aktyvuoti dirbtuvių kortele, įvedus PIN kodą;

b) „autentiškumo tikrinimas“

tai nurodytai tapatybei nustatyti ir patikrinti skirta funkcija;

c) „autentiškumas“

tai savybė, nurodanti, kad informaciją pateikusias šalies tapatybę galima patikrinti;

d) „saviagnostika“

tai pareikalavus atliekami patikrinimai, kuriuos atlikti nurodo operatorius arba išorinė įranga;

e) „kalendorinė diena“

tai laikas nuo 00.00 val. iki 24.00 val. Visos kalendorinės dienos nustatomos pagal UTC (visuotinį sukoordinuotąjį laiką);

f) „kalibravimas“

tai duomenų atmintyje laikomų transporto priemonės parametrų atnaujinimas arba patvirtinimas. Transporto priemonės parametrus sudaro jos identifikacija (TPIN, TPRN ir registruojančiosios valstybės narės žymuo) ir charakteristikos (w, k, l, padangų dydis, greičio ribotuvo nustatymas (jei yra), esamas UTC laikas, hodometro (kilometražo skaitiklio) rodmuo);

tachografui sukalibruoti reikia dirbtuvių kortelės;

g) „kortelės numeris“

tai unikalus 16 rašmenų numeris, kuris identifikuoja tachografo kortelę valstybėje narėje. Kortelės numerį sudaro kortelių numeracijos indeksas (jei naudojamas), pakeitimo indeksas ir atnaujinimo indeksas;

taigi kortelė identifikuojama ją išduodančios valstybės narės numeriu ir kortelės numeriu;

h) „kortelių numeracijos indeksas“

tai kortelės numerio 14 rašmenų segmentas, naudojamas skirtingoms įmonei ar institucijai, kurios turi teisę gauti keletą tachografo kortelių, išduodamoms kortelėms atskirti. Įmonei ar institucijai priskiriamas unikalus numeris, sudarantis pirmus 13 kortelės numerio rašmenų;

i) „kortelės atnaujinimo numeris“

tai kortelės numerio 16 rašmenų segmentas, didinamas kiekvienąsyk atnaujinus tachografo kortelę;

j) „kortelės pakeitimo numeris“

tai kortelės numerio 15 rašmenų segmentas, didinamas kiekvienąsyk pakeitus tachografo kortelę;

k) „transporto priemonės būdingasis koeficientas“

tai skaitmeninė charakteristika, nustatanti išėjimo signalo, skleidžiamo transporto priemonės sudedamosios dalies, kuria transporto priemonė yra sujungta su tachografu (pavarų dėžės išėjimo velenas arba ašis), vertę, kol įprastomis bandymo sąlygomis transporto priemonė nuvažiuoja vieną kilometrą (žr. VI skyriaus 5 poskyrį). Transporto priemonės būdingasis koeficientas yra išreiškiamas arba apsisukimais per kilometrą ($w = \dots$ aps./km), arba impulsais per kilometrą ($w = \dots$ imp./km);

l) **„įmonės kortelė“**

tai tachografo kortelė, kurią valstybės narės institucijos išduoda transporto priemonių su sumontuotu tachografu savininkui arba turėtojų;

įmonės kortelė leidžia tos įmonės užrakintame tachografe laikomus duomenis rodyti ekrane, juos perkelti ir spausdinti;

m) **„tachografo konstanta“**

tai skaitmeninė charakteristika, parodanti įvesties signalo vertę, reikalingą nuvažiuotam 1 km nuotoliui nustatyti ir užrašyti; ši konstanta turi būti išreikšta impulsais per kilometrą ($k = \dots \text{imp./km}$);

n) **„nepertraukiamo vairavimo trukmė“⁽¹⁾**

nepertraukiamo vairavimo trukmė apskaičiuojama kaip tam tikro vairuotojo esama bendroji vairavimo trukmė nuo paskutinio ne mažiau kaip 45 minučių trukmės BUVIMO PASIRENGUS DIRBTI, PERTRAUKOS/POILSIO arba NEŽINOMO⁽²⁾ laikotarpio (tas laikotarpis gali būti padalytas į keletą ne trumpesnių kaip 15 minučių atkarpų). Skaičiuojant atsižvelgiama į vairuotojo kortelės atmintyje įrašytus duomenis apie ankstesnę veiklą (jei reikia). Jeigu vairuotojas kortelės neįkiša, skaičiuojama remiantis įrašais atmintyje apie pastarąjį laikotarpį, kai kortelė nebuvo įkišta, susijusiais su atitinkamu plyšiu;

o) **„kontrolės kortelė“**

tai tachografo kortelė, kurią valstybių narių institucijos išduoda kompetentingoms kontrolės institucijoms;

kontrolės kortelė identifikuoja kontrolės instituciją (galbūt kontrolės pareigūną) ir leidžia skaityti, spausdinti ir (arba) perkelti duomenų atmintyje arba vairuotojo kortelės atmintyje esančius duomenis;

p) **„bendroji poilsio trukmė“⁽¹⁾**

bendroji poilsio trukmė apskaičiuojama kaip tam tikro vairuotojo esama bendroji ne mažiau kaip 15 minučių trukmės BUVIMO PASIRENGUS DIRBTI, PERTRAUKOS/POILSIO arba NEŽINOMO⁽²⁾ laikotarpio trukmė nuo paskutinio ne mažiau kaip 45 minučių trukmės BUVIMO PASIRENGUS DIRBTI, PERTRAUKOS/POILSIO arba NEŽINOMO⁽²⁾ laikotarpio (tas laikotarpis gali būti padalytas į keletą ne trumpesnių kaip 15 minučių atkarpų).

Skaičiuojant atsižvelgiama į vairuotojo kortelės atmintyje įrašytus duomenis apie ankstesnę veiklą (jei reikia). Skaičiuojant neatsižvelgiama į neigiamos trukmės nežinomus laikotarpius (nuo nežinomo laikotarpio pradžios iki jo pabaigos), susidarancius dėl dviejų skirtingų tachografų laiko dalinio sutapimo.

Jeigu vairuotojas kortelės neįkiša, skaičiuojama remiantis įrašais duomenų atmintyje apie pastarąjį laikotarpį, kai kortelė nebuvo įkišta, susijusiais su atitinkamu plyšiu;

q) **„duomenų atmintis“**

tai tachografe sumontuotas elektroninis duomenų laikymo įrenginys;

r) **„skaitmeninis parašas“**

prie duomenų paketo pridėti duomenys arba jo kriptografinė transformacija, leidžiantys duomenų paketo gavėjui įsitikinti duomenų paketo autentiškumu ir nepažeistumu;

s) **„duomenų perkėlimas“**

tai transporto priemonės arba tachografo kortelės atmintyje laikomų visų duomenų arba jų dalies kopijavimas kartu su skaitmeniniu parašu;

jokie laikomi duomenys juos perkeltiant negali būti pakeisti arba panaikinti;

⁽¹⁾ Šiuo būdu apskaičiuota nepertraukiamo vairavimo trukmė ir bendroji poilsio trukmė yra parametrai, pagal kuriuos tachografas apskaičiuoja perspėjimo dėl nepertraukiamo vairavimo trukmės parametą. Vien jais remiantis teisinių išvadų dėl minėtųjų trukmių daryti negalima.

⁽²⁾ NEŽINOMI laikotarpiai – tai tokie laikotarpiai, kai vairuotojo kortelė nebuvo įkišta į tachografą ir duomenys apie vairuotojo veiklą nebuvo įvesti rankomis.

t) **„vairuotojo kortelė“**

tai tachografo kortelė, kurią tam tikram vairuotojui išduoda valstybių narių institucijos;

vairuotojo kortelė identifikuoja vairuotoją ir yra skirta duomenims apie vairuotojo veiklą laikyti;

u) **„padangų efektyvusis apskritimo ilgis“**

tai atstumų, kuriuos nuvažiuoja vieną kartą visiškai apsisukdamas kiekvienas iš transporto priemonę varančių ratų (varantieji ratai), vidurkis. Šie atstumai turi būti išmatuoti standartinėmis bandymo sąlygomis (žr. VI skyriaus 5 poskyrį) ir yra išreikšti „l = ... mm“. Transporto priemonių gamintojams leidžiama nustatyti šiuos atstumus teoriniu apskaičiavimu, kurį atliekant atsižvelgiama į parengtos važiuoti nepakrautos transporto priemonės didžiausią leistiną ašių apkrovą ⁽¹⁾. Tokio teorinio skaičiavimo metodiką patvirtina kompetentinga valstybės narės institucija;

v) **„įvykis“**

tai tachografo aptiktas neįprastas veikimas, kuris gali pasireikšti mėginant sukčiauti;

w) **„gedimas“**

tai tachografo aptiktas neįprastas veikimas, kuris gali pasireikšti įrangai sutrikus ar sulūžus;

x) **„įrengimas“**

tai tachografo sumontavimas transporto priemonėje;

y) **„judesio jutiklis“**

tai tachografo dalis, siunčianti signalus, atitinkančius transporto priemonės greitį ir (arba) nuvažiuotą atstumą;

z) **„negaliojanti kortelė“**

tai sugedusi, po pirminio autentiškumo tikrinimo neleistina kortelė arba kortelė, kurios galiojimo laikas dar neprasidėjo arba jau baigėsi;

aa) **„nekontroliuojama“**

kai pagal Tarybos reglamento (EEB) Nr. 3820/85 nuostatas tachografo naudoti nereikalaujama;

bb) **„greičio viršijimas“**

tai leistino transporto priemonės greičio viršijimas, apibrėžiamas kaip bet kuris ilgiau kaip 60 sekundžių trukmės laikotarpis, kuriuo išmatuotas transporto priemonės greitis viršija greičio ribotuvo, nurodyto 1992 m. vasario 10 d. Tarybos direktyvoje 92/6/EEB dėl tam tikrų kategorijų variklinių transporto priemonių greičio ribotuvų įrengimo ir naudojimo Bendrijoje ⁽²⁾, nustatytą vertę;

cc) **„periodinė patikra“**

tai operacijų kompleksas, kurios atliekamos patikrinti, ar tachografas veikia tinkamai ir ar jo nustatymai atitinka transporto priemonės parametrus;

dd) **„spausdintuvas“**

tai tachografo komponentas, kuris spausdina spaudinius su laikomais duomenimis;

ee) **„tachografas“**

tai visa įranga, skirta įrengti transporto priemonėse automatiškai arba pusiau automatiškai rodyti, registruoti ir laikyti išsamią informaciją apie šių transporto priemonių judėjimą ir tam tikrus jų vairuotojų darbo laikotarpius;

⁽¹⁾ 1997 m. liepos 22 d. Direktyva 97/27/EB dėl tam tikrų kategorijų transporto priemonių ir jų priekabų masės bei matmenų ir iš dalies keičianti Direktyvą 70/156/EEB (OL L 233, 1997 8 25, p. 1).

⁽²⁾ OL L 57, 1992 3 2, p. 27.

ff) „atnaujinimas“

tai naujos tachografo kortelės išdavimas pasibaigus galioti arba sugedus senajai ir ją atidavus išduodančiajai institucijai. Atnaujinimas garantuoja, kad vienu metu nebus dviejų galiojančių kortelių;

gg) „remontas“

tai bet koks judesio jutiklio arba transporto priemonės remontas, dėl kurio reikia išjungti jo maitinimą arba atjungti kitus tachografo komponentus ar jį atidaryti;

hh) „pakeitimas“

tai naujos tachografo kortelės išdavimas vietoj senosios, kuri paskelbta pamesta, pavogta ar sugedusia ir nėra grąžinta išduodančiajai institucijai. Pakeitimas niekuomet negarantuoja, kad vienu metu nebus dviejų galiojančių kortelių;

ii) „apsaugotumo atestacija“

tai ITSEC ⁽¹⁾ atestacijos institucijos atliekamas procesas, kuriuo tikrinama, ar tachografas arba tachografo kortelė atitinka 10 priedėlyje „Bendrieji apsaugos tikslai“ nustatytus apsaugotumo reikalavimus;

jj) „savitikra“

tai tachografo periodiškai ir automatiškai atliekami sutrikimų patikrinimai;

kk) „tachografo kortelė“

kortelė, turinti mikroprocesorių, skirta naudoti su tachografu. Iš tachografo kortelių tachografas gali nustatyti kortelės turėtojo tapatybę (arba tapatybės grupę), į kortelę galima perrašyti ir laikyti duomenis. Tachografo kortelės būna tokios:

- vairuotojo kortelė,
- kontrolės kortelė,
- dirbtuvių kortelė,
- įmonės kortelė;

ll) „tipo patvirtinimas“

tai valstybės narės atliekamas procesas, kuriuo tikrinama, ar tachografas (ar jo komponentas) arba tachografo kortelė atitinka šio reglamento reikalavimus;

mm) „padangų dydis“

tai (išorinių varančiųjų ratų) padangų matmenų nuoroda pagal 1992 m. kovo 31 d. Direktyvą 92/23/EEB ⁽²⁾;

nn) „transporto priemonės identifikacija“

transporto priemonės identifikacijos numeriai: transporto priemonės registracijos numeris (TPRN) su registruojančiosios valstybės narės žymeniu ir transporto priemonės identifikacijos numeris (TPIN) ⁽³⁾;

oo) „transporto priemonės blokas (TPB)“

tai tachografas be judesio jutiklio ir jo jungiamųjų laidų. Transporto priemonės blokas gali būti vienas arba jų gali būti keli, paskirstyti visoje transporto priemonėje ir būtina atitinkantys šio reglamento apsaugotumo reikalavimus;

⁽¹⁾ 1995 m. balandžio 7 d. Tarybos rekomendacija 95/144/EB dėl bendrųjų informacinės technologijos saugumo vertinimo kriterijų (OL L 93, 1995 4 26, p. 27).

⁽²⁾ OL L 129, 1992 5 14, p. 95.

⁽³⁾ 1975 m. gruodžio 18 d. Direktyva 76/114/EEB dėl valstybių narių įstatymų, susijusių su variklinių transporto priemonių ir jų priekabų valstybinių registracijos numerių plokštelėmis ir įrašais jose, derinimo (OL L 24, 1976 1 30, p. 1).

pp) „savaitė“

(tachografo skaičiavimams) tai laikotarpis nuo pirmadienio 00.00 val. iki sekmadienio 24.00 val. pagal UTC;

qq) „dirbtuvių kortelė“

tai tachografo kortelė, kurią valstybės narės institucijos išduoda tos valstybės narės patvirtintam tachografo gamintojui, montuotojui, transporto priemonės gamintojui ar dirbtuvėms.

Dirbtuvių kortelė identifikuoja jos turėtoją ir leidžia tikrinti, kalibruoti ir (arba) perkelti duomenis iš tachografo.

II. BENDROS TACHOGRAFO CHARAKTERISTIKOS IR FUNKCIJOS

000 Bet kurioje transporto priemonėje, kurioje įmontuotas šio priedo nuostatas atitinkantis tachografas, turi būti greičio rodmenų ekranas ir hodometras. Jie gali būti įmontuoti pačiame tachografe.

1. Bendrosios ypatybės

Tachografas skirtas įrašyti, laikyti, rodyti, spausdinti ir pateikti su vairuotojo veikla susijusius duomenis.

001 Tachografas susideda iš laidų, judesio jutiklio ir transporto priemonės bloko.

002 Transporto priemonės bloke yra procesorius, duomenų atmintis ir laikrodis, du kortelės su mikroprocesoriumi sąsajos įtaisai (vairuotojo ir vairuotojo porininko), spausdintuvas, ekranas, vaizdinio perspėjimo įtaisas, kalibravimo ar duomenų perkėlimo jungtis ir įtaisai naudotojo informacijai įvesti.

Tachografas per papildomas jungtis gali būti prijungtas prie kitų įrenginių.

003 Prijungti arba įdiegti į tachografą bet kokias patvirtintas ar kitokias funkcijas, įtaisą ar įtaisy leidžiama tik tuomet, jei jie netrukdo ir negali sutrukdyti įrangai tinkamai bei saugiai veikti ir atitikti šio reglamento reikalavimus.

Tachografo naudotojų tapatybė nustatoma iš tachografo kortelių.

004 Tachografas suteikia atrankinės prieigos teises naudotis duomenimis ir funkcijomis pagal naudotojo tipą ir (arba) tapatybę.

Tachografas įrašo ir laiko duomenis savo duomenų atmintyje ir tachografo kortelėse.

Tai daroma pagal 1995 m. spalio 24 d. Direktyvą 95/46/EB dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ⁽¹⁾.

2. Funkcijos

005 Tachografas turi atlikti tokias funkcijas:

- stebėti kortelių įkišimo ir ištraukimo veiksmus,
- matuoti greitį ir atstumą,
- matuoti laiką (trukmę),
- stebėti vairuotojo veiklą,
- stebėti važiavimo būseną,
- leisti vairuotojui rankomis įvesti tokius duomenis:
 - vietų, kuriose prasideda ir (arba) baigiasi dienos darbo laikotarpiai, žymenis,
 - rankomis įvedamus duomenis apie vairuotojo veiklą,
 - apie ypatingas būsenas,

⁽¹⁾ OL L 281, 1995 11 23, p. 31.

- valdyti įmonės užraktus,
- stebėti kontrolės veiklą,
- aptikti įvykius ir (arba) gedimus,
- savidiagnostiką ir savitikrą,
- nuskaityti duomenų atmintyje laikomą informaciją,
- įrašyti ir laikyti informaciją duomenų atmintyje,
- nuskaityti tachografo kortelėse įrašytą informaciją,
- įrašyti ir laikyti informaciją tachografo kortelėse,
- rodyti ekrane,
- spausdinti,
- perspėti,
- perkelti duomenis į išorines laikmenas,
- persiųsti duomenis į papildomus išorinius įtaisus,
- kalibruoti,
- koreguoti laiką.

3. Darbo režimai

006 Tachografas turi dirbti keturiais darbo režimais:

- naudojimo režimu,
- kontrolės režimu,
- kalibravimo režimu,
- įmonės režimu.

007 Priklausomai nuo to, kokia galiojanti tachografo kortelė įkišama į kortelių sąsajos įtaisus, tachografas turi persijungti į tokius darbo režimus:

Darbo režimas		Vairuotojo plyšys				
		Kortelės nėra	Vairuotojo kortelė	Kontrolės kortelė	Dirbtuvių kortelė	Įmonės kortelė
Potrininko plyšys	Kortelės nėra	Naudojimo	Naudojimo	Kontrolės	Kalibravimo	Įmonės
	Vairuotojo kortelė	Naudojimo	Naudojimo	Kontrolės	Kalibravimo	Įmonės
	Kontrolės kortelė	Kontrolės	Kontrolės	Kontrolės (*)	Naudojimo	Naudojimo
	Dirbtuvių kortelė	Kalibravimo	Kalibravimo	Naudojimo	Kalibravimo (*)	Naudojimo
	Įmonės kortelė	Įmonės	Įmonės	Naudojimo	Naudojimo	Įmonės (*)

008 (*) Tokiais atvejais tachografas naudoja tik į vairuotojo plyšį įkištą kortelę.

- 009 Tachografas turi nepaisyti įkištų negaliojančių kortelių; galima tik pamatyti, išspausdinti ir perkelti informaciją iš kortelių, kurių galiojimo laikas pasibaigęs.
- 010 Visos II skyriaus 2 poskyryje išvardytos funkcijos turi veikti bet kuriuo darbo režimu, išskyrus tokius atvejus:
- kalibravimo funkcija galima naudotis tik kalibravimo režimu,
 - laiko nustatymo funkcija ne kalibravimo režimu yra apribota,
 - rankinio vairuotojo informacijos duomenų įvedimo funkcija veikia tik naudojimo ir kalibravimo režimais,
 - įmonės užrakto valdymo funkcija galima naudotis tik įmonės režimu,
 - kontrolės veiklos stebėsenos funkcija galima naudotis tik kontrolės režimu,
 - duomenų perkėlimo funkcija neveikia naudojimo režimu (išskyrus 150 reikalavime numatytus atvejus).
- 011 Tachografas turi gebėti išvesti duomenis į ekraną, spausdintuvą ar išorines sąsajas, išskyrus tokius atvejus:
- naudojimo režimu bet kokia įkištos tachografo kortelės neatitinkanti asmens tapatybės informacija (pavardė ir vardas) užtamsinama, o įkištos tachografo kortelės numerio neatitinkantis numeris užtamsinamas iš dalies (užtamsinamas kiekvienas lyginis rašmuo skaičiuojant iš kairės į dešinę),
 - įmonės režimu gali būti išvesti tik kitų įmonių (identifikuojamų pagal pirmuosius 13 įmonės kortelės numerio rašmenų) neužrakintų laikotarpių su vairuotoju susiję duomenys (081, 084 ir 087 reikalavimai),
 - kai į tachografą neįkišta jokia kortelė, gali būti išvesti tik esamos ir aštuonių ankstesnių kalendorinių dienų su vairuotoju susiję duomenys.

4. Apsauga

Sistemos apsauga skirta apsaugoti duomenų atmintį taip, kad prie jų negalima būtų neleistinai prieiti ir jais pasinaudoti, aptikti bet kokius mėginimus tai padaryti, saugoti tarp judesio jutiklio bei transporto priemonės bloko ir tarp tachografo bei tachografo kortelių perduodamų duomenų nepažeistumą ir autentiškumą bei tikrinti perkeliamų duomenų nepažeistumą ir autentiškumą.

- 012 Tam, kad sistema būtų saugi, tachografas turi atitikti judesio jutiklio ir transporto priemonės bloko bendruosiuose apsaugos tiksluose (10 priedėlis) nurodytus reikalavimus.

III. TACHOGRAFO GAMINIMO IR JO VEIKIMO REIKALAVIMAI

1. Kortelių įkišimo ir ištraukimo veiksmų stebėseną

- 013 Tachografas turi stebėti kortelių sąsajos įrangą ir registruoti kortelių įkišimo ir ištraukimo veiksmus.
- 014 Įkišus kortelę tachografas turi nustatyti, ar įkištoji kortelė yra galiojanti tachografo kortelė, ir jei taip – nustatyti jos rūšį.
- 015 Tachografas turi būti tokios konstrukcijos, kad tinkamai įkišus kortelę į sąsajos įtaisą, ji būtų užfiksuojama.
- 016 Tachografo kortelės gali būti išvedamos iš įrangos tik transporto priemonei sustojus ir įrašius į jas reikiamus duomenis. Kortelė turi būti išvedama naudotojo veiksmu.

2. Greičio ir atstumo matavimas

- 017 Ši funkcija turi nuolatos matuoti bendrą transporto priemonės nuvažiuotą atstumą ir gebėti pateikti hodometro vertės rodmenį.
- 018 Ši funkcija turi nuolatos matuoti transporto priemonės greitį ir gebėti pateikti jo vertės rodmenį.

- 019 Greičio matavimo funkcija taip pat turi pateikti informaciją apie tai, ar transporto priemonė juda, ar stovi. Transporto priemonė laikoma judančia, jei funkcija bent penkias sekundes gauna didesnę kaip 1 imp./s dažnio signalą iš judesio jutiklio; priešingu atveju transporto priemonė laikoma stovinčia.

Bet kurioje transporto priemonėje esantys greitį rodantys įtaisai (spidometrai) ir nuvažiuotą atstumą rodantys įtaisai (hodometrai), sumontuoti šio reglamento nuostatas atitinkančiuose tachografuose, turi atitikti reikalavimus dėl didžiausių leistinų paklaidų, nustatytų šiame priede (III skyriaus 2 poskyrio 1 ir 2 punktuose).

2.1. Nuvažiuoto atstumo matavimas

- 020 Nuvažiuotas atstumas gali būti matuojamas:
- įskaičiuojant į priekį ir atbulomis nuvažiuotą atstumą,
 - įskaičiuojant tik į priekį nuvažiuotą atstumą.
- 021 Tachografas turi matuoti atstumą nuo 0 iki 9 999 999,9 km.
- 022 Atstumas turi būti matuojamas su tokia paklaida (ne mažiau kaip 1 000 m atstumas):
- iki sumontavimo: $\pm 1 \%$,
 - sumontavus ir atliekant periodines patikras: $\pm 2 \%$,
 - naudojant: $\pm 4 \%$.

- 023 Atstumas turi būti matuojamas 0,1 km ar smulkesniais vienetais.

2.2. Greičio matavimas

- 024 Tachografas turi matuoti nuo 0 iki 220 km/h greitį.
- 025 Tam, kad būtų matuojama ne daugiau kaip su ± 6 km/h paklaida, ir atsižvelgiant į:
- ± 2 km/h įvesties duomenų (skirtingos padangos ir kt.) paklaidą,
 - ± 1 km/h matavimų įrengiant arba atliekant periodines patikras paklaidą,
- kai transporto priemonės būdingasis koeficientas yra nuo 4 000 iki 25 000 imp./km, tachografas turi matuoti nuo 20 iki 180 km/h greitį su ± 1 km/h paklaida.

Pastaba: dėl duomenų laikymo įrangos tikslumo galima papildoma $\pm 0,5$ km/h tachometre registruojamo greičio paklaida.

- 025a Greitis turi būti teisingai išmatuojamas su leistina paklaida ne vėliau kaip praėjus 2 sekundėms po greičio kaitos pabaišos, kai jis pasikeičia iki 2 m/s^2 sparta.
- 026 Greitis turi būti matuojamas 1 km/h ar didesniu tikslumu.

3. Laiko matavimas

- 027 Laikas turi būti matuojamas nuolatos ir skaitmeniniu būdu parodoma data bei laikas pagal UTC.
- 028 Visoje tachografo sistemoje (įrašuose, spaudiniuose, keičiantis duomenimis, ekrane ir kt.) data turi būti registruojama pagal UTC datą ir laiką.
- 029 Vietos laikui nustatyti turi būti įmanoma pakeisti rodomą laiką pusės valandos žingsniais.
- 030 Tipo patvirtinimo sąlygomis laiko matavimo paklaida gali būti ne didesnė kaip ± 2 s.
- 031 Laikas turi būti matuojamas 1 sekundės ar didesniu tikslumu.
- 032 Laiko matavimo tipo patvirtinimo sąlygomis neturi sutrikdyti išorinio maitinimo nebuvimas trumpesnę kaip 12 mėnesių laiką.

4. Vairuotojo veiklos stebėseną

- 033 Ši funkcija nuolatos ir atskirai turi stebėti vieno vairuotojo ir vieno vairuotojo porininko veiklą.
- 034 Vairuotojo veiklos rūšys turi būti tokios: VAIRAVIMAS, DARBAS, BUVIMAS PASIRENGUS DIRBTI ir PERTRAUKA/POILSIS.
- 035 Vairuotojui ir (arba) vairuotojui porininkui turi būti įmanoma rankomis pasirinkti DARBA, BUVIMĄ PASIRENGUS DIRBTI ir PERTRAUKĄ/POILSĮ.
- 036 Kai transporto priemonė važiuoja, vairuotojui turi būti automatiškai parenkama VAIRAVIMO veiklos rūšis, o vairuotojui porininkui – BUVIMO PASIRENGUS DIRBTI.
- 037 Kai transporto priemonė sustoja, vairuotojui turi būti automatiškai parenkama DARBO veiklos rūšis.
- 038 Pirmasis veiklos pasikeitimas ne vėliau kaip praėjus 120 sekundžių po automatinio pasikeitimo į DARBA dėl to, kad transporto priemonė sustoja, turi būti laikomas įvykusi transporto priemonei stovint (todėl galbūt atšaukiamas DARBO veiklos rūšies nustatymas).
- 039 Ši funkcija turi teikti informaciją apie veiklos pasikeitimus registravimo funkcijoms vienos minutės tikslumu.
- 040 Jei kuriuo nors kalendorinės minutės momentu imama vykdyti VAIRAVIMO veiklą, VAIRAVIMU turi būti laikoma visa ta minutė.
- 041 Jei prieš tam tikrą minutę buvusią ir po jos einančią minutėmis buvo vykdoma VAIRAVIMO veikla, visa ta minutė turi būti laikoma VAIRAVIMU.
- 042 Jei pagal pirmiau nurodytus reikalavimus kalendorinė minutė nelaikoma VAIRAVIMU, ji turi būti laikoma tos rūšies veikla, kuri tą minutę truko ilgiausiai (arba vėliausiaja iš vienodai trukusių veiklų).
- 043 Ši funkcija taip pat nuolatos turi stebėti vairuotojo nepertraukiamo vairavimo trukmę ir bendrąją poilsio trukmę.

5. Važiavimo būsenos stebėseną

- 044 Ši funkcija nuolatos automatiškai turi stebėti važiavimo būseną.
- 045 Kai į įrangą įkišamos dvi galiojančios vairuotojo kortelės, turi būti parenkama ĮGULOS važiavimo būseną, visais kitais atvejais – VIENO VAIRUOTOJO važiavimo būseną.

6. Vairuotojo rankomis įvedami duomenys

6.1. Vietų, kuriose prasideda ir (arba) baigiasi dienos darbo laikotarpiai, žymenų įvedimas

- 046 Naudojantis šia funkcija turi būti galima įvesti vietų, kuriose prasideda ir (arba) baigiasi vairuotojo ir (arba) vairuotojo porininko dienos darbo laikotarpiai, žymenis.
- 047 Vietos apibrėžiamos kaip šalys ir, jei reikia papildomai, kaip regionai.
- 048 Ištraukiant vairuotojo (arba dirbtuvių) kortelę, tachografas turi pasiūlyti vairuotojui (porininkui) įvesti „vietą, kurioje baigėsi dienos darbo laikotarpis“.
- 049 Tachografas turi leisti ignoruoti šį siūlymą.
- 050 Vietų, kuriose prasideda ir (arba) baigiasi dienos darbo laikotarpiai, žymenis įvesti turi būti įmanoma ir be kortelės arba kitu laiku, o ne įkišant arba ištraukiant kortelę.

6.2. Duomenų apie vairuotojo veiklą įvedamas rankomis

- 050a Įkišus vairuotojo (arba dirbtuvių) kortelę (ir tik tuo metu) tachografas turi:
- priminti kortelės turėtojų paskutinio kortelės ištraukimo datą ir laiką,
 - paprašyti kortelės turėtoją nurodyti, ar įkišus kortelę turi būti pratęstas dienos darbo laikotarpis.

Tachografas turi leisti neatsakyti į šį klausimą, atsakyti teigiamai arba neigiamai:

- jei kortelės turėtojas neatsako į klausimą, tachografas turi pasiūlyti įvesti „vietos, kurioje prasideda dienos darbo laikotarpis, žymenį“. Tachografas turi leisti ignoruoti šį siūlymą. Jei vietos žymuo įvedamas, tuomet jis turi būti užregistruotas duomenų atmintyje bei tachografo kortelės atmintyje ir susietas su kortelės įkišimo laiku,
- jei atsakoma teigiamai arba neigiamai, tachografas turi pasiūlyti kortelės turėtojui rankomis įvesti veiklos pavadinimą (DARBAS, BUVIMAS PASIRENGUS DIRBTI arba PERTRAUKA/POILSIS), datą ir pradžios bei pabaigos laiką apsiribojant tik laikotarpiu nuo paskutinio kortelės ištraukimo iki dabartinio įkišimo ir neleidžiant skirtingų rūšių veiklos trukmei iš dalies sutapti. Tai daroma laikantis tokios tvarkos:
 - jei kortelės turėtojas klausimą atsako teigiamai, tachografas turi pasiūlyti kortelės turėtojui rankomis chronologine seka įvesti laikotarpį nuo paskutinio kortelės ištraukimo iki dabartinio įkišimo vykdytos veiklos pavadinimus. Procesas baigiasi, kai rankomis įvestos veiklos pabaigos laikas sutampa su kortelės įkišimo laiku,
 - jei kortelės turėtojas klausimą atsako neigiamai, tachografas turi:

Pastabos: jei kortelės turėtojas nenurodo, kada baigėsi ankstesnis darbo laikotarpis ir rankomis įveda veiklos pavadinimą, kurios pabaigos laikas sutampa su kortelės įkišimo laiku, tachografas turi:

- daryti prielaidą, kad darbo laikotarpis baigėsi prasidėjus pirmajam POILSIO (arba likusiam NEŽINOMAM) laikotarpiui ištraukus kortelę arba ją ištraukiant (jei nėra įvestas poilsio laikotarpis ir nėra vienas laikotarpis nelieka NEŽINOMAS),
- daryti prielaidą, kad pradžios laikas sutampa su kortelės įkišimo laiku,
- atlikti toliau nurodytus žingsnius,
- tuomet, jei atitinkamo darbo laikotarpio pabaigos laikas skiriasi nuo kortelės ištraukimo laiko arba tuo metu nėra įvestas dienos darbo laikotarpio pabaigos vietos žymuo, pasiūlyti kortelės turėtojui „patvirtinti arba įvesti vietos, kurioje baigėsi dienos darbo laikotarpis, žymenį“ (tachografas turi leisti ignoruoti šį siūlymą). Jei vietos žymuo įvedamas, jis turi būti užregistruotas tik tachografo kortelės atmintyje ir tik tuomet, jei skiriasi nuo žymens, įvesto ištraukiant kortelę (jei tuomet žymuo buvo įvestas), ir susietas su darbo laikotarpio pabaigos laiku,
- tuomet pasiūlyti kortelės turėtojui įvesti esamo dienos darbo laikotarpio (arba su ta transporto priemone susijusios veiklos, jei šiuo laikotarpiu kortelės turėtojas anksčiau naudojo registracijos lapą) „pradžios laiką“ ir „vietos, kur prasideda dienos darbo laikotarpis, žymenį“ (tachografas turi leisti ignoruoti šį siūlymą). Jei vietos žymuo įvedamas, jis turi būti užregistruotas tik tachografo kortelės atmintyje ir susietas su darbo laikotarpio pradžios laiku. Jei šis pradžios laikas sutampa su kortelės įkišimo laiku, vietos žymuo taip pat užregistruojamas duomenų atmintyje,
- tuomet, jei pradžios laikas skiriasi nuo kortelės įkišimo laiko, pasiūlyti vairuotojui rankomis chronologine seka įrašyti veiklos rūšis nuo šio pradžios laiko iki kortelės įkišimo laiko. Procesas baigiasi, kai rankomis įvestos veiklos pabaigos laikas sutampa su kortelės įkišimo laiku,
- tuomet tachografas iki patvirtinimo pasirinkus specialią komandą turi leisti kortelės turėtojui pakeisti bet kurios rankomis įvestos veiklos rūšies pavadinimą, o patvirtinus – nebeleisti jokių pakeitimų,
- jei kortelės turėtojas atsako į pradinį klausimą ir neįveda įrašų apie veiklą, tachografas daro prielaidą, kad kortelės turėtojas ignoravo klausimą.

Viso proceso metu tachografas turi nebepriimti įrašų:

- jei su įrangos žmogaus-mašinos sąsaja nesąveikaujama ilgiau kaip vieną minutę (po 30 sekundžių perspėjant registruojamą ir galbūt girdimuojamą būdais),
 - ištraukus kortelę arba įkišus kito vairuotojo (ar dirbtuvių) kortelę,
 - transporto priemonei pradėjus važiuoti,
- ir patvirtinti jau įvestą informaciją.

6.3. Informacijos apie ypatingas būsenas įvedimas

050b Tachografas turi leisti vairuotojui esamuoju laiku įvesti informaciją apie tokias dvi ypatingas būsenas:

- NEKONTROLIUOJAMA (pradžia, pabaiga),
- KELTO PERKĖLA/GELEŽINKELIO PERVAŽA.

Pasirinkus būseną NEKONTROLIUOJAMA, būsenos KELTO PERKĖLA/GELEŽINKELIO PERVAŽA pasirinkti negalima.

Jei įkišama arba ištraukiama vairuotojo kortelė, būsena NEKONTROLIUOJAMA turi būti automatiškai užbaigta.

7. Įmonės užraktų valdymas

- 051 Ši funkcija turi leisti valdyti užraktus, kuriuos įmonė nustato, kad pati uždraustų sau įmonės režimu prieiti prie duomenų.
- 052 Įmonės užraktus sudaro pradžios data/laikas (užrakinimas) ir pabaigos data/laikas (atrakinimas), susieti su įmonės identifikacija, kurią apibrėžia įmonės kortelės numeris (užrakinant).
- 053 Užraktus galima „užrakinti“ ir „atrakinti“ tik esamuoju laiku.
- 054 Atrakinti turi galėti tik ta įmonė, kuri „užrakino“ (ką nurodo pirmieji 13 įmonės kortelės rašmenų), arba
- 055 kitai įmonei „užrakinus“ savo užraktą, ankstesnės įmonės užraktas turi būti automatiškai „atrakinamas“.
- 055a Jei įmonė užrakina naują užraktą, o ankstesnis užraktas buvo tos pačios įmonės, tuomet daroma prielaida, kad ankstesnis užraktas nebuvo „atrakintas“, ir jis lieka „užrakintas“.

8. Kontrolės veiklos stebėseną

- 056 Ši funkcija turi stebėti RODYMO EKRANE, SPAUSDINIMO, TPB ir kortelės DUOMENŲ PERKĖLIMO veiklą kontrolės režimu.
- 057 Ši funkcija taip pat turi stebėti GREIČIO VIRŠIJIMO KONTROLĖS veiklą kontrolės režimu. Greičio kontrolės pasireiškimu laikoma tai, kad kontrolės režimu į spausdintuvą arba ekraną pateikiamas „greičio viršijimo“ pranešimas arba iš TPB atminties perkeliama duomenys apie „įvykius ir gedimus“.

9. Įvykių ir (arba) gedimų aptikimas

- 058 Ši funkcija turi aptikti tokius įvykius ir (arba) gedimus:

9.1. „Negaliojančios kortelės įkišimo“ įvykis

- 059 Šis įvykis turi būti užfiksuojamas įkišus bet kokią negaliojančią kortelę ir (arba) pasibaigus įkištos kortelės galiojimo laikui.

9.2. „Kortelių nesuderinamumo“ įvykis

- 060 Šis įvykis turi būti užfiksuojamas, kai kartu įkišamos dvi kortelės, kurių derinio sankirta toliau esančioje lentelėje pažymėta X:

Kortelių nesuderinamumas		Vairuotojo plyšys				
		Kortelės nėra	Vairuotojo kortelė	Kontrolės kortelė	Dirbtuvių kortelė	Įmonės kortelė
Porininko plyšys	Kortelės nėra					
	Vairuotojo kortelė				X	
	Kontrolės kortelė			X	X	X
	Dirbtuvių kortelė		X	X	X	X
	Įmonės kortelė			X	X	X

9.3. „Dalinio laiko sutapimo“ įvykis

- 061 Šis įvykis turi būti užfiksuojamas, kai vairuotojo kortelės paskutinio ištraukimo data ir laikas, užfiksuoti kortelės atminyje, yra vėlesni už tachografo, į kurį kortelė įkišta, esamą datą ir laiką.

9.4. „Važiavimo be tinkamos kortelės“ įvykis

- 062 Šis įvykis turi būti užfiksuojamas, kai kartu įkišamos dvi kortelės, kurių derinio sankirta toliau esančioje lentelėje pažymėta X, ir kai vairuotojo veiklos rūšis pasikeičia į VAIRAVIMĄ arba esant VAIRAVIMO vairuotojo veiklai pasikeičia darbo režimas:

Kortelių nesuderinamumas		Vairuotojo plyšys				
		Kortelės nėra (arba ji yra negaliojanti)	Vairuotojo kortelė	Kontrolės kortelė	Dirbtuvių kortelė	Įmonės kortelė
Porininko plyšys	Kortelės nėra (arba ji yra negaliojanti)	X		X		X
	Vairuotojo kortelė	X		X	X	X
	Kontrolės kortelė	X	X	X	X	X
	Dirbtuvių kortelė	X	X	X		X
	Įmonės kortelė	X	X	X	X	X

9.5. „Kortelės įkišimo važiuojant“ įvykis

- 063 Šis įvykis turi būti užfiksuojamas, kai esant VAIRAVIMO vairuotojo veiklai į bet kurį plyšį įkišama tachografo kortelė.

9.6. „Paskutinės kortelės panaudos netinkamo užbaigimo“ įvykis

- 064 Šis įvykis turi būti užfiksuojamas, kai įkišus kortelę tachografas nustato, kad, nepaisant III skyriaus 1 poskyrio nuostatų, ankstesnė kortelės panauda užbaigta netinkamai (kortelė ištraukta nebaigus įrašyti į ją visų reikiamų duomenų). Šis įvykis fiksuojamas tik dėl vairuotojo ir dirbtuvių kortelių.

9.7. „Greičio viršijimo“ įvykis

- 065 Šis įvykis turi būti užfiksuojamas kiekvienąsyk viršijus greitį.

9.8. „Maitinimo nutrūkimo“ įvykis

- 066 Šis įvykis turi būti užfiksuojamas ne kalibravimo režimu, kai judesio jutiklio ir (arba) transporto priemonės bloko maitinimas nutrūksta ilgesniam kaip 200 milisekundžių laikui. Pertraukimo slenkstį nustato gamintojas. Šis įvykis neturi būti fiksuojamas dėl įtampos kritimo užvedant variklį.

9.9. „Duomenų apie judėjimą klaidos“ įvykis

- 067 Šis įvykis turi būti užfiksuojamas, kai nutrūksta įprastas duomenų srautas tarp judesio jutiklio ir transporto priemonės bloko ir (arba) įvykus duomenų vientisumo arba autentiškumo klaidai keičiantis duomenimis tarp judesio jutiklio ir transporto priemonės bloko.

9.10. „Mėginimo pažeisti apsaugą“ įvykis

- 068 Šis įvykis turi būti užfiksuojamas, kai ne kalibravimo režimu pakenkiama judesio jutiklio ir (arba) transporto priemonės mazgo apsaugotumui, kaip nurodyta šių komponentų bendruosiuose apsaugos tiksluose.

9.11. „Kortelės“ gedimas

- 069 Šis gedimas turi būti užfiksuojamas, kai naudojantis tachografo kortele ji sugenda.

9.12. „Tachografo“ gedimas

- 070 Šis gedimas turi būti užfiksuojamas, kai ne kalibravimo režimu įvyksta bet kuris šių gedimų:

- TPB vidinis gedimas,
- spausdintuvo gedimas,
- ekrano gedimas,
- duomenų perkėlimo sutrikimas,
- jutiklio gedimas.

10. Savidiagnostika ir savitikra

- 071 Tachografas turi pats aptikti gedimus atlikdamas savidiagnostiką ir savitikrą, kaip nurodyta lentelėje:

Tikrinamas poagregatis	Savitikra	Savidiagnostika
Programinė įranga		Nepažeistumas
Duomenų atmintis	Prieiga	Prieiga duomenų nepažeistumas
Kortelių sąsajos įtaisai	Prieiga	Prieiga
Klaviatūra		Rankinis patikrinimas
Spausdintuvas	(pagal gamintojo nustatymus)	Spaudinys
Ekranas		Vizualus patikrinimas
Duomenų perkėlimas (atliekama tik perkeliant duomenis)	Tinkamas veikimas	
Jutiklis	Tinkamas veikimas	Tinkamas veikimas

11. Nuskaitymas iš duomenų atminties

- 072 Tachografas turi gebėti nuskaityti bet kokius savo duomenų atmintyje laikomus duomenis.

12. Informacijos įrašymas ir laikymas duomenų atmintyje

Šiame poskyryje:

- „365 dienos“ – tai vairuotojo vidutinės veiklos transporto priemonėje 365 kalendorinės dienos. Vidutinė dienos veikla transporto priemonėje apibrėžiama pagal informaciją apie ne mažiau kaip šešis vairuotojus arba vairuotojus porininkus, šešis kortelių įkišimo ir ištraukimo ciklus ir 256 veiklos rūšių pasikeitimus. Taigi per „365 dienas“ iš viso apibūdinami 2 190 vairuotojų (porininkų), 2 190 kortelių įkišimo ir ištraukimo ciklų ir 93 440 veiklos rūšių pasikeitimų,
- jei nenurodyta kitaip, laikas registruojamas vienos minutės tikslumu,
- hodometro vertės registruojamos vieno kilometro tikslumu,
- greitis registruojamas 1 km/h tikslumu.

073 Duomenų atmintyje laikomiems tipo patvirtinimo sąlygomis neturi pakenkti išorinio maitinimo nebuvimas trumpiau nei 12 mėnesių.

074 Tachografas savo duomenų atmintyje turi gebėti netiesiogiai arba tiesiogiai registruoti tokią informaciją:

12.1. Įrangos identifikacijos duomenys

12.1.1. Transporto priemonės bloko identifikacijos duomenys

075 Tachografas turi gebėti laikyti savo atmintyje tokius transporto priemonės identifikacijos duomenis:

- gamintojo pavadinimą,
- gamintojo adresą,
- komponento šifrą,
- serijos numerį,
- programinės įrangos versijos numerį,
- programinės įrangos įdiegimo datą,
- įrangos pagaminimo datą,
- patvirtinimo numerį.

076 Transporto priemonės bloko identifikacijos duomenis visam laikui įrašo transporto priemonės bloko gamintojas, išskyrus programinės įrangos duomenis ir patvirtinimo numerį, kurie gali keistis atnaujinant programinę įrangą.

12.1.2. Judesio jutiklio identifikacijos duomenys

077 Judesio jutiklis savo atmintyje turi gebėti laikyti tokius identifikacijos duomenis:

- gamintojo pavadinimą,
- komponento šifrą,
- serijos numerį,
- patvirtinimo numerį,
- įterptojo apsaugos komponento vardą (pvz., vidinės mikroschemos (mikroprocesoriaus) komponento šifrą),
- operacinės sistemos vardą (pvz., programinės įrangos versijos numerį).

- 078 Judesio jutiklio identifikacijos duomenis jame visam laikui įrašo judesio jutiklio gamintojas.
- 079 Transporto priemonės blokas savo atmintyje turi gebėti registruoti ir laikyti tokius tuo metu su juo sujungto judesio jutiklio identifikacijos duomenis:
- serijos numerį,
 - patvirtinimo numerį,
 - pirmojo sujungimo datą.

12.2. *Apsaugos elementai*

- 080 Tachografas turi gebėti laikyti atmintyje tokius apsaugos elementus:

- europinį atvirąjį raktą,
- valstybės narės pažymėjimą,
- įrangos pažymėjimą,
- įrangos slaptojo raktą.

Tachografo apsaugos elementus į įrangą įdiegia transporto priemonės bloko gamintojas.

12.3. *Duomenys apie vairuotojo kortelės įkišimą ir ištraukimą*

- 081 Kiekvienu vairuotojo arba dirbtuvių kortelės įkišimo ir ištraukimo ciklu tachografas turi užregistruoti ir laikyti savo atmintyje:
- kortelės turėtojo pavardę ir vardą (-us), įrašytus kortelės atmintyje,
 - kortelės numerį, išduodančiosios valstybės narės žymenį ir kortelės galiojimo pabaigos datą, įrašytus kortelės atmintyje,
 - įkišimo datą ir laiką,
 - transporto priemonės hodometro rodmens vertę įkišant kortelę,
 - plyšio, į kurį kortelė įkišta, žymenį,
 - ištraukimo datą ir laiką,
 - transporto priemonės hodometro rodmens vertę ištraukiant kortelę,
 - tokią kortelės atmintyje įrašytą informaciją apie transporto priemonę, kuria anksčiau naudojosi vairuotojas:
 - TPRN ir registruojančiosios valstybės narės žymenį,
 - kortelės ištraukimo datą ir laiką,
 - ženklą, nurodantį, ar įkišęs kortelę jos turėtojas rankomis įvedė veiklos rūšis, ar ne.

- 082 Duomenų atmintis turi gebėti išlaikyti šiuos duomenis ne trumpiau kaip 365 dienas.

- 083 Kai duomenų kaupimo talpa išnaudojama, nauji duomenys turi būti rašomi ant seniausiųjų įrašų.

12.4. Duomenys apie vairuotojo veiklą

084 Pasikeitus vairuotojo ir (arba) vairuotojo porininko veiklai ir (arba) važiavimo būsenai ir (arba) įkišus arba ištraukus vairuotojo arba dirbtuvių kortelę, tachografas turi užregistruoti ir laikyti duomenų atmintyje:

- važiavimo būseną (ĮGULA, VIENAS VAIRUOTOJAS),
- plyšys (VAIRUOTOJO, VAIRUOTOJO PORININKO),
- kortelė atitinkamame plyšyje (ĮKIŠTA, NEĮKIŠTA) (žr. pastabą),
- veiklos rūšį (VAIRAVIMAS, BUVIMAS PASIRENGUS DIRBTI, DARBAS, PERTRAUKA/POILSIS),
- pasikeitimo datą ir laiką.

Pastaba: ĮKIŠTA reiškia, kad į plyšį įkišta galiojanti vairuotojo ar dirbtuvių kortelė. NEĮKIŠTA, priešingai, reiškia, kad į plyšį neįkišta galiojanti vairuotojo ar dirbtuvių kortelė (pvz., įkišta įmonės kortelė arba neįkišta jokia kortelė).

Pastaba: vairuotojo rankomis įvesta informacija apie veiklą duomenų atmintyje neregistruojama.

085 Duomenų atmintis turi gebėti išlaikyti duomenis apie vairuotojo veiklą ne trumpiau kaip 365 dienas.

086 Kai duomenų kaupimo talpa išnaudojama, nauji duomenis turi būti rašomi ant seniausiųjų įrašų.

12.5. Vietos, kur prasideda ir (arba) baigiasi dienos darbo laikotarpiai

087 Kiekvienąsyk vairuotojui (porininkui) įvedus vietos, kur prasideda ir (arba) baigiasi dienos darbo laikotarpis, žymenį, tachografas turi užregistruoti ir laikyti savo atmintyje:

- jei taikytina, vairuotojo (porininko) kortelės numerį ir išduodančiosios valstybės narės žymenį,
- įrašo datą ir laiką (arba su įrašu susijusią datą ir laiką, kai įrašoma įvedant rankomis),
- įrašo tipą (pradžią ar pabaigą, įrašo aplinkybės),
- įvestus šalies ir regiono žymenis,
- transporto priemonės hodometro rodmens vertę.

088 Duomenų atmintis turi gebėti išlaikyti duomenis apie laikotarpių pradžią ir (arba) pabaigą ne trumpiau kaip 365 dienas (darant prielaidą, kad vienas vairuotojas įrašo duomenis dukart per dieną).

089 Kai duomenų kaupimo talpa išnaudojama, nauji duomenys turi būti rašomi ant seniausiųjų įrašų.

12.6. Hodometro duomenys

090 Tachografas savo duomenų atmintyje turi užregistruoti hodometro rodmens vertę ir datą kiekvienos kalendorinės dienos vidurnaktį.

091 Duomenų atmintis turi gebėti išlaikyti hodometro vidurnakčio rodmens vertes ne trumpiau kaip 365 dienas.

092 Kai duomenų kaupimo talpa išnaudojama, nauji duomenys turi būti rašomi ant seniausiųjų įrašų.

12.7. Išsamūs duomenys apie greitį

093 Tachografas turi užregistruoti ir laikyti savo atmintyje ne mažiau kaip 24 valandų transporto priemonės judėjimo trukmės informaciją apie momentinį transporto priemonės greitį kiekvieną sekundę ir atitinkamą datą bei laiką.

12.8. Duomenys apie įvykius

Šiame punkte nurodytais tikslais laikas registruojamas vienos sekundės tikslumu.

094

Tachografas turi užregistruoti ir laikyti savo atmintyje tokius duomenis apie kiekvieną aptiktą įvykį pagal tokias duomenų laikymo taisykles:

Įvykis	Duomenų laikymo taisyklės	Apie kiekvieną įvykį užregistruojami duomenys
Kortelių nesuderinamumas	— 10 paskutinių įvykių.	— įvykio pradžios data ir laikas, — įvykio pabaigos data ir laikas, — nesuderinamų kortelių rūšis, numeriai ir išduodančioji valstybė narė.
Važiavimas be reikiamos kortelės	— ilgiausiai trukęs įvykis iš paskutinių 10 dienų, kuriomis jis įvyko, — penki ilgiausi įvykiai per 365 dienas.	— įvykio pradžios data ir laikas, — įvykio pabaigos data ir laikas, — įvykio pradžioje ir (arba) pabaigoje įkištos kortelės rūšis, numeris ir išduodančioji valstybė narė, — panašių įvykių tą dieną skaičius.
Kortelės įkišimas važiuojant	— ilgiausiai trukęs įvykis iš paskutinių 10 dienų, kuriomis jis įvyko.	— įvykio data ir laikas, — kortelės rūšis, numeris ir išduodančioji valstybė narė, — panašių įvykių tą dieną skaičius.
Paskutinė kortelės panauda netinkamai užbaigta	— 10 paskutinių įvykių.	— kortelės įkišimo data ir laikas, — kortelės rūšis, numeris ir išduodančioji valstybė narė, — paskutiniai nuo kortelės nuskaityti panaudos duomenys: — kortelės įkišimo data ir laikas, — TPRN ir registruojančioji valstybė narė.
Greičio viršijimas ⁽¹⁾	— svarbiausias įvykis iš paskutinių 10 dienų, kuriomis jis įvyko, — penki svarbiausi įvykiai per 365 dienas, — pirmasis po paskutinio kalibravimo įvykęs įvykis.	— įvykio pradžios data ir laikas, — įvykio pabaigos data ir laikas, — didžiausias įvykio metu išmatuotas greitis, — įvykio išmatuoto greičio aritmetinis vidurkis, — kortelės rūšis, numeris ir išduodančioji valstybė narė (jei taikytina), — panašių įvykių tą dieną skaičius.

Įvykis	Duomenų laikymo taisyklės	Apie kiekvieną įvykį užregistruojami duomenys
Maitinimo nutrūkimas ⁽²⁾	— ilgiausias įvykis iš paskutinių 10 dienų, kuriomis jis įvyko, — penki ilgiausi įvykiai per 365 dienas.	— įvykio pradžios data ir laikas, — įvykio pabaigos data ir laikas, — įvykio pradžioje ir (arba) pabaigoje įkištos kortelės rūšis, numeris ir išduodančioji valstybė narė, — panašių įvykių tą dieną skaičius.
Duomenų apie judėjimą klaida	— ilgiausiai trukęs įvykis iš paskutinių 10 dienų, kuriomis jis įvyko, — penki ilgiausiai trukę įvykiai per 365 dienas.	— įvykio pradžios data ir laikas, — įvykio pabaigos data ir laikas, — įvykio pradžioje ir (arba) pabaigoje įkištos kortelės rūšis, numeris ir išduodančioji valstybė narė, — panašių įvykių tą dieną skaičius.
Mėginimas pažeisti apsaugą	— 10 paskutinių kiekvienos rūšies įvykių.	— įvykio pradžios data ir laikas, — įvykio pabaigos data ir laikas (jei tinka), — įvykio pradžioje ir (arba) pabaigoje įkištos kortelės rūšis, numeris ir išduodančioji valstybė narė, — įvykio rūšis.

095

⁽¹⁾ Tachografas savo atmintyje taip pat registruoja ir laiko:

- paskutinės GREIČIO VIRŠIJIMO KONTROLĖS datą ir laiką,
- pirmojo greičio viršijimo po tos GREIČIO VIRŠIJIMO KONTROLĖS datą ir laiką,
- greičio viršijimo įvykių po paskutinės GREIČIO VIRŠIJIMO KONTROLĖS skaičių.

⁽²⁾ Šie duomenys gali būti užregistruoti tik vėl atsiradus maitinimui, laikas gali būti nurodytas minutės tikslumu.

12.9. Duomenys apie gedimus

Šiame punkte nurodytais tikslais laikas registruojamas vienos sekundės tikslumu.

096

Tachografas turi bandyti užregistruoti ir laikyti savo atmintyje tokius duomenis apie kiekvieną aptiktą gedimą pagal tokias duomenų laikymo taisykles:

Gedimas	Duomenų laikymo taisyklės	Apie kiekvieną gedimą užregistruojami duomenys
Kortelės gedimas	— 10 paskutinių vairuotojo kortelės gedimų.	— gedimo pradžios data ir laikas, — gedimo pabaigos data ir laikas, — kortelės rūšis, numeris ir išduodančioji valstybė narė.
Tachografo gedimai	— 10 paskutinių kiekvienos rūšies gedimų, — pirmasis gedimas po paskutinio kalibravimo.	— gedimo pradžios data ir laikas, — gedimo pabaigos data ir laikas, — gedimo rūšis, — gedimo pradžioje ir (arba) pabaigoje įkištos kortelės rūšis, numeris ir išduodančioji valstybė narė.

12.10. Duomenys apie kalibravimą

- 097 Tachografas turi užregistruoti ir laikyti savo atmintyje duomenis apie:
- žinomus kalibravimo parametrus aktyvavimo momentu,
 - patį pirmąjį kalibravimą atlikus jo aktyvavimą,
 - patį pirmąjį kalibravimą šioje transporto priemonėje (identifikuojamoje pagal jos TPIN),
 - penkis pastaruosius kalibravimus (jei per vieną kalendorinę dieną atliekami keli kalibravimai, užregistruojami duomenys tik apie paskutinį iš jų).
- 098 Turi būti registruojami tokie kiekvieno kalibravimo duomenys:
- kalibravimo tikslas (aktyvavimas, pirmasis įrengimas, įrengimas, periodinė patikra),
 - dirbtuvių pavadinimas ir adresas,
 - dirbtuvių kortelės numeris, kortelę išduodanti valstybė narė ir kortelės galiojimo pabaigos laikas,
 - transporto priemonės identifikacija,
 - atnaujinti arba patvirtinti parametrai: w, k, l, padangų dydis, greičio ribotuvo nustatymas, hodometro (rodmens sena ir nauja vertės), data ir laikas (sena ir nauja vertės).
- 099 Judesio jutiklio atmintyje turi būti registruojami ir laikomi tokie duomenys apie judesio jutiklio įrengimą:
- pirmas sujungimas su TPB (data, laikas, TPB patvirtinimo numeris, TPB serijos numeris),
 - paskutinis sujungimas su TPB (data, laikas, TPB patvirtinimo numeris, TPB serijos numeris).

12.11. Duomenys apie laiko koregavimą

- 100 Tachografas turi užregistruoti ir laikyti savo atmintyje duomenis apie:
- paskutinį laiko koregavimą,
 - paskutinius penkis didžiausius laiko koregavimus nuo paskutinio kalibravimo, atliktus kalibravimo režimu (f apibrėžimas).
- 101 Turi būti registruojami tokie duomenys apie laiko koregavimus:
- data ir laikas, sena vertė,
 - data ir laikas, nauja vertė,
 - dirbtuvių pavadinimas ir adresas,
 - dirbtuvių kortelės numeris, kortelę išduodanti valstybė narė ir kortelės galiojimo pabaigos laikas.

12.12. Duomenys apie kontrolės veiklą

- 102 Tachografas turi užregistruoti ir laikyti savo atmintyje tokius duomenis apie 20 pastarųjų kontrolės veiklą:
- kontrolės datą ir laiką,
 - kontrolės kortelės numerį ir ją išduodančios valstybės narės žymenį,
 - kontrolės rūšį (rodymas ekrane ir (arba) spausdinimas ir (arba) duomenų perkėlimas iš TPB ir (arba) duomenų perkėlimas iš kortelės).

- 103 Jei perkeliami duomenys, turi būti užregistruojamos pirmosios ir paskutiniosios dienų, kurių duomenys perkeliama, datos.

12.13. Duomenys apie įmonės užraktus

- 104 Tachografas turi užregistruoti ir laikyti savo atmintyje tokius duomenis apie 20 pastarųjų įmonės užraktų:

- užrakinimo datą ir laiką,
- atrakinimo datą ir laiką,
- įmonės kortelės numerį ir ją išduodančios valstybės narės žymenį,
- įmonės pavadinimą ir adresą.

12.14. Duomenys apie duomenų perkėlimo veiklą

- 105 Tachografas turi užregistruoti ir laikyti savo atmintyje tokius duomenis apie duomenų iš atminties perkėlimą į išorines laikmenas įmonės arba kalibravimo režimu:

- duomenų perkėlimo datą ir laiką,
- įmonės arba dirbtuvių kortelės numerį ir ją išduodančios valstybės narės žymenį,
- įmonės arba dirbtuvių pavadinimą ir adresą.

12.15. Duomenys apie ypatingas būsenas

- 105a Tachografas turi užregistruoti ir laikyti savo atmintyje tokius duomenis apie ypatingas būsenas:

- būsenos datą ir laiką,
- ypatingos būsenos rūšį.

- 105b Duomenų atmintis turi gebėti išlaikyti duomenis apie ypatingas būsenas ne trumpiau kaip 365 dienas (darant prielaidą, kad per dieną vidutiniškai pradedama ir baigiama viena būsena). Kai duomenų kaupimo talpa išnaudojama, nauji duomenys rašomi ant seniausiųjų įrašų.

13. Tachografo kortelėse įrašytos informacijos nuskaitymas

- 106 Tachografas turi gebėti nuskaityti iš tachografo kortelių informaciją, būtiną:

- kortelės rūšiai, turėtojai, anksčiau naudotai transporto priemonei, paskutinio kortelės ištraukimo datai bei laikui ir tuo metu pasirinktai veiklai nustatyti,
- patikrinti, ar paskutinė kortelės panauda buvo užbaigta tinkamai,
- vairuotojo nepertraukiamo vairavimo trukmei, bendrajai poilsio trukmei ir ankstesnės ir esamos savaitės bendrajai poilsio trukmei ir bendrajai vairavimo trukmei apskaičiuoti,
- prašomiems spaudiniams su vairuotojo kortelės atmintyje įrašytais duomenimis išspausdinti,
- duomenims perkelti iš vairuotojo kortelės į išorines laikmenas.

- 107 Įvykus nuskaitymo klaidai tachografas turi ne daugiau kaip tris kartus mėginti nuskaityti iš naujo, o jei tai nepavyksta – paskelbti kortelę sugedusia ir negaliojančia.

14. Informacijos įrašymas į tachografo korteles ir laikymas

- 108 Tik įkišus kortelę tachografas turi nustatyti vairuotojo arba dirbtuvių kortelės atmintyje „kortelės panaudos duomenis“.

- 109 Tachografas turi įrašyti į galiojančias vairuotojo, dirbtuvių ir (arba) kontrolės korteles visą kortelės turėtojų skirtą naują informaciją, susijusią su to laikotarpiu, kuriuo kortelė įkišta. Kortelėse laikomi duomenys nurodyti IV skyriuje.
- 109a Tachografas turi įrašyti į galiojančias vairuotojo ir (arba) dirbtuvių korteles jų turėtojų rankomis įvestus duomenis apie vairuotojo veiklą ir vietą (kaip nurodyta IV skyriaus 5.2.5 ir 5.2.6 papunkčiuose).
- 110 Tachografo kortelių duomenys turi būti atnaujinami taip, kad, kai reikia, ir atsižvelgiant kortelių duomenų kaupimo talpą, naujausi duomenys pakeistų seniausius.
- 111 Įvykus įrašymo klaidai tachografas turi ne daugiau kaip tris kartus mėginti įrašyti iš naujo, o jei tai nepavyksta — paskelbti kortelę sugedusia ir negaliojančia.
- 112 Prieš išvesdamas vairuotojo kortelę ir įrašęs joje visus reikiamus duomenis, tachografas turi perkrauti kortelės panaudos duomenis.

15. Rodymas ekrane

- 113 Ekranas turi būti ne mažiau kaip 20 rašmenų dydžio.
- 114 Rašmuo turi būti ne mažesnis kaip 5 mm aukščio ir 3,5 mm pločio.
- 114a Ekranas turi gebėti atvaizduoti ISO 8859 1 ir 7 dalyse nustatytus Lotynų 1 ir Graikų rašmenų rinkinius, kaip nurodyta 1 priedėlio 4 skyriuje „Rašmenų rinkiniai“. Ekrane rašmenys gali būti vaizduojami supaprastintai (pvz., rašmenys su kirčiais gali būti rašomi be kirčio ženklų arba vietoj mažųjų raidžių rašomos didžiosios).
- 115 Ekranas apšvietimas neturi akinti.
- 116 Rodmenys turi būti iš tachografo išorės.
- 117 Tachografas turi gebėti parodyti ekrane:
- numatytuosius duomenis,
 - perspėjimų informaciją,
 - informaciją, susijusią su naudojimosi meniu,
 - kitus naudotojo pageidaujamus duomenis.

Tachografo ekrane gali būti rodoma papildoma informacija, jei ji aiškiai atskiriama nuo pirmiau reikalaujamos informacijos.

- 118 Tachografo ekrane turi būti naudojamos 3 priedėlyje išvardytos piktogramos arba jų deriniai. Ekrane gali būti pateikiamos ir papildomos piktogramos bei jų deriniai, jei jie aiškiai atskiriami nuo pirmiau minėtų piktogramų ir jų derinių.
- 119 Transporto priemonėi judant ekranas turi būti visuomet įjungtas.
- 120 Tachografe gali būti rankomis arba automatiškai valdoma funkcija, IŠJUNGIANTI ekraną, kai transporto priemonė stovi.
- Rodymo ekrane formatas nurodytas 5 priedėlyje.

15.1. Numatytais rodinys

- 121 Kai nereikia rodyti jokios kitos informacijos, tachografas pagal nutylėjimą turi rodyti:
- vietos laiką (UTC laikas + vairuotojo nustatyta pokytis),
 - darbo režimą,
 - esamą vairuotojo veiklą ir esamą vairuotojo porininko veiklą,

- su vairuotoju susijusią informaciją:
 - jei esama veikla yra VAIRAVIMAS – jo nepertraukiamo vairavimo trukmę ir tuometinę bendrąją poilsio trukmę,
 - jei esama veikla yra ne VAIRAVIMAS – šios veiklos esamą trukmę (nuo jos pasirinkimo momento) ir tuometinę bendrąją poilsio trukmę,
- su vairuotoju porininku susijusią informaciją:
 - jo veiklos esama trukmę (nuo jos pasirinkimo momento).

- 122 Su kiekvienu vairuotojo susiję duomenys turi būti pateikiami aiškiai, paprastai ir nedviprasmiškai. Jeigu su vairuotoju ir vairuotoju porininku susijusios informacijos negalima parodyti vienu metu, tachografas pagal nutylėjimą turi rodyti su vairuotoju susijusią informaciją, o naudotojui yra leidžiama pasirinkti su vairuotoju porininku susijusios informacijos rodinį.
- 123 Jeigu dėl ekrano pločio pagal nutylėjimą negalima rodyti darbo režimo, tachografas trumpam turi parodyti naują darbo režimą, kai jis pasirenkamas.
- 124 Įkišus kortelę tachografas turi trumpam parodyti kortelės turėtojo pavardę (pavadinimą).
- 124a Kai pradedama būsena NEKONTROLIUOJAMA, tuomet numatytame rodinyje turi būti piktograma, žyminti, kad būsena pradėta (leidžiama tuo metu nerodyti vairuotojo veiklos).

15.2. *Perspėjamasis rodinys*

- 125 Tachografas turi rodyti perspėjamąją informaciją visų pirma 3 priedėlyje nurodytomis piktogramomis, kai reikia, prirašydamas papildomą skaitmenimis užkoduotą informaciją. Taip pat gali būti rodomas raidinis perspėjimo paaiškinimas vairuotojo pageidaujama kalba.

15.3. *Naudojimasis meniu*

- 126 Tachografo komandomis turi būti galima pasinaudoti per atitinkamą meniu sistemą.

15.4. *Kiti rodiniai*

- 127 Turi būti galima pasirinkti tokius ekrano rodinius:
- UTC datą ir laiką,
 - darbo režimą (jei tai nerodoma pagal numatytąjį nustatymą),
 - vairuotojo nepertraukiamo vairavimo trukmę ir bendrąją poilsio trukmę,
 - vairuotojo porininko nepertraukiamo vairavimo trukmę ir bendrąją poilsio trukmę,
 - ankstesnės ir esamos savaitės vairuotojo bendrą vairavimo trukmę,
 - ankstesnės ir esamos savaitės vairuotojo porininko bendrą vairavimo trukmę,
 - bet kurio iš šių spaudinių turinį, spausdinant tokiu pačiu formatu, kaip ir patys spaudiniai.
- 128 Spaudinio turinys turi būti rodomas nuosekliai, eilutė po eilutės. Jei ekrano plotis yra mažesnis kaip 24 rašmenys, visa informacija vairuotojui turi būti pateikiama atitinkamais būdais (keletu eilučių, „bėgančia“ eilute ir pan.). Ekrane gali būti nerodomos spaudinio eilutės, skirtos užpildyti ranka.

16. *Spausdinimas*

- 129 Tachografas turi gebėti spausdinti informaciją iš savo atminties ir (arba) iš tachografo kortelių tokių šių rūšių spaudiniuose:
- vairuotojo veiklos kasdienis spaudinys iš kortelės,
 - vairuotojo veiklos kasdienis spaudinys iš transporto priemonės bloko,

- įvykių ir gedimų spaudinys iš kortelės,
- įvykių ir gedimų spaudinys iš transporto priemonės bloko,
- techninių duomenų spaudinys,
- greičio viršijimo spaudinys.

Šių spaudinių formatas ir turinys išsamiai apibūdinti 4 priedėlyje.

Spaudinių pabaigoje gali būti pateikti papildomi duomenys.

Tachografas taip pat gali spausdinti papildomus spaudinius, jei jie aiškiai atskiriami nuo pirmiau minėtų šešių spaudinių.

- 130 „Vairuotojo veiklos kasdienį spaudinį iš kortelės“ ir „įvykių ir gedimų spaudinį iš kortelės“ turi būti įmanoma išspausdinti tik tuomet, kai į tachografą įkišta vairuotojo arba dirbtuvių kortelė. Prieš spausdindamas tachografas atnaujinama atitinkamoje kortelės atmintyje laikomus duomenis.
- 131 Tam, kad išspausdintų „vairuotojo veiklos kasdienį spaudinį iš kortelės“ arba „įvykių ir gedimų spaudinį iš kortelės“, tachografas:
- jei yra įkišta tik viena šių kortelių – automatiškai pasirenka vairuotojo kortelę arba dirbtuvių kortelę,
 - jei yra įkištos abi šios kortelės – nurodo komandą reikiamai kortelei pasirinkti arba pasirenka į vairuotojo plyšį įkištą kortelę.
- 132 Spausdintuvas turi gebėti spausdinti 24 rašmenis vienoje eilutėje.
- 133 Rašmuo turi būti ne mažesnis kaip 2,1 mm aukščio ir 1,5 mm pločio.
- 133a Spausdintuvas turi gebėti spausdinti atvaizduoti ISO 8859 1 ir 7 dalyse nustatytus Lotynų 1 ir Graikų rašmenų rinkinius, kaip nurodyta 1 priedėlio 4 skyriuje „Rašmenų rinkiniai“.
- 134 Spausdintuvai turi būti tokios konstrukcijos, kad spaudiniai būtų pakankamai ryškūs ir juos skaitant nekiltų dviprasmybių.
- 135 Spaudinių matmenys ir įrašai juose turi nesikeisti įprasto drėgnio (nuo 10 iki 90 %) ir temperatūros sąlygomis.
- 136 Spausdindamas tachografas turi gebėti susitvarkyti pasibaigus popieriui: įdėjus naują popierių pradėti spausdinti iš naujo arba tęsti spausdinimą toliau ir pateikti nedviprasmišką nuorodą į pirmiau išspausdintą dalį.
- 137 Lehetőség van e dokumentumokra kézzel krott jegyzetet rívezetni, mint pl. a jírművezető alíkrísa.
- 138 A papkrellítísnak a nyomtatís folyamín tórténő megszakadísa esetén és a papkr /jratóltése utín a menetkró készülék vagy az elejétől fogva /jra kezdí a nyomtatíst, vagy a megszakktís pontjítól folytatja azt tovíbb, félreérthetetlen utalíst téve az elözöleg kinyomtatott részre.

17. Perspėjimai

- 139 Tachografas turi perspėti vairuotoją, kai aptinka įvykį ir (arba) gedimą.
- 140 Perspėjimas dėl maitinimo nutrūkimo gali būti atidėtas iki maitinimas vėl bus tiekiamas.
- 141 Tachografas turi perspėti vairuotoją prieš 15 minučių iki baigiantis 4 valandų ir 30 minučių nepertraukiamo vairavimo laikotarpiui ir jam pasibaigus.
- 142 Perspėjimai turi būti regimieji. Kartu gali būti ir papildomi girdimieji perspėjimai.

- 143 Regimieji perspėjimai turi būti aiškiai atpažįstami naudotojui, būti vairuotojo regos lauke ir aiškiai matomi tiek dieną, tiek naktį.
- 144 Regimųjų perspėjimų komponentai gali būti įmontuoti tachografe ir (arba) nuotoliniai.
- 145 Pastaruoju atveju jie turi būti paženklinėti raide „T“ ir būti gintarinės arba oranžinės spalvos.
- 146 Perspėjimas turi trukti ne mažiau kaip 30 sekundžių, nebent naudotojas, baksteldamas bet kurį tachografo klavišą, patvirtintų, jog jį pastebėjo. Po pirmojo patvirtinimo neturi būti panaikintas perspėjimo priežasties rodinys, nurodytas kitoje pastraipoje.
- 147 Perspėjimo priežastis turi būti rodoma tachografo ekrane tol, kol naudotojas, paspausdamas tam tikrą klavišą arba pasirinkdamas tam tikrą tachografo komandą, patvirtina, kad ją mato.
- 148 Gali būti pateikiami papildomi perspėjimai, jei vairuotojas negali jų supainioti su pirmiau minėtais.

18. Duomenų perkėlimas į išorines laikmenas

- 149 Tachografas turi gebėti nurodžius per kalibravimo/duomenų perkėlimo jungtį perkelti duomenis iš savo atminties arba vairuotojo kortelės į išorines laikmenas. Prieš perkeldamas duomenis tachografas turi atnaujinti atitinkamos kortelės duomenis.
- 150 Be to, tachografas gali bet kuriuo darbo režimu persiųsti duomenis per kitą jungtį šiuo kanalu patvirtintai įmonei (kaip papildoma funkcija). Tokiu atveju turi galioti įmonės režimo duomenų prieigos teisės.
- 151 Persiunčiant duomenys negali būti niekaip pakeisti ar ištrinti.

Kalibravimo/duomenų perkėlimo jungties elektrinė sąsaja nurodyta 6 priedėlyje.

Duomenų perkėlimo protokolai nurodyti 7 priedėlyje.

19. Duomenų persiuntimas į papildomus išorinius įtaisus

- 152 Kai tachografas neturi greičio ir (arba) hodometro rodmenų funkcijų, jis turi siųsti išeinantįjį signalą (-us), kad galima būtų pamatyti ekrane transporto priemonės greitį (spidometro rodmenį) ir (arba) visą nuvažiuotą atstumą (hodometro rodmenį).
- 153 Transporto priemonės blokas taip pat turi gebėti teikti tokius duomenis per reikiamą skirtąją nuosekliają jungtį, nepriklausomą nuo papildomos VVT šynos jungties (ISO 11898 Kelių transporto priemonės. Keitimasis skaitmenine informacija. Vietinis valdiklio tinklas (VVT), skirtas didelės spartos ryšiui), kad jie galėtų būti apdoroti kita transporto priemonėje įrengta elektronine įranga:

- esamą UTC datą ir laiką,
- transporto priemonės greitį,
- visą transporto priemonės nuvažiuotą atstumą (hodometro rodmenį),
- tuo metu pasirinktą vairuotojo ir vairuotojo porininko veiklą,
- informaciją apie tai, ar į vairuotojo ir vairuotojo porininko (jei taikytina) plyšį įkišta kokia nors tachografo kortelė, ir informaciją apie atitinkamos kortelės identifikaciją (kortelės numerį ir išduodančiosios valstybės narės žymenį).

Tai pat gali būti išvedami ir kiti papildomi duomenys.

Kai transporto priemonės degimas įjungtas, minėti duomenis turi būti siunčiami nuolatos. Kai transporto priemonės degimas išjungtas, atitinkami duomenys turi būti išsiunčiami bent jau tuomet, kai pasikeičia vairuotojo arba vairuotojo porininko veikla ir (arba) įkišama arba ištraukiama tachografo kortelė. Jei esant išjungtam transporto priemonės degimui duomenų išvedimas sulaikomas, jie turi būti pateikti degimą įjungus.

20. Kalibravimas

154 Kalibravimo funkcija turi leisti:

- automatiškai sujungti judesio jutiklį su TPB,
- skaitmeniniu būdu priderinti tachografo konstantą (k) prie transporto priemonės būdinguoju koeficientu (w) (transporto priemonėse su dviem ar daugiau pagrindinės pavaros perdavimo skaičių turi būti įmontuotas keitimo įtaisas, kuris automatiškai suderintų šiuos perdavimo skaičius su tokiu perdavimo skaičiumi, kuriuo remiantis įrangą buvo pritaikyta transporto priemonei),
- neribotai koreguoti esamą laiką,
- koreguoti esamą hodometro rodmens vertę,
- atnaujinti atmintyje laikomus judesio jutiklio identifikacijos duomenis,
- atnaujinti arba patvirtinti kitus tachometrui žinomus duomenis: transporto priemonės tapatybę, w, l, padangų dydį ir greičio ribotuvo nustatymą (jei yra).

155 Sujungiant judesio jutiklį su TPB, turi būti atliekami bent jau tokie veiksmai:

- atnaujinami judesio jutiklio atmintyje laikomi jo įrengimo duomenys (jei reikia),
- iš judesio jutiklio į TPB atmintį nukopijuojami reikiami judesio jutiklio identifikacijos duomenys.

156 Kalibravimo funkcija turi gebėti įvesti reikiamus duomenis per kalibravimo/duomenų perkėlimo laikantis 8 priedėlyje nustatyto kalibravimo protokolo. Kalibravimo funkcija gali įvesti reikiamus duomenis ir per kitas jungtis.

21. Laiko koregavimas

157 Laiko koregavimo funkcija turi leisti koreguoti esamą laiką ne mažesniais kaip vienos minutės pokyčiais ir ne dažniau kaip kas septynias dienas.

158 Kalibravimo režimu laiko koregavimo funkcija turi leisti koreguoti esamą laiką be apribojimų.

22. Eksploatacinės savybės

159 Transporto priemonės blokas turi visiškai tinkamai veikti nuo – 20 °C iki 70 °C, o judesio jutiklis nuo – 40 °C iki 135 °C temperatūroje. Duomenys atmintyje turi būti išlaikomi iki –40 °C temperatūroje.

160 Tachografas turi visiškai tinkamai veikti esant nuo 10 % iki 90 % drėgno.

161 Tachografas turi būti apsaugotas nuo viršįtampio, maitinimo poliškumo apsikeitimo ir trumpojo jungimo.

162 Tachografas turi atitikti 1995 m. spalio 31 d. Komisijos direktyvą 95/54/EB ⁽¹⁾, derinančią su technikos pažanga Tarybos direktyvą 72/245/EEB ⁽²⁾ dėl elektromagnetinio suderinamumo, ir turi būti apsaugotas nuo elektrostatinų iškrovų ir trumpalaikių srovių.

23. Medžiagos

163 Visos tachografo sudedamosios dalys turi būti pagamintos iš pakankamai stabilų, mechaniškai atsparių, turinčių pastovias elektrines ir magnetines savybes, medžiagų.

164 Įprastomis naudojimo sąlygomis visos vidinės įrangos dalys turi būti apsaugotos nuo drėgmės ir dulkių.

165 Transporto priemonės blokas turi būti IP 40, o judesio jutiklis – IP 64 apsaugos klasės pagal standartą IEC 529.

⁽¹⁾ OL L 266, 1995 11 8, p. 1.

⁽²⁾ OL L 152, 1972 7 6, p. 15.

166 Tachografas turi atitikti jam taikomas ergonominio dizaino technines specifikacijas.

167 Tachografas turi būti apsaugotas nuo atsitiktinės žalos.

24. Ženkilai

168 Jei tachografas rodo transporto priemonės hodometro rodmenis vertę ir greitį, jo ekrane turi būti tokie užrašai:

— greta nuotolį rodančio skaičiaus turi būti užrašytas atstumo matavimo vienetas, žymimas santrumpa „km“,

— greta greitį rodančio skaičiaus – užrašas „km/h“.

Tachografas gali būti nustatytas rodyti greitį myliomis per valandą, tuomet ir greičio matavimo vienetą žyminti santrumpa turi būti „mph“.

169 Ant kiekvieno atskiros tachografo komponento turi būti pritvirtinta plokštelė, kurioje užrašyta tokia informacija:

— įrangos gamintojo pavadinimas ir adresas,

— gamintojo suteiktas komponento šifras ir įrangos pagaminimo metai,

— įrangos serijos numeris,

— įrangos tipo patvirtinimo ženklas.

170 Kai pirmiau nurodytai informacijai užrašyti nepakanka vietos, plokštelėje turi būti nurodytas bent gamintojo pavadinimas ar logotipas ir įrangos komponento šifras.

IV. TACHOGRAFO KORTELIŲ KONSTRUKCIJOS IR FUNKCINIAI REIKALAVIMAI

1. Regimieji duomenys

Kortelės priekyje yra:

171 kortelę išduodančios valstybės narės valstybine kalba arba kalbomis didžiosiomis raidėmis išspausdinti žodžiai „Vairuotojo kortelė“, „Kontrolės kortelė“, „Dirbtuvių kortelė“ arba „Įmonės kortelė“;

172 kortelės foną sudaro tie patys žodžiai kitomis valstybinėmis Bendrijos kalbomis:

ES	TARJETA DEL CONDUCTOR	TARJETA DE CONTROL	TARJETA DEL CENTRO DE ENSAYO	TARJETA DE LA EMPRESA
DK	FØRERKORT	KONTROLKORT	VÆRKSTEDSKORT	VIRKSOMHEDSKORT
DE	FAHRERKARTE	KONTROLLKARTE	WERKSTATTKARTE	UNTERNEHMENSKARTE
EL	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 KORTTILLA	VALVONTA KORTILLA	TESTAUSASEMA KORTILLA	YRITYSKORTILLA
SV	FÖRARKORT	KONTROLLKORT	VERKSTADSKORT	FÖRETAGSKORT

173 kortelę išduodančios valstybės narės pavadinimas (neprivalomas);

- 174 kortelę išduodančios valstybės narės skiriamasis ženklas, mėlynos spalvos stačiakampyje išspausdintas negatyvu ir apsup-
tas dvylika geltonos spalvos žvaigždžių. Skiriamieji ženklai yra šie:

B	Belgija
DK	Danija
D	Vokietija
GR	Graikija
E	Ispanija
F	Prancūzija
IRL	Airija
I	Italija
L	Liuksemburgas
NL	Nyderlandai
A	Austrija
P	Portugalija
FIN	Suomija
S	Švedija
UK	Jungtinė Karalystė

- 175 Informacija, būdinga išduotai kortelei ir sunumeruota taip:

	Vairuotojo kortelė	Kontrolės kortelė	Įmonės arba dirbtuvių kortelė
1.	Vairuotojo pavardė	Kontrolės institucijos pavadinimas	Įmonės arba dirbtuvių pavadinimas
2.	Vairuotojo vardas (-ai)	Ellenőrző személy vezetéknéve (adott esetben)	Kirlyatulajdonos vezetéknéve (adott esetben)
3.	Įjrmūvezető születési dátuma	Ellenőrző személy utónéve(i) (adott esetben)	Kirlyatulajdonos utónéve (adott esetben)
4.(a)	Kortelės galiojimo pradžios data		
(b)	Kortelės galiojimo pabaigos data		
(c)	Išduodančiosios institucijos pavadinimas (galima spausdinti 2-ame puslapyje)		
(d)	Kitas, ne pateiktasis 5 antraštėje, numeris administravimo tikslams (neprivaloma)		
5.(a)	Vairuotojo pažymėjimo (galiojančio išduodant vairuotojo kortelę) numeris		
5.(b)	Kortelės numeris		
6.	Vairuotojo nuotrauka	Kontrolieriaus nuotrauka (neprivaloma)	—
7.	Vairuotojo parašas	Kortelės turėtojo parašas (neprivaloma)	
8.	Kortelės turėtojo nuolatinė gyvenamoji vieta arba pašto adresas (neprivaloma)	Kontrolės institucijos pašto adresas	Įmonės arba dirbtuvių pašto adresas

- 176 datos turi būti rašomos formatais „dd/mm/yyyy“ arba „dd.mm.yyyy“ (diena, mėnesis, metai);

kitoje kortelės pusėje yra:

- 177 kortelės priekyje sunumeruotų punktų paaiškinimas;

- 178 kortelės turėtoji specialiai raštu sutikus, gali būti įrašyta ir su kortelės administravimu nesusijusi informacija, jei tai nie-
kaip nepakeistų tachografo kortelės naudojimo paskirties.

BENDRIJOS VAIRUOTOJO KORTELĖS PAVYZDYS

PRIEKINĖ PUSĖ		UŽPAKALINĖ PUSĖ	
A	VAIRUOTOJO KORTELĖ 1. 2. 3. 4a. 4c. 5a. 5b. 6. 7. (8.)	VALSTYBĖ NARĖ TARJETA DEL CONDUCTOR FØRERKORT FAHRERKARTE ΚΑΡΤΑ Ο ΔΗΤΟΥ DRIVER CARD CARTE DE CONDUCTEUR CÁRTA TIOMÁNAÍ CARTA DEL CONDUCENTE BESTUURDESKAART CARTÃO DE CONDUTOR KULJETTAJAKORTILLA FÖRARKORT 4b. (4d.)	B
B	KONTROLĖS KORTELĖ 1. (2.) (3.) 4a. 4c. (4d.) 5b. (6.) (7.) 8.	VALSTYBĖ NARĖ TARJETA DE CONTROL KONTROLKORT KONTROLLKARTE ΚΑΡΤΑ ΕΛΕΓΧΟΥ CONTROL CARD CARTE DE CONTROLEUR CÁRTA STIÚRTHA CARTA DI CONTROLLO CONTOLEKAART CARTÃO DE CONTROLO VALVONTAKORTILLA KONTROLLKORT (4b.)	B
B	DIRBTUVIŲ KORTELĖ 1. (2.) (3.) 4a. 4c. (4d.) 5b. (7.) 8.	VALSTYBĖ NARĖ TARJETA DEL CENTRO DE ENSAYO VÆRKSTEDSKORT WERKSTATTKARTE ΚΑΡΤΑ ΚΕΝΤΡΟΥ ΔΟΚΙΜΩΝ WORKSHOP CARD CARTE D'ATELIER CÁRTA CEARDLAINNE CARTA DELL'OFFICINA WERKPLAATSKAART CARTÃO DO CENTRO DE ENSAIO TESTAUSASEMAKORTILLA VERKSTADSKORT (4b.)	B
B	ĮMONĖS KORTELĖ 1. (2.) (3.) 4a. 4c. (4d.) 5b. (7.) 8.	VALSTYBĖ NARĖ TARJETA DE LA EMPRESA VIRKSOMHEDSKORT UNTERNEHMENSKARTE ΚΑΡΤΑ ΕΠΙΧΕΙΡΗΣΕΩΣ COMPANY CARD CARTE D'ENTREPRISE CÁRTA COMHLACHTA CARTA DELL'AZIENDA BEDRUFSSKAART CARTÃO DE EMPRESA YRITYSKORTILLA FÖRETAGSKORT 4b. (4d.)	B

1. Pavardė 2. Vardas (-ai) 3. Gimimo data ir vieta 4a. Kortelės galiojimo pradžios data 4b. Kortelės administracinio galiojimo pabaigos data 4c. Išduodančioji institucija (4d.) Numeris, skirtas nacionaliniam administravimui 5a. Vairuotojo pažymėjimo numeris 5b. Kortelės numeris 6. Nuotrauka 7. Parašas (8.) Adresas <i>Prašome grąžinti:</i> INSTITUCIJOS PAVADINIMAS IR ADRESAS	1. Kontrolės 2. Pavardė 3. Vardas (-ai) institucija 4a. Kortelės galiojimo pradžios data 4b. Kortelės administracinio galiojimo pabaigos data 4c. Išduodančioji institucija (4d.) Numeris, skirtas nacionaliniam administravimui 5b. Kortelės numeris (6.) Nuotrauka (7.) Parašas 8. Adresas <i>Prašome grąžinti:</i> INSTITUCIJOS PAVADINIMAS IR ADRESAS
1. Dirbtuvių 2. Pavardė 3. Vardas (-ai) pavadinimas 4a. Kortelės galiojimo pradžios data 4b. Kortelės administracinio galiojimo pabaigos data 4c. Išduodančioji institucija (4d.) Numeris, skirtas nacionaliniam administravimui 5b. Kortelės numeris (7.) Parašas 8. Adresas <i>Prašome grąžinti:</i> INSTITUCIJOS PAVADINIMAS IR ADRESAS	1. Įmonės 2. Pavardė 3. Vardas (-ai) pavadinimas 4a. Kortelės galiojimo pradžios data 4b. Kortelės administracinio galiojimo pabaigos data 4c. Išduodančioji institucija (4d.) Numeris, skirtas nacionaliniam administravimui 5b. Kortelės numeris (7.) Parašas 8. Adresas <i>Prašome grąžinti:</i> INSTITUCIJOS PAVADINIMAS IR ADRESAS

179 Tachografų kortelių fono dominuojanti spalva turi būti tokia:

- vairuotojų kortelės: balta,
- kontrolės kortelės: mėlyna,
- dirbtuvių kortelės: raudona,
- įmonės kortelės: geltona.

180 Tachografo kortelės turi turėti bent tokius apsaugos nuo klastojimo ir apgadinimo elementus:

- apsauginio dizaino foną su smulkiu ornamentiniu raštu ir spalvotais spaudiniais,
- nuotraukos srityje apsauginio dizaino fonas ir nuotrauka turi iš dalies sutapti,
- bent vieną dvispalvę mikrošrifto eilutę.

- 181 Pasikonsultavusios su Komisija valstybės narės gali naudoti papildomų spalvų ir ženklų, pvz., nacionalinius simbolius ir apsaugos elementus, jei tai nepažeidžia kitų šio priedo nuostatų.

2. Apsauga

Sistemos apsauga skirta saugoti tarp kortelių ir tachografo perduodamų duomenų nepažeistumą bei autentiškumą, iš kortelių perkeliama duomenų nepažeistumą bei autentiškumą, leisti įrašyti tam tikrą informaciją į korteles tik tachografui, užkirsti kelią bet kokioms galimybėms falsifikuoti kortelėse laikomus duomenis, saugoti nuo klastojimo ir aptikti bet kokius mėginimus tai padaryti.

- 182 Tam, kad sistema būtų saugi, tachografo kortelės turi atitikti tachografo kortelių bendruosiuose apsaugos tiksluose nurodytus reikalavimus (10 priedelis).
- 183 Informaciją iš tachografo kortelių turi būti įmanoma nuskaityti ir kita įranga, pvz., asmeniniais kompiuteriais.

3. Standartai

- 184 Tachografo kortelės turi atitikti tokių standartų reikalavimus:

- ISO/IEC 7810 Identifikacijos kortelės. Fizinės savybės,
- ISO/IEC 7816 Identifikacijos kortelės. Integriniai grandynai:
 - 1 dalis. Fizinės savybės,
 - 2 dalis. Matmenys ir kontaktų vieta,
 - 3 dalis. Elektroniniai signalai ir siuntimo protokolai,
 - 4 dalis. Tarpusavio keitimosi tarpšakinės komandos,
 - 8 dalis. Apsauginės tarpšakinės komandos,
- ISO/IEC 10373 Identifikacijos kortelės. Bandymų metodika.

4. Aplinkos ir elektros specifikacijos

- 185 Tachografo kortelės turi gebėti tinkamai veikti visomis Bendrijos teritorijoje dažniausiai būnančiomis klimato sąlygomis ir bent jau nuo -25°C iki $+70^{\circ}\text{C}$ temperatūroje, o trumpam – iki $+85^{\circ}\text{C}$ temperatūroje. „Trumpam“ reiškia ne ilgiau kaip 4 valandas kiekvieną dieną ir ne daugiau kaip 100 kartų per visą kortelės naudojimo laiką.
- 186 Tachografo kortelės turi visiškai tinkamai veikti esant nuo 10 % iki 90 % drėgnio.
- 187 Pagal aplinkos ir elektros specifikacijų reikalavimus naudojamos tachografo kortelės turi visiškai tinkamai veikti penkerius metus.
- 188 Tachografo kortelės turi atitikti 1995 m. spalio 31 d. Komisijos direktyvą 95/54/EB ⁽¹⁾ dėl elektromagnetinio suderinamumo ir turi būti apsaugotas nuo elektrostatinio iškvėpų.

5. Duomenų laikymas

Šiame poskyryje:

- jei nenurodyta kitaip, laikas registruojamas vienos minutės tikslumu,
- hodometro vertės registruojamos vieno kilometro tikslumu,
- greitis registruojamas 1 km/h tikslumu.

Duomenų laikymo reikalavimus atitinkančios tachografo kortelių funkcijos, komandos ir loginė struktūra nurodytos 2 priedėlyje.

⁽¹⁾ OL L 266, 1995 11 8, p. 1.

- 189 Šiame poskyryje nurodyta mažiausia įvairių taikomųjų duomenų rinkmenų laikymo talpa. Tachografo kortelės turi gebėti nurodyti tachografiui esamą šių duomenų rinkmenų laikymo talpą.

Visi su kita galima kortelės paskirtimi susiję papildomi duomenys, kurie gali būti laikomi tachografo kortelėse, turi būti laikomi pagal 1995 m. spalio 24 d. Direktyvą 95/46/EB dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ⁽¹⁾.

5.1. Kortelės identifikacijos ir apsaugos duomenys

5.1.1. Taikomosios programos identifikacija

- 190 Tachografo kortelės turi gebėti laikyti atmintyje tokius taikomosios programos identifikacijos duomenis apie:

- tachografo taikomosios programos identifikaciją,
- tachografo kortelės identifikacijos rūšį.

5.1.2. Mikroschemos identifikacija

- 191 Tachografo kortelės turi gebėti laikyti atmintyje tokius integrinio grandyno (IC) identifikacijos duomenis:

- IC serijos numerį,
- IC pagaminimo žymenis.

5.1.3. IC kortelės identifikacija

- 192 Tachografo kortelės turi gebėti laikyti atmintyje tokius mikroschemos identifikacijos duomenis:

- kortelės serijos numerį (įskaitant pagaminimo žymenis),
- kortelės tipo patvirtinimo numerį,
- kortelės suasmeninimo identifikaciją (ID),
- įterptąjį ID,
- IC vardą.

5.1.4. Apsaugos elementai

- 193 Tachografo kortelės turi gebėti laikyti atmintyje tokius apsaugos elementų duomenis:

- europinį atvirąjį raktą,
- valstybės narės pažymėjimą,
- kortelės pažymėjimą,
- kortelės slaptąjį raktą.

5.2. Vairuotojo kortelė

5.2.1. Kortelės identifikacija

- 194 Vairuotojo kortelė turi gebėti laikyti atmintyje tokius kortelės identifikacijos duomenis:

- kortelės numerį,
- išduodančiosios valstybės, išduodančiosios institucijos pavadinimą, išdavimo datą,
- kortelės galiojimo pradžios ir pabaigos datą.

⁽¹⁾ OL L 281, 1995 11 23, p. 31.

5.2.2. Kortelės turėtojo identifikacija

195 Vairuotojo kortelė turi gebėti laikyti atmintyje tokius jos turėtojo identifikacijos duomenis:

- turėtojo pavardę,
- turėtojo vardą (-us),
- gimimo datą,
- pageidaujamą kalbą.

5.2.3. Informacija apie vairuotojo pažymėjimą

196 Vairuotojo kortelė turi gebėti laikyti atmintyje tokius duomenis apie vairuotojo pažymėjimą:

- išduodančiosios valstybės, išduodančiosios institucijos pavadinimą,
- vairuotojo pažymėjimo (galiojančio išduodant kortelę) numerį.

5.2.4. Duomenys apie naudotas transporto priemones

197 Vairuotojo kortelė turi gebėti laikyti atmintyje tokius duomenis apie kiekvieną kalendorinę dieną, kurią kortelė buvo naudota, ir apie kiekvieną tos transporto priemonės naudojimo laikotarpį tą dieną (laikotarpis aprėpia visus kortelės įkišimo ir ištraukimo ciklus transporto priemonėje):

- pirmojo transporto priemonės panaudojimo datą ir laiką (t. y. pirmojo kortelės įkišimo tą transporto priemonės naudojimo laikotarpį datą ir laiką, o jei laikotarpis tęsiasi – žymenį 00.00),
- transporto priemonės hodometro rodmens vertę tuo metu,
- paskutiniojo transporto priemonės panaudojimo datą ir laiką (t. y. paskutiniojo kortelės ištraukimo tą transporto priemonės naudojimo laikotarpį datą ir laiką, o jei laikotarpis tęsiasi – žymenį 23.59),
- transporto priemonės hodometro rodmens vertę tuo metu,
- transporto priemonės TPRN ir registruojančiosios valstybės narės žymenį.

198 Vairuotojo kortelė turi gebėti išlaikyti atmintyje ne mažiau kaip 84 tokius įrašus.

5.2.5. Duomenys apie vairuotojo veiklą

199 Vairuotojo kortelė turi gebėti laikyti atmintyje tokius duomenis apie kiekvieną kalendorinę dieną, kurią kortelė buvo naudota arba kurią vairuotojas rankomis įvedė duomenis apie veiklą:

- datą,
- naudojimo dienos skaitiklio rodmens vertę (kuri kiekvieną naudojimo dieną padidėja vienetu),
- bendrą tą dieną vairuotojo nuvažiuotą atstumą,
- vairuotojo būseną 00.00 val.,
- ar vairuotojas pakeitė veiklos rūšį ir (arba) važiavimo būseną ir (arba) įkišo ar ištraukė savo kortelę:
 - važiavimo būseną (ĮGULA, VIENAS VAIRUOTAS),
 - plyšys (VAIRUOTOJO, VAIRUOTOJO PORININKO),
 - kortelės būseną (ĮKIŠTA, NEĮKIŠTA),
 - veiklos rūšį (VAIRAVIMAS, BUVIMAS PASIRENGUS DIRBTI, DARBAS, PERTRAUKA/POILSIS),
 - pasikeitimo datą ir laiką.

200 Vairuotojo kortelės atmintis turi gebėti išlaikyti duomenis ne mažiau kaip apie vairuotojo 28 dienų veiklą (vidutinę vairuotojo veiklą sudaro 93 veiklos pokyčiai per dieną).

- 201 197 ir 199 reikalavimuose išvardyti duomenys turi būti laikomi taip, kad juos galima būtų gauti chronologine tvarka, net ir iš dalies sutapus laikui.

5.2.6. Vietos, kur prasideda ir (arba) baigiasi dienos darbo laikotarpiai

- 202 Vairuotojo kortelė turi gebėti laikyti atmintyje tokius vairuotojo įvedamus duomenis, susijusius su vietomis, kur prasideda ir (arba) baigiasi dienos darbo laikotarpiai:

- įrašo datą ir laiką (arba su įrašu susijusią datą ir laiką, kai įrašoma įvedant rankomis),
- įrašo tipą (pradžią ar pabaigą, įrašo aplinkybės),
- įvestus šalies ir regiono žymenis,
- transporto priemonės hodometro rodmenis vertę.

- 203 Vairuotojo kortelė turi gebėti išlaikyti atmintyje ne mažiau kaip 42 poras tokių įrašų.

5.2.7. Duomenys apie įvykius

Šiame papunktyje nurodytais tikslais laikas registruojamas sekundės tikslumu.

- 204 Vairuotojo kortelė turi gebėti laikyti atmintyje informaciją apie tokius įvykius, tachografo aptiktus tuomet, kai kortelė buvo įkišta:

- dalinį laiko sutapimą (kai tai atsitiko dėl kortelės),
- kortelės įkišimą važiuojant (jei įkišta ta kortelė),
- paskutinę kortelės panauda tinkamai neužbaigta (kai naudota ta kortelė),
- maitinimo nutrūkimą,
- duomenų apie judėjimą klaidą,
- bandymus pažeisti apsaugą.

- 205 Vairuotojo kortelė turi gebėti laikyti atmintyje tokią informaciją apie minėtus įvykius:

- įvykio kodą,
- įvykio pradžios (arba kortelės įkišimo, jei įvykis vyko tuo metu) datą ir laiką,
- įvykio pabaigos (arba kortelės ištraukimo, jei įvykis vyko tuo metu) datą ir laiką,
- transporto priemonės, kurioje įvykis įvyko, TPRN ir registruojančiosios valstybės narės žymenį.

Pastaba: įvykus „dalinio laiko sutapimo“ įvykiui:

- įvykio pradžios data ir laikas turi sutapti su kortelės ištraukimo iš ankstesnės transporto priemonės data ir laiku,
- įvykio pabaigos data ir laikas turi sutapti su kortelės įkišimo į ankstesnę transporto priemonę data ir laiku,
- a įjrmū adatai megegyeznek az eseményt előidéző aktuális įjrmū adataival.

Pastaba: įvykus įvykiui „paskutinę kortelės panauda tinkamai neužbaigta“:

- įvykio pradžios data ir laikas turi sutapti su tinkamai neužbaigtos panaudos kortelės įkišimo data ir laiku,
- įvykio pabaigos data ir laikas turi sutapti su panaudos, kurios metu įvykis buvo aptiktas, kortelės įkišimo data ir laiku,
- duomenys apie transporto priemonę turi atitikti tą transporto priemonę, kurioje panauda nebuvo tinkamai užbaigta.

- 206 Vairuotojo kortelė turi gebėti laikyti atmintyje duomenis apie šešis paskutinius kiekvienos rūšies įvykius (t. y. iš viso 36 įvykius).

5.2.8. *Duomenys apie gedimus*

Šiame papunktyje nurodytais tikslais laikas registruojamas sekundės tikslumu.

- 207 Vairuotojo kortelė turi gebėti laikyti atmintyje informaciją apie tokius gedimus, tachografo aptiktus tuomet, kai kortelė buvo įkišta:

- kortelės gedimą (kai tai atsitiko dėl kortelės),
- tachografo gedimą.

- 208 Vairuotojo kortelė turi gebėti laikyti atmintyje tokią informaciją apie minėtus gedimus:

- gedimo kodą,
- gedimo pradžios (arba kortelės įkišimo, jei gedimas vyko tuo metu) datą ir laiką,
- gedimo pabaigos (arba kortelės ištraukimo, jei gedimas vyko tuo metu) datą ir laiką,
- transporto priemonės, kurioje gedimas įvyko, TPRN ir registruojančiosios valstybės narės žymenį.

- 209 Vairuotojo kortelė turi gebėti laikyti atmintyje duomenis apie dvylika paskutinių kiekvienos rūšies gedimų (t. y. iš viso 24 gedimus).

5.2.9. *Duomenys apie kontrolės veiklą*

- 210 Vairuotojo kortelė turi gebėti laikyti atmintyje tokius duomenis apie kontrolės veiklą:

- kontrolės datą ir laiką,
- kontrolės kortelės numerį ir kortelę išduodančios valstybės narės žymenį,
- kontrolės rūšį (rodymas ekrane ir (arba) spausdinimas ir (arba) duomenų perkėlimas iš TPB ir (arba) duomenų perkėlimas iš kortelės),
- kurio laikotarpio duomenys perkelti (jei perkeliama duomenys),
- transporto priemonės TPRN ir registruojančiosios valstybės narės, kurioje buvo atliekama kontrolė, žymenį.

Pastaba: apsaugos reikalavimais numatyta, kad duomenų perkėlimas iš kortelės registruojamas tik tuomet, kai tai atliekama tachografu.

- 211 Vairuotojo kortelė turi gebėti išlaikyti atmintyje vieną tokį įrašą.

5.2.10. *Duomenys apie kortelės panaudą*

- 212 Vairuotojo kortelė turi gebėti laikyti atmintyje tokius duomenis, susijusius su transporto priemone, kurioje buvo pradėta esama jos panauda:

- panaudos pradžios (t. y. kortelės įkišimo) datą ir laiką vienos sekundės tikslumu,
- TPRN ir registruojančiosios valstybės narės žymenį.

5.2.11. *Duomenys apie ypatingas būsenas*

- 212a Vairuotojo kortelė turi gebėti laikyti atmintyje duomenis, susijusius su ypatingomis būsenomis, kurios prasidėjo tuomet, kai kortelė buvo įkišta:

- įrašo datą ir laiką,
- ypatingos būsenos rūšį.

212b Vairuotojo kortelė turi gebėti išlaikyti atmintyje 56 tokius įrašus.

5.3. *Dirbtuvių kortelė*

5.3.1. *Apsaugos elementai*

213 Dirbtuvių kortelė turi gebėti laikyti atmintyje asmeninės identifikacijos numerį (PIN kodą).

214 Dirbtuvių kortelė turi gebėti laikyti atmintyje šifravimo raktus, skirtus judesio jutikliams sujungti su transporto priemonės blokais.

5.3.2. *Kortelės identifikacija*

215 Dirbtuvių kortelė turi gebėti laikyti atmintyje tokius kortelės identifikacijos duomenis:

- kortelės numerį,
- išduodančiosios valstybės žymenį, išduodančiosios institucijos pavadinimą, išdavimo datą,
- kortelės galiojimo pradžios ir pabaigos datą.

5.3.3. *Kortelės turėtojo identifikacija*

216 Dirbtuvių kortelė turi gebėti laikyti atmintyje tokius jos turėtojo identifikacijos duomenis:

- dirbtuvių pavadinimą,
- dirbtuvių adresą,
- turėtojo pavardę,
- turėtojo vardą (-us),
- pageidaujamą kalbą.

5.3.4. *Duomenys apie panaudotas transporto priemones*

217 Dirbtuvių kortelė turi gebėti laikyti atmintyje įrašus apie panaudotas transporto priemones taip pat kaip vairuotojo kortelė.

218 Dirbtuvių kortelė turi gebėti išlaikyti atmintyje ne mažiau kaip 4 tokius įrašus.

5.3.5. *Duomenys apie vairuotojo veiklą*

219 Dirbtuvių kortelė turi gebėti laikyti atmintyje duomenis apie vairuotojo veiklą taip pat kaip vairuotojo kortelė.

220 Dirbtuvių kortelės atmintis turi gebėti išlaikyti duomenis bent apie vairuotojo vienos dienos veiklą.

5.3.6. *Vietos, kur prasideda ir (arba) baigiasi dienos darbo laikotarpiai*

221 Dirbtuvių kortelė turi gebėti laikyti atmintyje įrašus apie dienos darbo laikotarpių pradžią ir (arba) pabaigą taip pat kaip vairuotojo kortelė.

222 Dirbtuvių kortelė turi gebėti išlaikyti atmintyje ne mažiau kaip tris poras tokių įrašų.

5.3.7. *Duomenys apie įvykius ir gedimus*

223 Dirbtuvių kortelė turi gebėti laikyti atmintyje įrašus apie įvykius ir gedimus taip pat kaip vairuotojo kortelė.

224 Dirbtuvių kortelė turi gebėti laikyti atmintyje duomenis apie tris paskutinius kiekvienos rūšies įvykius (t. y. iš viso apie 18 įvykių) ir šešis paskutinius kiekvienos rūšies gedimus (t. y. iš viso apie 12 gedimų).

5.3.8. *Duomenys apie kontrolės veiklą*

225 Dirbtuvių kortelė turi gebėti laikyti atmintyje duomenų apie kontrolės veiklą įrašus taip pat kaip vairuotojo kortelė.

5.3.9. Duomenys apie kalibravimą ir laiko koregavimą

- 226 Dirbtuvių kortelė turi gebėti laikyti atmintyje įrašus apie kalibravimą ir (arba) laiko koregavimus, atliktus tuomet, kai kortelė buvo įkišta į tachografą.
- 227 Kiekviename įrašė apie kalibravimą turi būti tokie duomenys:
- kalibravimo tikslas (pirmasis įrengimas, įrengimas, periodinė patikra),
 - transporto priemonės identifikacija,
 - atnaujinti arba patvirtinti parametrai (w, k, l, padangų dydis, greičio ribotuvo nustatymas, hodometro (rodmens sena ir nauja vertės), data ir laikas (sena ir nauja vertės),
 - tachografo identifikacija (TPB komponento šifras, TPB serijos numeris, judesio jutiklio serijos numeris).
- 228 Dirbtuvių kortelė turi gebėti išlaikyti ne mažiau kaip 88 tokius įrašus.
- 229 Dirbtuvių kortelė turi gebėti laikyti atmintyje bendrą su ja atliktų kalibravimų skaičių.
- 230 Dirbtuvių kortelė turi gebėti laikyti atmintyje bendrą po paskutinio duomenų perkėlimo atliktų kalibravimų skaičių.

5.3.10. Duomenys apie ypatingas būsenas

- 230a Dirbtuvių kortelė turi gebėti laikyti atmintyje duomenis, susijusius su ypatingomis būsenomis, taip pat kaip vairuotojo kortelė. Dirbtuvių kortelė turi gebėti išlaikyti atmintyje du tokius įrašus.

5.4. Kontrolės kortelė

5.4.1. Kortelės identifikacija

- 231 Kontrolės kortelė turi gebėti laikyti atmintyje tokius kortelės identifikacijos duomenis:
- kortelės numerį,
 - išduodančiosios valstybės žymenį, išduodančiosios institucijos pavadinimą, išdavimo datą,
 - kortelės galiojimo pradžios ir pabaigos datą (jei yra).

5.4.2. Kortelės turėtojo identifikacija

- 232 Kontrolės kortelė turi gebėti laikyti atmintyje tokius jos turėtojo identifikacijos duomenis:
- kontrolės institucijos pavadinimą,
 - kontrolės institucijos adresą,
 - turėtojo pavardę,
 - turėtojo vardą (-us),
 - pageidaujamą kalbą.

5.4.3. Duomenys apie kontrolės veiklą

- 233 Kontrolės kortelė turi gebėti laikyti atmintyje tokius duomenis apie kontrolės veiklą:
- kontrolės datą ir laiką,
 - kontrolės rūšį (rodymas ekrane ir (arba) spausdinimas ir (arba) duomenų perkėlimas iš TPB ir (arba) duomenų perkėlimas iš kortelės),

- kurio laikotarpio duomenys perkelti (jei perkeliama duomenys),
- transporto priemonės TPRN ir registruojančiosios valstybės narės, kurioje buvo atliekama kontrolė, žymenį,
- patikrintos vairuotojo kortelės numerį ir išduodančiosios valstybės narės žymenį.

234 Kontrolės kortelė turi gebėti išlaikyti atmintyje ne mažiau kaip 230 tokių įrašų.

5.5. Įmonės kortelė

5.5.1. Kortelės identifikacija

235 Įmonės kortelė turi gebėti laikyti atmintyje tokius kortelės identifikacijos duomenis:

- kortelės numerį,
- išduodančiosios valstybės, išduodančiosios institucijos pavadinimą, išdavimo datą,
- kortelės galiojimo pradžios ir pabaigos datą (jei yra).

5.5.2. Kortelės turėtojo identifikacija

236 Įmonės kortelė turi gebėti laikyti atmintyje tokius jos turėtojo identifikacijos duomenis:

- įmonės pavadinimą,
- įmonės adresą.

5.5.3. Duomenys apie įmonės veiklą

237 Įmonės kortelė turi gebėti laikyti atmintyje tokius duomenis apie įmonės veiklą:

- veiklos datą ir laiką,
- veiklos rūšį (TPB užrakinimas ir (arba) atrakinimas ir (arba) duomenų perkėlimas iš TPB ir (arba) duomenų perkėlimas iš kortelės),
- kurio laikotarpio duomenys perkelti (jei perkeliama duomenys),
- transporto priemonės TPRN ir registruojančiosios valstybės narės, kurioje buvo atliekama kontrolė, žymenį,
- kortelės numerį ir išduodančiosios valstybės narės žymenį.

238 Įmonės kortelė turi gebėti išlaikyti atmintyje ne mažiau kaip 230 tokių įrašų.

V. TACHOGRAFO ĮRENGIMAS

1. Įrengimas

239 Nauji tachografo prietaisai pristatomi montuotojams arba transporto priemonių gamintojams neaktyvuoti, visi III skyriaus 20 poskyryje išvardyti kalibravimo parametrai yra nustatyti ties reikiamomis ir galiojančiomis numatytosiomis vertėmis. Jei nėra tinkama kuri nors konkreti vertė, vietoj raidinių parametrų turi būti įrašyta klaustukų eilutė, o skaitmeniniai parametrai nustatyti ties 0.

240 Prieš aktyvuojant tachografas turi leisti pasinaudoti kalibravimo funkcija net ir ne kalibravimo režimu.

241 Prieš aktyvuojant tachografas turi neregistruoti ir nelaikyti duomenų, nurodytų III skyriaus 12.3–12.9 ir 12.12–12.14 poskyriuose.

242 Montuodamas transporto priemonės gamintojas nustato visus žinomus parametrus.

- 243 Transporto priemonių gamintojai arba montuotojai aktyvuoja įrengtą tachografą iki transporto priemonei išvažiuojant iš montavimo patalpų.
- 244 Tachografaai aktyvuojami automatiškai, pirmą kartą įkišus į bet kurią kortelių sąsajos įtaisą dirbtuvių kortelę.
- 245 Ypatingos judesio jutiklio ir transporto priemonės bloko sujungimo operacijos (jei jų reikia) turi būti automatiškai atliekamos prieš arba aktyvavimo metu.
- 246 Aktyvuotas tachografas turi imti visiškai tinkamai veikti ir taikyti prieigos prie duomenų teises.
- 247 Aktyvavus turi imti visiškai tinkamai veikti tachografo registravimo ir duomenų laikymo funkcijos.
- 248 Po įrengimo atliekamas kalibravimas. Per pirmąjį kalibravimą įvedamas TPRN. Kalibravimas atliekamas per dvi savaites po įrengimo arba TPRN priskyrimo – kas būna vėliau.
- 248a Tachografas turi būti įrengtas tokioje transporto priemonės vietoje, kad savo sėdynėje sėdėdamas vairuotojas galėtų naudotis reikiamomis jo funkcijomis.

2. Įrengimo plokštelė

- 249 Ant įrengiant patikrinto tachografo, jame ar prie jo turi būti pritvirtinta aiškiai matoma ir lengvai prieinama įrengimo plokštelė. Po kiekvienos patvirtinto montuotojo arba dirbtuvių patikros vietoje senesnės turi būti pritvirtinta nauja plokštelė.
- 250 Plokštelėje turi būti bent tokia informacija:
- patvirtinto montuotojo pavardė ar dirbtuvės pavadinimas, adresas ir firmos pavadinimas,
 - transporto priemonės būdingasis koeficientas: „ $w = \text{imp./km}$ “,
 - tachografo konstanta: „ $k = \text{imp./km}$ “,
 - padangų efektyvusis apskritimo ilgis: „ $1 = \dots \text{ mm}$ “,
 - padangų dydis,
 - transporto priemonės charakteristikos koeficiento nustatymo ir padangų efektyviojo apskritimo ilgio išmatavimo data,
 - transporto priemonės identifikacijos numeris.

3. Plombavimas

- 251 Užplombuojamos tokios dalys:
- visos jungtys, kurias išardžius atsirastų neaptinkamų pokyčių arba neaptinkamai dingtų duomenys,
 - įrengimo plokštelė, nebent ji būtų pritvirtinta taip, kad plokštelę būtų galima nuimti tik sugadinus jos žymenis.
- 252 Pirmiau išvardytas plombas leidžiama nuimti:
- avariniu atveju,
 - įrengiant, reguliuojant ar remontuojant greičio ribotuvą arba kokį nors kitą kelių eismo saugumą užtikrinantį įtaisą, jeigu tachografas tebeveikia patikimai, be sutrikimų ir iš karto sumontavus greitį reguliuojantį arba kokį nors kitą kelių eismo saugą užtikrinantį įtaisą, o kitais atvejais – per septynias dienas; jį iš naujo užplombuoja patvirtintas montuotojas arba dirbtuvės (laikantis VI skyriaus nuostatų).

- 253 Kiekvieną kartą nuėmus plombas turi būti surašomas aktas, kuriame nurodomos to priežastys ir kuris turi būti pateiktas kompetentingai institucijai.

VI. TIKRINIMAI, PATIKROS IR REMONTAS

Reikalavimai dėl atvejų, kuriais leidžiama nuimti plombas, kaip nurodyta Reglamento (EEB) Nr. 3821/85 su paskutiniais pakeitimais, padarytais Reglamentu (EB) Nr. 2135/98, 12 straipsnio 5 dalyje, apibrėžti šio priedo V skyriaus 3 poskyryje.

1. Montuotojų arba dirbtuvių patvirtinimas

Valstybės narės patvirtina, reguliariai kontroliuoja ir sertifikuoja institucijas, kurios atlieka:

- montavimo darbus,
- tikrinimus,
- patikras,
- remontą.

Pagal šio reglamento 12 straipsnio 1 dalies nuostatas dirbtuvių kortelės išduodamos tik tokiems montuotojams ir (arba) dirbtuvėms, kuriems yra leista aktyvuoti ir (arba) kalibruoti tachografus pagal šio priedo nuostatas (išskyrus atvejus, kai tinkamai pateisinama):

- kurie negali gauti įmonės kortelės,
- kurių kita profesinė veikla nesudaro galimybės pakenkti bendram sistemos apsaugotumui, kaip apibrėžta 10 priedėlyje.

2. Naujų arba suremontuotų prietaisų patikrinimas

- 254 Kiekvienas naujas ar pataisytas įtaisas turi būti patikrinamas, ar tinkamai veikia, tiksliai rodo bei registruoja ir yra sukalibruotas, atsižvelgiant į III skyriaus 2.1 ir 2.2 punktuose nustatytas ribas, ir užplombuojamas pagal V skyriaus 3 poskyrio nuostatas.

3. Įrengimo patikra

- 255 Įrengiant transporto priemonėje, visa sistema (įskaitant patį tachografą) turi atitikti III skyriaus 2.1 ir 2.2 poskyriuose nurodytus didžiausius leistinus nuokrypius.

4. Periodinės patikros

- 256 Transporto priemonėse sumontuota įranga turi būti periodiškai tikrinama po kiekvieno jos remonto, kiekvienąkart pasikeitus transporto priemonės būdingajam koeficientui ar padangų efektyviajam apskritimo ilgiui, jei įrangos UTC laiko rodmuo skiriasi nuo tikrojo laiko daugiau kaip 20 minučių, pasikeitus TPRN arba bent kartą per dvejus metus (24 mėnesius) po paskutinės patikros.

- 257 Patikros metu turi būti tikrinama:

- ar tachografas veikia tinkamai, įskaitant duomenų laikymo tachografo kortelėse funkciją,
- ar įranga atitinka III skyriaus 2.1 ir 2.2 poskyriuose nurodytus didžiausius leistinus nuokrypius;
- ar tachografas yra su tipo patvirtinimo ženklu,
- ar pritvirtinta įrengimo plokštelė,
- ar nepažeistos tachografo ir kitų jo įrangos dalių plombos,
- padangų dydis ir tikrasis jų apskritimo ilgis.

- 258 Per šias patikras tachografas turi būti sukalibruojamas.

5. Paklaidų matavimas

- 259 Tachografą įmontavus ir eksploatuojant, paklaidos nustatomos toliau išvardytais būdais, laikytinai standartinėmis bandymo sąlygomis:
- parengta važiuoti nepakrauta transporto priemonė,
 - slėgis padangose pagal gamintojo instrukcijas,
 - padangos nusidėvėjusios ne daugiau, nei leidžia nacionaliniai įstatymai,
 - transporto priemonės judėjimas:
 - savo varikliu varoma transporto priemonė važiuoja tiesia linija lygiu keliu $50 \text{ km/h} \pm 5 \text{ km/h}$ greičiu. Matavimo atstumas turi būti ne trumpesnis kaip 1 000 m,
 - bandymą galima daryti ir kitais būdais, pvz., bandymų stende, jei jų rezultatų tikslumas panašus.

6. Remontas

- 260 Dirbtuvės turi gebėti perkelti duomenis iš tachografo, kad galėtų juos pateikti atitinkamai transporto įmonei.
- 261 Jei dėl tachografo gedimo, net atlikus dirbtuvėse remontą, jame įrašytų duomenų perkelti neįmanoma, patvirtintos dirbtuvės turi išduoti transporto įmonėms duomenų neperkeliamumo pažymėjimą. Dirbtuvės saugo kiekvieno išduoto pažymėjimo kopiją ne trumpiau kaip metus.

VII. KORTELĖS IŠDAVIMAS

Valstybių narių nustatyta kortelių išdavimo tvarka turi atitikti tokius reikalavimus:

- 262 Pirmą kartą išduodant tachografo kortelę pareiškėjui, jos numeracijos indeksas (jei naudojamas) ir pakeitimo indeksas turi būti nustatyti ties 0.
- 263 Visos vienai kontrolės institucijai, vienerioms dirbtuvėms ar vienai transporto įmonei išduodamos neasmeninės kortelės turi būti su pirmaisiais 13 skaitmenų ir turėti skirtingus numeracijos indeksus.
- 264 Vietoj esamos tachografo kortelės išduodamos ją pakeičiančios kortelės numeris turi būti toks pats, kaip ir pakeistosios, tik pakeitimo indeksas didinamas viena pozicija (tokia seka: 0, ..., 9, A, ..., Z).
- 265 Vietoj esamos tachografo kortelės išduodamos ją pakeičiančios kortelės galiojimo pabaigos data turi būti tokia pati, kaip ir pakeistosios.
- 266 Vietoj esamos tachografo kortelės išduodamos ją atnaujinančios kortelės numeris turi būti toks pats, kaip ir pakeistosios, tik pakeitimo indeksas grąžinamas į 0, o atnaujinimo indeksas didinamas viena pozicija (tokia seka: 0, ..., 9, A, ..., Z).
- 267 Jei esama tachografo kortelė administravimo duomenims pakeisti keičiama toje pačioje valstybėje narėje, laikomasi atnaujinimo taisyklių, jei kitoje valstybėje narėje – pirmojo išdavimo taisyklių.
- 268 Neasmeninių dirbtuvių ar kontrolės kortelių eilutėje „kortelės turėtojo pavardė“ įrašomas dirbtuvių arba kontrolės institucijos pavadinimas.

VIII. TACHOGRAFŲ IR TACHOGRAFO KORTELIŲ TIPO PATVIRTINIMAS

1. Pagrindinės nuostatos

Šiame skyriuje žodžiai „tachografas“ reiškia „tachografą arba jo komponentus“. Tipo patvirtinimas nereikalingas judesio jutiklį su TPB jungiantiems laidams. Tachografo naudojamas popierius laikomas tachografo komponentu.

- 269 Tachografas pateikiamas tvirtinti kartu su visais įmontuotais papildomais įtaisais.
- 270 Tvirtinant tachografo ir tachografo kortelių tipą atliekami apsaugotumo, veikimo ir funkcinio suderinamumo bandymai. Jei šių bandymų rezultatai tinkami, tai nurodoma atitinkamame pažymėjime.
- 271 Valstybių narių tipo patvirtinimo institucijos suteikia tipo patvirtinimo sertifikatą pagal šio reglamento 5 straipsnio nuostatas tik gavusios tipo patvirtinimo paraiškoje nurodyto tachografo arba tachografo kortelės:
- apsaugotumo pažymėjimą,
 - veikimo pažymėjimą,
 - funkcinio suderinamumo pažymėjimą.
- 272 Prieš pakeičiant tachografo programinę arba techninę įrangą arba medžiagas, iš kurios jis gaminamas, pranešama tipo patvirtinimą tachografui suteikusiai institucijai. Ši institucija patvirtina gamintojui pratešianti tipo patvirtinimą arba gali pareikalauti gauti naujus veikimo, apsaugotumo ir (arba) funkcinio suderinamumo pažymėjimus.
- 273 Tachografo programinės įrangos tobulinimo in situ tvarka turi būti patvirtinta tipo patvirtinimą tachografui suteikusios institucijos. Programinę įrangą tobulinant neturi būti nei pakeista, nei ištrinta jokių tachografe laikomų duomenų apie vairuotojo veiklą. Programinę įrangą tobulinti galima tik tuomet, kai už tai atsako įrangos gamintojas.

2. Apsaugos pažymėjimas

- 274 Apsaugos pažymėjimas išduodamas laikantis šio priedo 10 priedėlio nuostatų.

3. Veikimo pažymėjimas

- 275 Kiekvienas pageidaujantis gauti tipo patvirtinimo sertifikatą pateikia valstybės narės tipo patvirtinimo institucijai visą jos pareikalautą medžiagą ir dokumentaciją.
- 276 Veikimo pažymėjimas išduodamas tik tuomet, jei visų 9 priedėlyje nurodytų veikimo bandymų rezultatai yra tinkami.
- 277 Veikimo pažymėjimą išduoda tipo patvirtinimo institucija. Pažymėjime nurodomas jos gavėjo pavadinimas, modelio identifikacija, išsamus atliktų bandymų sąrašas ir gauti rezultatai.

4. Funkcinio suderinamumo pažymėjimas

- 278 Funkcinio suderinamumo bandymus atlieka viena Europos Komisijos įgaliota laboratorija, už kurią atsako Komisija.
- 279 Laboratorija registruoja gamintojų pateikiamus funkcinio suderinamumo bandymų prašymus chronologine jų gavimo tvarka.
- 280 Prašymai oficialiai registruojami pateikus laboratorijai:
- funkcinio suderinamumo bandymams reikalingą medžiagą ir dokumentus,
 - atitinkamą apsaugos pažymėjimą,
 - atitinkamą veikimo pažymėjimą.
- Gamintojui pranešama prašymo įregistravimo data.
- 281 Laboratorija neatlieka funkcinio suderinamumo bandymų su tais tachografais arba tachografo kortelėmis, kuriems nesuteikti apsaugos ir veikimo pažymėjimai.
- 282 Visi prašantys atlikti funkcinio suderinamumo bandymus gamintojai įsipareigoja palikti už tokius bandymus atsakingai laboratorijai visą medžiagą ir reikiamus dokumentus.

Funkcinio suderinamumo bandymai pagal šio priedo 9 priedėlio 5 dalies nuostatas turi būti atliekami su visų rūšių tachografais arba tachografo kortelėmis:

- kurių tipo patvirtinimas tebegalioja,
- kuriems turi būti suteiktas patvirtinimas ir kurie turi galiojantį funkcinio suderinamumo pažymėjimą.

- 284 Laboratorija išduoda funkcinio suderinamumo pažymėjimą gamintojui tik sėkmingai atlikus visus reikiamus funkcinio suderinamumo bandymus.
- 285 Jei 283 reikalavime reikalaujami vieno ar daugiau tachografų arba tachografo kortelių funkcinio suderinamumo bandymų rezultatai yra netinkami, funkcinio suderinamumo pažymėjimas neišduodamas, kol gamintojas nepadarys reikiamų pakeitimų ir įranga išlaikys bandymus. Padedama atitinkamų gamintojų laboratorija nustato nesklandumo priežastį ir stengiasi padėti gamintojui rasti techninį sprendimą. Jei gamintojas modifikavo savo gaminį, jis turi gauti atitinkamų institucijų patvirtinimą, kad apsaugotumo ir veikimo pažymėjimai tebegalioja.
- 286 Funkcinio suderinamumo pažymėjimas galioja šešis mėnesius. Jis atšaukiamas, jei gamintojas negauna atitinkamo tipo patvirtinimo sertifikato. Gamintojas pateikia funkcinio suderinamumo pažymėjimą valstybės narės tipo patvirtinimo institucijai, išdavusiai veikimo pažymėjimą.
- 287 Bet kuris funkcinį nesuderinamumą sukėlęs elementas neturi būti naudojamas pelnui gauti arba padėti pirmavimui pasiekti.

5. Tipo patvirtinimo sertifikatas

- 288 Valstybės narės tipo patvirtinimo institucija gali išduoti tipo patvirtinimo sertifikatą, kai tik gauna reikiamus pažymėjimus.
- 289 Išduodant tipo patvirtinimo sertifikatą gamintojui, jo kopija išsiunčiama už funkcinio suderinamumo bandymus atsakingai laboratorijai.
- 290 Už funkcinio suderinamumo bandymus atsakinga laboratorija turi turėti svetainę internete, kurioje skelbiamas ir atnaujinamas tokių tachografų ir tachografo kortelių modelių sąrašas:
- dėl kurių buvo užregistruoti funkcinio suderinamumo bandymų prašymai;
 - kuriems buvo išduotas funkcinio suderinamumo pažymėjimas (net ir laikinasis);
 - kuriems buvo išduotas tipo patvirtinimo sertifikatas.

6. Išskirtinė tvarka: pirmieji funkcinio suderinamumo pažymėjimai

- 291 Keturių mėnesių laikotarpį po to, kai patvirtinama, kad pirmoji tachografo ir tachografo kortelės (vairuotojo, dirbtuvių, kontrolės ir įmonės kortelių) pora yra funkciškai suderinama, visi pagal tą laikotarpį įregistruotus prašymus išduoti funkcinio suderinamumo pažymėjimai (įskaitant ir patį pirmąjį) yra laikinieji.
- 292 Šiam laikotarpiui praėjus visų funkciškai suderinamų gaminių funkcinio suderinamumo pažymėjimai laikomi nuolatiniais.
- 293 Jei per šį laikotarpį aptinkama funkcinio suderinamumo nesklandumų, už funkcinio suderinamumo bandymus atsakinga laboratorija, padedama visų susijusių gamintojų, turi nustatyti nesklandumų priežastis ir pasiūlyti jiems padaryti reikiamas modifikacijas.
- 294 Jei pasibaigus šiam laikotarpiui lieka funkcinio suderinamumo nesklandumų, už funkcinio suderinamumo bandymus atsakinga laboratorija, kartu su susijusiais gamintojais ir atitinkamus veikimo pažymėjimus išdavusiomis tipo patvirtinimo institucijomis turi rasti funkcinio suderinamumo nesklandumų priežastis ir nustatyti, kokiais modifikacijomis turi padaryti kiekvienas susijęs gamintojas. Techninių sprendimų turi būti ieškoma ne ilgiau kaip du mėnesius, o jei per tą laiką bendro sprendimo nerandama, Komisija, pasikonsultavusi su už funkcinio suderinamumo bandymus atsakinga laboratorija, turi nuspręsti, kuris tachografas (ar tachografai) ir kortelės gauna nuolatinį funkcinio suderinamumo pažymėjimą, ir turi nurodyti to priežastis.
- 295 Funkcinio suderinamumo bandymų prašymai, įregistruoti laboratorijoje nuo keturių mėnesių laikotarpio po pirmo laikinojo funkcinio suderinamumo pažymėjimo išdavimo pabaigos iki 294 reikalavime nurodyto Komisijos sprendimo priėmimo datos, atidedami iki bus sutvarkyti pradiniai funkcinio suderinamumo nesklandumai. Vėliau tokie prašymai nagrinėjami chronologine jų registracijos tvarka.

1 priedėlis

DUOMENŲ ŽODYNĖLIS

Turinys

1.	Įvadas	332
1.1.	Duomenų tipų apibrėžimo metodas	332
1.2.	Nuorodos	332
2.	Duomenų tipų apibrėžimai	333
2.1.	ActivityChangeInfo	333
2.2.	Address	334
2.3.	BCDString	334
2.4.	CalibrationPurpose	334
2.5.	CardActivityDailyRecord	335
2.6.	CardActivityLengthRange	335
2.7.	CardApprovalNumber	335
2.8.	CardCertificate	335
2.9.	CardChipIdentification	335
2.10.	CardConsecutiveIndex	336
2.11.	CardControlActivityDataRecord	336
2.12.	CardCurrentUse	336
2.13.	CardDriverActivity	336
2.14.	CardDrivingLicenceInformation	337
2.15.	CardEventData	337
2.16.	CardEventRecord	337
2.17.	CardFaultData	338
2.18.	CardFaultRecord	338
2.19.	CardIccIdentification	338
2.20.	CardIdentification	339
2.21.	CardNumber	339
2.22.	CardPlaceDailyWorkPeriod	339
2.23.	CardPrivateKey	340
2.24.	CardPublicKey	340
2.25.	CardRenewalIndex	340
2.26.	CardReplacementIndex	340
2.27.	CardSlotNumber	340
2.28.	CardSlotsStatus	340
2.29.	CardStructureVersion	341

2.30.	CardVehicleRecord	341
2.31.	CardVehiclesUsed	341
2.32.	Certificate	342
2.33.	CertificateContent	342
2.34.	CertificateHolderAuthorisation	342
2.35.	CertificateRequestID	343
2.36.	CertificationAuthorityKID	343
2.37.	CompanyActivityData	343
2.38.	CompanyActivityType	344
2.39.	CompanyCardApplicationIdentification	344
2.40.	CompanyCardHolderIdentification	344
2.41.	ControlCardApplicationIdentification	345
2.42.	ControlCardControlActivityData	345
2.43.	ControlCardHolderIdentification	345
2.44.	ControlType	346
2.45.	CurrentDateTime	346
2.46.	DailyPresenceCounter	346
2.47.	Datef	347
2.48.	Distance	347
2.49.	DriverCardApplicationIdentification	347
2.50.	DriverCardHolderIdentification	347
2.51.	EntryTypeDailyWorkPeriod	348
2.52.	EquipmentType	348
2.53.	EuropeanPublicKey	348
2.54.	EventFaultType	348
2.55.	EventFaultRecordPurpose	349
2.56.	ExtendedSerialNumber	350
2.57.	FullCardNumber	350
2.58.	HighResOdometer	350
2.59.	HighResTripDistance	350
2.60.	HolderName	350
2.61.	K-ConstantOfRecordingEquipment	351
2.62.	KeyIdentifier	351
2.63.	L-TyreCircumference	351
2.64.	Language	351
2.65.	LastCardDownload	351
2.66.	ManualInputFlag	351
2.67.	ManufacturerCode	352

2.68.	MemberStateCertificate	352
2.69.	MemberStatePublicKey	353
2.70.	Name	353
2.71.	NationAlpha	353
2.72.	NationNumeric	354
2.73.	NoOfCalibrationRecords	355
2.74.	NoOfCalibrationSinceDownload	355
2.75.	NoOfCardPlaceRecords	355
2.76.	NoOfCardVehicleRecords	355
2.77.	NoOfCompanyActivityRecords	355
2.78.	NoOfControlActivityRecords	356
2.79.	NoOfEventsPerType	356
2.80.	NoOfFaultsPerType	356
2.81.	OdometerValueMidnight	356
2.82.	OdometerShort	356
2.83.	OverspeedNumber	356
2.84.	PlaceRecord	356
2.85.	PreviousVehicleInfo	357
2.86.	PublicKey	357
2.87.	RegionAlpha	357
2.88.	RegionNumeric	357
2.89.	RSAPublicModulus	358
2.90.	RSAPublicExponent	358
2.91.	RSAPublicExponent	358
2.92.	SensorApprovalNumber	358
2.93.	SensorIdentification	358
2.94.	SensorInstallation	359
2.95.	SensorInstallationSecData	359
2.96.	SensorOSIdentifier	359
2.97.	SensorPaired	359
2.98.	SensorPairingDate	360
2.99.	SensorSerialNumber	360
2.100.	SensorSCIdentifier	360
2.101.	Signature	360
2.102.	SimilarEventsNumber	360
2.103.	SpecificConditionType	360
2.104.	SpecificConditionRecord	360
2.105.	Speed	361

2.106.	SpeedAuthorised	361
2.107.	SpeedAverage	361
2.108.	SpeedMax	361
2.109.	TdesSessionKey	361
2.110.	TimeReal	361
2.111.	TyreSize	361
2.112.	VehicleIdentificationNumber	362
2.113.	VehicleRegistrationIdentification	362
2.114.	VehicleRegistrationNumber	362
2.115.	VuActivityDailyData	362
2.116.	VuApprovalNumber	362
2.117.	VuCalibrationData	362
2.118.	VuCalibrationRecord	363
2.119.	VuCardIWDData	363
2.120.	VuCardIWRRecord	364
2.121.	VuCertificate	364
2.122.	VuCompanyLocksData	364
2.123.	VuCompanyLocksRecord	365
2.124.	VuControlActivityData	365
2.125.	VuControlActivityRecord	365
2.126.	VuDataBlockCounter	365
2.127.	VuDetailedSpeedBlock	365
2.128.	VuDetailedSpeedData	366
2.129.	VuDownloadablePeriod	366
2.130.	VuDownloadActivityData	366
2.131.	VuEventData	366
2.132.	VuEventRecord	367
2.133.	VuFaultData	367
2.134.	VuFaultRecord	367
2.135.	VuIdentification	368
2.136.	VuManufacturerAddress	368
2.137.	VuManufacturerName	368
2.138.	VuManufacturingDate	368
2.139.	VuOverSpeedingControlData	369
2.140.	VuOverSpeedingEventData	369
2.141.	VuOverSpeedingEventRecord	369
2.142.	VuPartNumber	369
2.143.	VuPlaceDailyWorkPeriodData	370

2.144.	VuPlaceDailyWorkPeriodRecord	370
2.145.	VuPrivateKey	370
2.146.	VuPublicKey	370
2.147.	VuSerialNumber	370
2.148.	VuSoftInstallationDate	370
2.149.	VuSoftwareIdentification	370
2.150.	VuSoftwareVersion	371
2.151.	VuSpecificConditionData	371
2.152.	VuTimeAdjustmentData	371
2.153.	VuTimeAdjustmentRecord	371
2.154.	W-VehicleCharacteristicConstant	371
2.155.	WorkshopCardApplicationIdentification	372
2.156.	WorkshopCardCalibrationData	372
2.157.	WorkshopCardCalibrationRecord	372
2.158.	WorkshopCardHolderIdentification	373
2.159.	WorkshopCardPIN	373
3.	Verčių ir dydžių ribos	374
3.1.	Vairuotojo kortelės verčių ribos	374
3.2.	Dirbtuvių kortelės verčių ribos	374
3.3.	Kontrolės kortelės verčių ribos	374
3.4.	Įmonės kortelės verčių ribos	374
4.	Rašmenų rinkiniai	374
5.	Kodavimas	374

1. ĮVADAS

Šiame priedėlyje nustatyti tachografe ir tachografo kortelėse naudojami duomenų formatai, duomenų elementai ir duomenų struktūra.

1.1. Duomenų tipų apibrėžimo metodas

Šiame priedėlyje duomenų tipai apibrėžiami kalba ASN.1. Ji leidžia paprastus ir struktūrizuotus duomenis apibrėžti nenaudojant jokios specialios perkėlimo sintaksės (kodavimo taisyklių), kuri būtų priklausoma nuo programos ir aplinkos.

ASN.1 tipų pavadinimų sudarymo taisyklės nustatytos pagal ISO/IEC 8824-1. Tai reiškia, kad:

- kiek įmanoma, duomenų tipo prasmė nusakoma parenkant pavadinimą,
- kai duomenų tipas susideda iš kitų duomenų tipų, duomenų tipo pavadinimas yra viena raidžių seka, prasidedanti didžiąja raide, o kitos didžiosios raidės pavadinime naudojamos atskiriems žodžiams išskirti,
- šiaip jau duomenų tipų pavadinimai susiję su duomenų tipų, iš kurių jie sudaryti, įrangos, kurioje duomenys laikomi, ir su duomenimis susijusios funkcijos pavadinimais.

Jei ASN.1 tipas jau apibrėžtas kitame standarte ir jei jis tinka naudoti tachografuose, tuomet šiame priedėlyje bus nurodytas būtent šis ASN.1 tipas.

Tam, kad būtų galima taikyti kelių rūšių kodavimo taisykles, kai kurie ASN.1 tipai šiame priedėlyje apriboti verčių diapazono vardais. Verčių diapazono vardai nurodyti 3 skyriuje.

1.2. Nuorodos

Šiame Priedėlyje naudoti tokie šaltiniai:

ISO 639	Kalbų pavadinimų pateikimo kodas. Pirmasis leidimas: 1988 m.
EN 726-3	Identifikacijos kortelių sistemos. Telekomunikacijų kortelės su integriniais grandynais ir terminalai. 3 dalis. Nuo programos nepriklausomų kortelių reikalavimai. 1994 m. gruodžio mėn.
ISO 3779	Kelių transporto priemonės. Transporto priemonių identifikacijos numeris (TPIN). Turinys ir sandara. 3 leidimas: 1983 m.
ISO/IEC 7816-5	Informacinė technologija. Identifikacijos kortelės. Kortelės su integriniais grandynais ir kontaktais. 5 dalis. Programų vardų numeravimo sistema ir registravimo tvarka. Pirmasis leidimas: 1994 m. + 1 pataisa: 1996 m.
ISO/IEC 8824-1	Informacinė technologija. Abstrakčios sintaksės žymėjimo sistema 1 (ASN.1). Pagrindinės žymėjimo sistemos specifikacija. 2 leidimas: 1998 m.
ISO/IEC 8825-2	Informacinė technologija. Kodavimo naudojant ASN.1 taisyklės. Paketinio kodavimo taisyklės (PER). 2 leidimas: 1998 m.
ISO/IEC 8859-1	Informacinė technologija. 8 bitų vienu baitu užkoduotų grafinių simbolių rinkiniai. 1 dalis. Lotyniška abėcėlė Nr. 1. Pirmasis leidimas: 1987 m.
ISO/IEC 8859-7	Informacinė technologija. 8 bitų vienu baitu užkoduotų grafinių simbolių rinkiniai. 7 dalis. Lotynų ir graikų abėcėlė. Pirmasis leidimas: 1987 m.
ISO 16844-3	Kelių transporto priemonės. Tachografų sistemos. Judesio jutiklio sąsaja. WD 3-20/05/99.

2. DUOMENŲ TIPŲ APIBRĖŽIMAI

Bet kurių toliau nurodytų duomenų tipų numatytoji „nežinomo“ arba „netaikytino“ turinio vertė sudaroma duomenų elementą užpildant „FF“ baitais.

2.1. ActivityChangeInfo

Šiuo duomenų tipu dviejų baitų ilgio žodžiu užkoduojama vairuotojo arba vairuotojo porininko kortelės plyšio būsena 00.00 val. ir (arba) vairuotojo būsena 00.00 val. ir (arba) važiavimo būsenos pasikeitimai ir (arba) kortelės būsenos pasikeitimai. Šis duomenų tipas susijęs su 084, 109a, 199 ir 219 reikalavimais.

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

Priskiriamos vertės – Sinchronizavimas pagal okteta: 'scpaattttttttttt'B (16 bitų)

Irašams duomenų atmintyje (arba plyšio būseną):

's'B	Plyšys:
	'0'B: VAIRUOTOJAS,
	'1'B: VAIRUOTOJAS PORININKAS,
'c'B	Važiavimo būsena:
	'0'B: VIENAS VAIRUOTOJAS,
	'1'B: ĮGULA,
'p'B	Vairuotojo (arba dirbtuvių) kortelės būsena atitinkamame plyšyje:
	'0'B: ĮKIŠTA, kortelė įkišta,
	'1'B: NEĮKIŠTA, kortelė neįkišta (arba ištraukta),
'aa'B	Veikla:
	'00'B: PERTRAUKA/POILSIS,
	'01'B: BUVIMAS PASIRENGUS DIRBTI,
	'10'B: DARBAS,
	'11'B: VAIRAVIMAS
'ttttttttttttt'B	Pokyčio laikas: minučių skaičius nuo tos dienos 00.00 val.

Irašams vairuotojo (arba dirbtuvių) kortelės atmintyje (ir vairuotojo būsena):

's'B	Plyšys (netaikytina, kai 'p' = 1, išskyrus kaip nurodyta pastaboje):
	'0'B: VAIRUOTOJAS,
	'1'B: 2. VAIRUOTOJAS PORININKAS,
'c'B	Važiavimo būsena (kai 'p' = 0) arba Kita veiklos būsena (kai 'p' = 1):
	'0'B: VAIRUOTOJAS, '1'B: ĮGULA
	'0'B: NEŽINOMA '1'B: ŽINOMA (= įvesta rankomis)
'p'B	Kortelės būsena:
	'0'B: ĮKIŠTA, kortelė įkišta į tachografą,
	'1'B: NEĮKIŠTA, kortelė neįkišta (arba ištraukta),

'aa'B Veikla (netaikytina, kai 'p' = 1 ir 'c' = 0, išskyrus kaip nurodyta pastaboje):

'00'B: PERTRAUKA/POILSIS,

'01'B: BUVIMAS PASIRENGUS DIRBTI,

'10'B: DARBAS,

'11'B: VAIRAVIMAS,

'ttttttttttt'B Pokyčio laikas: minučių skaičius nuo tos dienos 00.00 val.

Pastaba atvejui „kortelės ištraukimas“

Kai kortelė ištraukiama:

- 's' taikytina ir nurodo plyšį, iš kurio kortelė buvo ištraukta,
- 'c' turi būti nustatyta į 0,
- 'p' turi būti nustatyta į 1,
- 'aa' turi koduoti tuo metu pasirinktą veiklą.

Įvedant rankomis žodžio bitai 'c' ir 'aa' (laikomi kortelės atmintyje) vėliau gali būti perrašyti, kad matytųsi, kas buvo įvesta.

2.2. Address

Adresas.

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

codePage nurodo ISO/IEC 8859 dalį, kuri buvo naudota adresui užkoduoti.

address adresas, užkoduotas pagal ISO/IEC 8859-codePage.

2.3. BCDString

BCDString naudojamas dešimtainiams skaitmenims pateikti dvejetainiu kodu (BCD). Šis duomenų tipas naudojamas vienam dešimtainiam skaitmeniui pateikti vienu pusiniu oktetu (4 bitais). BCDString paremtas „CharacterStringType“ pagal ISO/IEC 8824-1.

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

BCDString naudojama žymėjimo sistema „hstring“. Pats kairiausias šešioliktainis skaitmuo yra svarbiausias okteto pusinis oktetas. Jei reikia, daugiau oktetų sudaroma nuo paties kairiausio pusinio okteto pozicijos pirmajame oktete įterpian pusinius oktetus, kurie baigiasi nuliu.

Leidžiami tokie skaitmenys: 0, 1, ... 9.

2.4. CalibrationPurpose

Šis kodas paaiškina, kodėl buvo įrašytas kalibravimo parametrų rinkinys. Šis duomenų tipas susijęs su 097 ir 098 reikalavimais.

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

Priskiriamos vertės:

- '00'H rezervuoti vertė,
- '01'H aktyvavimas: žinomų kalibravimo parametrų įrašymas aktyvuojant TPB,

'02'H pirmasis įrengimas: pirmasis TPB kalibravimas atlikus jo aktyvavimą,

'03'H įrengimas: pirmasis TPB kalibravimas esamoje transporto priemonėje,

'04'H periodinė patikra.

2.5. CardActivityDailyRecord

Kortelės atmintyje laikoma informacija, susijusi su vairuotojo veikla konkrečią kalendorinę dieną. Šis duomenų tipas susijęs su 199 ir 219 reikalavimais.

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

activityPreviousRecordLength – ankstesnio dienos įrašo bendras ilgis baitais. Didžiausią galimą vertę apibrėžia OKTETO EILUTĖS, kurioje yra tie įrašai, ilgis (žr. 3 dalį – **CardActivityLengthRange**). Kai šis įrašas tampa seniausiu dienos įrašu, **activityPreviousRecordLength** vertė turi būti nustatyta į 0.

activityRecordLength – įrašo bendras ilgis baitais. Didžiausią galimą vertę apibrėžia OKTETO EILUTĖS, kurioje yra tie įrašai, ilgis.

activityRecordDate – įrašo data.

activityDailyPresenceCounter – kortelės buvimo tą dieną skaitiklis.

activityDayDistance – bendras tą dieną nuvažiuotas atstumas.

activityChangeInfo – **ActivityChangeInfo** duomenų rinkinys apie vairuotoją tą dieną. Jame gali būti ne daugiau kaip 1 440 verčių (vienas veiklos rūšies pasikeitimas per minutę). Šiame rinkinyje visuomet yra vairuotojo būsenos 00.00 val. **activityChangeInfo** kodas.

2.6. CardActivityLengthRange

Laisvų baitų įrašams apie vairuotojo veiklą skaičius vairuotojo arba dirbtuvių kortelės atmintyje.

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

Priskiriamos vertės: žr. 3 dalį.

2.7. CardApprovalNumber

Kortelės tipo patvirtinimo numeris.

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

Priskiriamos vertės: nenustatytos.

2.8. CardCertificate

Kortelės atvirojo rakto pažymėjimas.

```
CardCertificate ::= Certificate.
```

2.9. CardChipIdentification

Kortelės atmintyje laikoma informacija apie kortelės integrinio grandyno (IC) identifikaciją (191 reikalavimas).

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


activityPointerOldestDayRecord – seniausio užbaigto dienos įrašo eilutėje **activityDailyRecords** laikymo vietos pradžios nuoroda (baitų skaičius nuo eilutės pradžios). Didžiausią galimą vertę apibrėžia eilutės ilgis.

activityPointerNewestRecord – naujausio dienos įrašo eilutėje **activityDailyRecords** laikymo vietos pradžios nuoroda (baitų skaičius nuo eilutės pradžios). Didžiausią galimą vertę apibrėžia eilutės ilgis.

activityDailyRecords – duomenims apie vairuotojo veiklą kiekvieną kalendorinę dieną, kurią kortelė buvo naudojama, laikyti turima talpa (duomenų struktūra: **CardActivityDailyRecord**).

Priskiriamos vertės: į šią okteto eilutę cikliška įrašomi **CardActivityDailyRecord** įrašai. Pirmą kartą pradedama rašyti nuo pirmojo eilutės baido. Visi nauji įrašai prirašomi prie ankstesniųjų pabaigos. Kai eilutė užpildoma, vėl pradedama rašyti nuo pirmojo jos baido, neatsižvelgiant į tai, kad duomenų elementas pertraukiamas. Prieš įrašant į eilutę naujus duomenis apie veiklą (didinant esamą **activityDailyRecord** arba pradedant naują), kurie pakeičia senesnius duomenis, turi būti atnaujinamas parametras **activityPointerOldestDayRecord**, kuris nurodo naują seniausio užbaigto dienos įrašo vietą, o šio (naujo) seniausio užbaigto dienos įrašo parametras **activityPreviousRecord-Length** turi būti grąžintas į 0.

2.14. CardDrivingLicenceInformation

Vairuotojo kortelės atmintyje laikoma informacija, susijusi su kortelės turėtojo vairuotojo pažymėjimo duomenimis (196 reikalavimas).

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

drivingLicenceIssuingAuthority – už vairuotojo pažymėjimų išdavimą atsakinga institucija.

drivingLicenceIssuingNation – vairuotojo pažymėjimą išdavusios institucijos šalis.

drivingLicenceNumber – vairuotojo pažymėjimo numeris.

2.15. CardEventData

Vairuotojo arba dirbtuvių kortelės atmintyje laikoma informacija apie su kortelės turėtoju susijusius įvykius (204 ir 223 reikalavimai).

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

CardEventData – didėjančios **EventFaultType** vertės sąlygota įrašų **cardEventRecords** seka (išskyrus įrašus, susijusius su bandymais pažeisti apsaugą, kurie kaupiami paskutiniame sekos rinkinyje).

cardEventRecords – įrašų apie tam tikros rūšies (arba bandymo pažeisti apsaugą įvykių kategorijos) įvykius seka.

2.16. CardEventRecord

Vairuotojo arba dirbtuvių kortelės atmintyje laikoma informacija apie su kortelės turėtoju susijusį įvykį (205 ir 223 reikalavimai).

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

eventType – įvykio rūšis.

eventBeginTime – įvykio pradžios data ir laikas.

eventEndTime – įvykio pabaigos data ir laikas.

eventVehicleRegistration – transporto priemonės, kurioje įvykis įvyko, TPRN ir registruojančioji valstybė narė.

2.17. CardFaultData

Vairuotojo arba dirbtuvių kortelės atmintyje laikoma informacija apie su kortelės turėtoju susijusius gedimus (207 ir 223 reikalavimai).

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

CardFaultData – įrašų apie tachografo gedimus seka ir po jos einanti įrašų apie kortelės gedimus seka.

cardFaultRecords – įrašų apie tam tikros rūšies (tachografo arba kortelės) gedimus rinkinys.

2.18. CardFaultRecord

Vairuotojo arba dirbtuvių kortelės atmintyje laikoma informacija apie su kortelės turėtoju susijusį gedimą (208 ir 223 reikalavimai).

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

faultType – gedimo rūšis.

faultBeginTime – gedimo pradžios data ir laikas.

faultEndTime – gedimo pabaigos data ir laikas.

faultVehicleRegistration – transporto priemonės, kurioje gedimas įvyko, TPRN ir registruojančioji valstybė narė.

2.19. CardIccIdentification

Kortelės atmintyje laikoma kortelės su integriniu grandynu (IC) identifikacijos informacija (192 reikalavimus).

```
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 – EN 726-3 nustatytas **Clockstop** režimas.

cardExtendedSerialNumber – kortelės su integriniu grandynu serijos numeris ir pagaminimo žymuo, kaip nustatyta EN 726-3 ir kaip nurodo duomenų tipas **ExtendedSerialNumber**.

cardApprovalNumber – kortelės tipo patvirtinimo numeris.

cardPersonaliserID – kortelės suasmeninimo ID, kaip nurodyta EN 726-3.

embedderIcAssemblerId – įmontuotojo (IC surinkėjo) vardas, kaip nurodyta EN 726-3.

icIdentifier – kortelės IC ir IC gamintojo vardas, kaip nurodyta EN 726-3.

2.20. CardIdentification

Kortelės atmintyje laikoma informacija apie kortelės identifikaciją (194, 215, 231, 235 reikalavimai).

CardIdentification ::= SEQUENCE

```

    cardIssuingMemberState      NationNumeric,
    cardNumber                   CardNumber,
    cardIssuingAuthorityName     Name,
    cardIssueDate                TimeReal,
    cardValidityBegin            TimeReal,
    cardExpiryDate               TimeReal
}

```

cardIssuingMemberState – kortelę išduodančios valstybės narės kodas.

cardNumber – kortelės numeris.

cardIssuingAuthorityName – kortelę išdavusios institucijos pavadinimas.

cardIssueDate – kortelės išdavimo dabartiniam turėtoji data.

cardValidityBegin – kortelės galiojimo pradžios data.

cardExpiryDate – kortelės galiojimo pabaigos data.

2.21. CardNumber

Kortelės numeris pagal g apibrėžimą.

CardNumber ::= CHOICE {

```

    SEQUENCE {
        driverIdentification      IA5String(SIZE(14)),
        cardReplacementIndex      CardReplacementIndex,
        cardRenewalIndex           CardRenewalIndex
    }
    SEQUENCE {
        ownerIdentification        IA5String(SIZE(13)),
        cardConsecutiveIndex        CardConsecutiveIndex,
        cardReplacementIndex        CardReplacementIndex,
        cardRenewalIndex            CardRenewalIndex
    }
}

```

driverIdentification – unikali vairuotojo identifikacija valstybėje narėje.

ownerIdentification – unikali įmonės, dirbtuvių arba kontrolės institucijos identifikacija valstybėje narėje.

cardConsecutiveIndex – kortelės numeracijos indeksas.

cardReplacementIndex – kortelės pakeitimo indeksas.

cardRenewalIndex – kortelės atnaujinimo indeksas.

Pirmoji pasirinkama seka tinka užkoduoti vairuotojo kortelės numeriui, antroji – dirbtuvių, kontrolės ir įmonės kortelės numeriui.

2.22. CardPlaceDailyWorkPeriod

Vairuotojo arba dirbtuvių kortelės atmintyje laikoma informacija apie vietas, kuriose prasideda ir (arba) baigiasi dienos darbo laikotarpiai (202 ir 221 reikalavimai).

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

placePointerNewestRecord – paskutinio atnaujinto įrašo apie vietą indeksas.

Priskiriamos vertės: skaičius, atitinkantis įrašų apie vietas skaitiklio vertę; pirmojo struktūros įrašo apie vietas vertė yra 0.

placeRecords – informacijos apie įvestas vietas įrašų rinkinys.

2.23. CardPrivateKey

Kortelės slaptasis raktas.

```
CardPrivateKey ::= RSAKeyPrivateExponent.
```

2.24. CardPublicKey

Kortelės atvirasis raktas.

```
CardPublicKey ::= PublicKey.
```

2.25. CardRenewalIndex

Kortelės atnaujinimo indeksas (į apibrėžimas).

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

Priskiriamos vertės: (žr. šio priedo VII skyrių).

'0' Pirmasis išdavimas.

Didėjimo tvarka: '0, ..., 9, A, ..., Z'.

2.26. CardReplacementIndex

Kortelės pakeitimo indeksas (į apibrėžimas).

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

Priskiriamos vertės: (žr. šio priedo VII skyrių).

'0' Pirmoji kortelė.

Didėjimo tvarka: '0, ..., 9, A, ..., Z'.

2.27. CardSlotNumber

Du transporto priemonės bloko plyšius kortelėms atskirti naudojamas kodas.

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

Priskiriamos vertės: tiksliau nenustatyta.

2.28. CardSlotsStatus

Kodas, nurodantis, kokių rūšių kortelės įkištos į du transporto priemonės bloko plyšius kortelėms.

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

}

vehiclePointerNewestRecord – paskutinio atnaujinto transporto priemonės įrašo indeksas.

Priskiriamos vertės: skaičius, atitinkantis įrašų apie transporto priemonės skaitiklio vertę; pirmojo struktūros įrašo apie transporto priemonės vertė yra 0.

cardVehicleRecords – informacijos apie naudotas transporto priemonės įrašų rinkinys.

2.32. Certificate

Sertifikavimo institucijos išduodamas atvirasis raktas.

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

Priskiriamos vertės: skaitmeninis parašas, naudojant dalį **CertificateContent** pagal 11 priedėlį „Bendrieji apsaugos mechanizmai“. Parašas (128 baitai) || Atvirojo rakto liekana (58 baitai) || Sertifikavimo institucijos žymuo (8 baitai).

2.33. CertificateContent

Atvirojo rakto pažymėjimo (grynasis) turinys pagal 11 priedėlį „Bendrieji apsaugos mechanizmai“.

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

certificateProfileIdentifier – atitinkamo pažymėjimo versija.

Priskiriamos vertės: '01h' (šios versijos).

CertificationAuthorityReference – žymi pažymėjimą išduodančią sertifikavimo instituciją. Jis taip pat žymi šios sertifikavimo institucijos atvirąjį raktą.

certificateHolderAuthorisation – žymi pažymėjimo turėtojo teises.

certificateEndOfValidity – pažymėjimo administracinio galiojimo pabaigos data.

certificateHolderReference – žymi pažymėjimo turėtoją. Taip pat žymi atvirąjį raktą.

publicKey – atvirasis raktas, kurį sertifikuoja šis pažymėjimas.

2.34. CertificateHolderAuthorisation

Pažymėjimo turėtojo teisių identifikacija.

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

tachographApplicationID – yra tachografo taikomosios programos vardas.

Priskiriamos vertės: 'FFh', '54h', '41h', '43h', '48h', '4Fh'. Šis AID yra patentuotas neregistruotos taikomosios programos vardas pagal ISO/IEC 7816-5.

equipmentType – yra įrangos, kuriai skirtas pažymėjimas, rūšies identifikacija.

Priskiriamos vertės: pagal duomenų tipą **EquipmentType**. Jei pažymėjimas yra valstybės narės, priskiriama vertė yra 0.

2.35. CertificateRequestID

Pažymėjimo prašymo unikali identifikacija. Jei generuojant pažymėjimą nežinomas transporto priemonės bloko, kuriam raktas skirtas, serijos numeris, galima naudoti ir kaip transporto priemonės bloko atvirąjį raktą.

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

requestSerialNumber – pažymėjimo prašymo serijos numeris, skirtingas kiekvienam gamintojui ir kiekvienam mėnesiui.

requestMonthYear – pažymėjimo prašymo metų ir mėnesio identifikacija.

Priskiriamos vertės: mėnuo (du skaitmenys) ir metai (du paskutiniai skaitmenys) BCD kodu.

crIdentifier: – vardas, skirtas atskirti pažymėjimo prašymui nuo pailginto serijos numerio.

Priskiriamos vertės: 'FFh'.

manufacturerCode: – pažymėjimo prašančio gamintojo skaitmeninis kodas.

2.36. CertificationAuthorityKID

Sertifikavimo institucijos (valstybės narės arba Europos sertifikavimo institucija) atvirasis raktas.

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

nationNumeric – sertifikavimo institucijos šalies skaitmeninis kodas.

nationAlpha – sertifikavimo institucijos šalies raidinis skaitmeninis kodas.

keySerialNumber – serijos numeris skirtingiems sertifikavimo institucijos raktams atskirti, jei jie būtų keičiami.

additionalInfo – dviejų baitų ilgio sritis papildomam kodui (skirta sertifikavimo institucijai).

caIdentifier – vardas, skirtas sertifikavimo institucijos rakto vardui atskirti nuo kitų raktų vardų.

Priskiriamos vertės: '01h'.

2.37. CompanyActivityData

Įmonės kortelės atmintyje laikoma informacija apie naudojant kortelę vykdytą veiklą (237 reikalavimas).

```
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 – paskutinio atnaujinto įrašo **companyActivityRecord** indeksas.

Priskiriamos vertės: skaičius, atitinkantis įrašų apie įmonės veiklą skaitiklio vertę; pirmojo struktūros įrašo apie įmonės veiklą vertė yra 0.

companyActivityRecords – visų įrašų apie įmonės veiklą rinkinys.

companyActivityRecord – informacijos apie vieną įmonės veiklą seka.

companyActivityType – įmonės veiklos rūšis.

companyActivityTime – įmonės veiklos data ir laikas.

cardNumberInformation – kortelės, iš kurios buvo perkelti duomenys, numeris ir išduodančioji valstybė narė (jei duomenys buvo perkelti iš kortelės).

vehicleRegistrationInformation – transporto priemonės, iš kurios buvo perkelti, užrakinti arba atrakinti duomenys, TPRN ir registruojančioji valstybė narė.

downloadPeriodBegin ir **downloadPeriodEnd** – apibrėžia laikotarpio, kurio duomenis buvo perkelti iš TPB, pradžią ir pabaigą (jei duomenys buvo perkelti).

2.38. CompanyActivityType

Kodas, žymintis įmonės veiklą, vykdytą naudojantis įmonės kortele.

```

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

```

2.39. CompanyCardApplicationIdentification

Įmonės kortelės atmintyje laikomi kortelės paskirties identifikacijos duomenys (190 reikalavimas).

```

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

```

typeOfTachographCardId – nurodo naudojamos kortelės rūšį.

cardStructureVersion – nurodo kortelės struktūros versiją.

noOfCompanyActivityRecords – nurodo, kiek įrašų apie įmonės veiklą gali tilpti kortelės atmintyje.

2.40. CompanyCardHolderIdentification

Įmonės kortelės atmintyje laikomi kortelės turėtojo identifikacijos duomenys (236 reikalavimas).

```

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

```

companyName – įmonės turėtojos pavadinimas.

companyAddress – įmonės turėtojos adresas.

cardHolderPreferredLanguage – įmonės turėtojos pageidaujama kalba.

2.41. ControlCardApplicationIdentification

Kontrolės kortelės atmintyje laikomi kortelės paskirties identifikacijos duomenys (190 reikalavimas).

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

typeOfTachographCardId – nurodo naudojamos kortelės rūšį.

cardStructureVersion – nurodo kortelės struktūros versiją.

noOfControlActivityRecords – nurodo, kiek įrašų apie kontrolės veiklą gali tilpti kortelės atmintyje.

2.42. ControlCardControlActivityData

Kontrolės kortelės atmintyje laikoma informacija apie naudojant kortelę vykdytą kontrolės veiklą (233 reikalavimas).

```
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 – paskutinio atnaujinto įrašo apie kontrolės veiklą indeksas.

Priskiriamos vertės: skaičius, atitinkantis įrašų apie kontrolės veiklą skaitiklio vertę; pirmojo struktūros įrašo apie kontrolės veiklą vertė yra 0.

controlActivityRecords – visų įrašų apie kontrolės veiklą rinkinys.

controlActivityRecord – informacijos apie vieną kontrolės veiklą seka.

controlType – kontrolės rūšis.

controlTime – kontrolės veiklos data ir laikas.

controlledCardNumber – kontroliuojamos kortelės numeris ir išduodančioji valstybė narė.

controlledVehicleRegistration – transporto priemonės, kurioje atlikta kontrolė, TPRN ir registruojančioji valstybė narė.

controlDownloadPeriodBegin ir **controlDownloadPeriodEnd** – apibrėžia laikotarpio, kurio duomenis buvo perkelti, pradžią ir pabaigą (jei duomenys buvo perkelti).

2.43. ControlCardHolderIdentification

Kontrolės kortelės atmintyje laikomi kortelės turėtojo identifikacijos duomenys (232 reikalavimas).

```

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

```

controlBodyName – kortelės turėtojo kontrolės institucija.

controlBodyAddress – kortelės turėtojo kontrolės institucijos adresas.

cardHolderName – kontrolės kortelės turėtojo pavardė ir vardas (-ai).

cardHolderPreferredLanguage – kortelės turėtojo pageidaujama kalba.

2.44. ControlType

Kodas, žymintis kontroliuojant vykdytą veiklą. Šis duomenų tipas susijęs su 102, 210 ir 225 reikalavimais.

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

Priskiriamos vertės – Sinchronizavimas pagal okteta: 'cvpdxxxx'B (8 bitai) (8 bitai)

```

'c'B      duomenų perkėlimas iš kortelės:
           '0'B: šios kontrolės metu duomenys iš kortelės nebuvo perkelti;
           '1'B: šios kontrolės metu duomenys iš kortelės buvo perkelti;
'v'B      duomenų perkėlimas iš TPB:
           '0'B: šios kontrolės metu duomenys iš TPB nebuvo perkelti;
           '1'B: šios kontrolės metu duomenys iš TPB buvo perkelti;
'p'B      spausdinimas:
           '0'B: šios kontrolės metu nebuvo spausdinama;
           '1'B: šios kontrolės metu buvo spausdinama;
'd'B      rodymas ekrane:
           '0'B: šios kontrolės metu ekranu nebuvo naudojama;
           '1'B: šios kontrolės metu ekranu buvo naudojama;
'xxxx'B   Nenaudojama.

```

2.45. CurrentDateTime

Esami data ir laikas, rodomi tachografe.

```
CurrentDateTime ::= TimeReal
```

Priskiriamos vertės: tiksliau nenustatyta.

2.46. DailyPresenceCounter

Vairuotojo arba dirbtuvių kortelės atmintyje laikomas skaitiklis, kurio vertė didinama kiekvieną kalendorinę dieną, kurią kortelė buvo įkišta į TPB. Šis duomenų tipas susijęs su 199 ir 219 reikalavimais.

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

Priskiriamos vertės: eilės tvarka didėjantis skaičius, kurio didžiausia vertė = 9 999; pasiekus didžiausią vertę vėl pradedama skaičiuoti nuo 0. Pirmą kartą išduodant kortelę skaičius nustatytas į 0.

2.47. Datef

Data, išreikšta greitai išspausdintinu skaitmeniniu formatu.

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

Priskiriamos vertės:

YYYY metai;
 mm mėnuo;
 dd diena;
 '00000000'H žymi, kad data nenustatyta.

2.48. Distance

Nuvažiuotas atstumas (skirtumo tarp dviejų transporto priemonės hodometro rodmens verčių rezultatas kilometrais).

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

Priskiriamos vertės: Dvinariai be ženklo. Vertė kilometrais nuo 0 iki 9 999 km.

2.49. DriverCardApplicationIdentification

Vairuotojo kortelės atmintyje laikomi kortelės paskirties identifikacijos duomenys (190 reikalavimas).

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

typeOfTachographCardId – nurodo naudojamos kortelės rūšį.

cardStructureVersion – nurodo kortelės struktūros versiją.

noOfEventsPerType – nurodo, kiek vienos rūšies įvykių gali būti užregistruota kortelės atmintyje.

noOfFaultsPerType – nurodo, kiek vienos rūšies gedimų gali būti užregistruota kortelės atmintyje.

activityStructureLength – nurodo laisvų baitų skaičių įrašams apie veiklą.

noOfCardVehicleRecords – nurodo, kiek įrašų apie transporto priemonę gali tilpti kortelės atmintyje.

noOfCardPlaceRecords – nurodo, kiek įrašų apie vietas gali tilpti kortelės atmintyje.

2.50. DriverCardHolderIdentification

Vairuotojo kortelės atmintyje laikomi kortelės turėtojo identifikacijos duomenys (195 reikalavimas).

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

cardHolderName – vairuotojo kortelės turėtojo pavardė ir vardas (-ai).

cardHolderBirthDate – vairuotojo kortelės turėtojo gimimo data.

cardHolderPreferredLanguage – vairuotojo kortelės turėtojo pageidaujama kalba.

2.51. EntryTypeDailyWorkPeriod

Kodas įrašo apie dienos darbo laikotarpio vietą pradžiai bei pabaigai ir būsenai atskirti.

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)

}

Priskiriamos vertės: pagal ISO/IEC 8824-1.

2.52. EquipmentType

Kodas įvairioms tachografo įrangos rūšims atskirti.

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)

Priskiriamos vertės: pagal ISO/IEC 8824-1.

Vertė 0 rezervuota pažymėjimo laukelyje „CHA“ valstybei narei arba Europai pažymėti.

2.53. EuropeanPublicKey

Europinis atvirasis raktas.

EuropeanPublicKey ::= PublicKey.

2.54. EventFaultType

Įvykį arba gedimą nusakantis kodas.

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

Priskiriamos vertės:

'0x'H	bendrieji įvykiai;
'00'H	jokios papildomos informacijos;
'01'H	įkišta negaliojanti kortelė;
'02'H	kortelių nesuderinamumas;
'03'H	dalinis laiko sutapimas;
'04'H	važiavimas be reikiamos kortelės;
'05'H	kortelė įkišta važiuojant;
'06'H	netinkamai užbaigta paskutinė kortelės panauda;
'07'H	viršytas greitis;

'08'H	pertrauktas maitinimas;
'09'H	duomenų apie judėjimą klaida;
nuo '0A'H iki '0F'H	RFU;
'1x'H	su transporto priemonės bloku susiję bandymų pažeisti apsaugą įvykiai;
'10'H	jokios papildomos informacijos;
'11'H	judesio jutiklio autentiškumo tikrinimo nepavykimas;
'12'H	tachografo kortelės autentiškumo tikrinimo nepavykimas;
'13'H	neleistinas judesio jutiklio pakeitimas;
'14'H	duomenų įvedimo į kortelę nepažeistumo klaida;
'15'H	laikomų duomenų apie naudotoją nepažeistumo klaida;
'16'H	vidinio duomenų perdavimo klaida;
'17'H	neleistinas korpuso atidarymas;
'18'H	kenkimas techninei įrangai;
nuo '19'H iki '1F'H	RFU;
'2x'H	su jutikliu susiję bandymų pažeisti apsaugą įvykiai;
'20'H	jokios papildomos informacijos;
'21'H	autentiškumo tikrinimo nepavykimas;
'22'H	laikomų duomenų nepažeistumo klaida;
'23'H	vidinio duomenų perdavimo klaida;
'24'H	neleistinas korpuso atidarymas;
'25'H	kenkimas techninei įrangai;
nuo '26'H iki '2F'H	RFU;
'3x'H	tachografo gedimai;
'30'H	jokios papildomos informacijos;
'31'H	TPB vidinis gedimas;
'32'H	spausdintuvo gedimas;
'33'H	ekrano gedimas;
'34'H	duomenų perkėlimo gedimas;
'35'H	jutiklio gedimas;
nuo '36'H iki '3F'H	RFU;
'4x'H	kortelės gedimai;
'40'H	jokios papildomos informacijos;
nuo '41'H iki '4F'H	RFU;
nuo '50'H iki '7F'H	RFU;
nuo '80'H iki 'FF'H	nustato gamintojas.

2.55. EventFaultRecordPurpose

Kodas, paaiškinantis, kodėl įvykis arba gedimas buvo užregistruotas.

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

Priskiriamos vertės:

'00'H	vienas iš 10 pastarųjų (arba paskutiniai) įvykiai arba gedimai;
'01'H	ilgiausias įvykis per pastarąsias 10 dienų;
'02'H	vienas iš 5 ilgiausių įvykių per pastarąsias 365 dienas;
'03'H	paskutinis įvykis per pastarąsias 10 dienų;
'04'H	rimčiausias įvykis per pastarąsias 10 dienų;
'05'H	vienas iš 5 rimčiausių įvykių per pastarąsias 365 dienas;
'06'H	pirmasis įvykis arba gedimas, įvykęs po paskutinio kalibravimo;
'07'H	vykstantis (esamas) įvykis arba gedimas;
nuo '08'H iki '7F'H	RFU;
nuo '80'H iki 'FF'H	nustato gamintojas.

2.56. ExtendedSerialNumber

Unikali įrangos identifikacija. Galima naudoti ir kaip įrangos atvirojo rakto vardą.

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

serialNumber – pažymėjimo prašymo serijos numeris, skirtingas kiekvienam gamintojui, įrangos tipui ir kiekvienam mėnesiui.

monthYear – pagaminimo metų (arba serijos numerio priskyrimo) ir mėnesio identifikacija.

Priskiriamos vertės: mėnuo (du skaitmenys) ir metai (du paskutiniai skaitmenys) BCD kodu.

type – įrangos rūšies vardas.

Priskiriamos vertės: nustato gamintojas, rezervuota vertė 'FFh'.

manufacturerCode: – pažymėjimo prašančio gamintojo skaitmeninis kodas.

2.57. FullCardNumber

Tachografo kortelę visiškai identifikuojantis kodas.

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

cardType – tachografo kortelės rūšis.

cardIssuingMemberState – kortelę išdavusios valstybės narės kodas.

cardNumber – kortelės numeris.

2.58. HighResOdometer

Transporto priemonės hodometro rodmens vertė: bendras transporto priemonės naudojimo metu nuvažiuotas atstumas.

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

Priskiriamos vertės: Dvinariai be ženklo. Vertė 1/200 km padalomis nuo 0 iki 21 055 406 km.

2.59. HighResTripDistance

Per visą arba dalį kelionės nuvažiuotas atstumas.

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

Priskiriamos vertės: Dvinariai be ženklo. Vertė 1/200 km padalomis nuo 0 iki 21 055 406 km.

2.60. HolderName

Kortelės turėtojo pavardė ir vardas (-ai).

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

holderSurname – turėtojo pavardė. Pavardė yra be titulų.

Priskiriamos vertės: kai kortelė yra neasmeninė, holderSurname yra ta pati informacija kaip companyName, workshopName arba controlBodyName.

holderFirstNames – turėtojo vardas (-ai) ir inicialai.

2.61. K-ConstantOfRecordingEquipment

Tachografo konstanta (m apibrėžimas).

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

Priskiriamos vertės: impulsai per kilometrą nuo 0 iki 64 255 imp./km.

2.62. KeyIdentifier

Atvirojo rakto unikalus vardas, naudojamas raktui nurodyti ir pasirinkti. Jis taip pat identifikuoja rakto turėtoją.

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

Pirmasis pasirinkimas tinka transporto priemonės bloko arba tachografo kortelės atvirajam raktui nurodyti.

Antrasis pasirinkimas tinka transporto priemonės bloko atvirajam raktui nurodyti (jei transporto priemonės bloko serijos numeris generuojant pažymėjimą nežinomas).

Trečiasis pasirinkimas tinka valstybės narės atvirajam raktui nurodyti.

2.63. L-TyreCircumference

Ratų padangų efektyvusis apskritimo ilgis (u apibrėžimas).

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

Priskiriamos vertės: Dvinariai be ženklų. Vertė 1/8 mm padalomis nuo 0 iki 8 031 mm.

2.64. Language

Kalbą identifikuojantis kodas.

Language ::= IA5String(SIZE(2))

Priskiriamos vertės: dviejų mažųjų raidžių kodas pagal ISO 639.

2.65. LastCardDownload

Paskutinio duomenų perkėlimo iš kortelės data ir laikas, laikomi vairuotojo kortelės atmintyje (skirti ne kontrolei). Datą gali keisti TPB arba bet koks kortelės nuskaitymo įrenginys.

LastCardDownload ::= TimeReal

Priskiriamos vertės: tiksliau nenustatyta.

2.66. ManualInputFlag

Kodas, žymintis, ar tuo metu, kai kortelė buvo įkišta, kortelės turėtojas rankomis įvedė informaciją apie vairuotojo veiklą ar ne (081 reikalavimas).

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

Priskiriamos vertės: tiksliau nenustatyta.

2.67. ManufacturerCode

Gamintoją identifikuojantis kodas.

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

Priskiriamos vertės:

'00'H	neturima informacijos;
'01'H	rezervuota vertė;
'02'H .. '0F'H	rezervuota panaudoti vėliau;
'10'H	ACTIA;
'11'H .. '17'H	rezervuota gamintojams, kurių pavadinimai prasideda raide A;
'18'H .. '1F'H	rezervuota gamintojams, kurių pavadinimai prasideda raide B;
'20'H .. '27'H	rezervuota gamintojams, kurių pavadinimai prasideda raide C;
'28'H .. '2F'H	rezervuota gamintojams, kurių pavadinimai prasideda raide D;
'30'H .. '37'H	rezervuota gamintojams, kurių pavadinimai prasideda raide E;
'38'H .. '3F'H	rezervuota gamintojams, kurių pavadinimai prasideda raide F;
'40'H	„Giesecke & Devrient GmbH“;
'41'H	GEM plus;
'42'H .. '47'H	rezervuota gamintojams, kurių pavadinimai prasideda raide G;
'48'H .. '4F'H	rezervuota gamintojams, kurių pavadinimai prasideda raide H;
'50'H .. '57'H	rezervuota gamintojams, kurių pavadinimai prasideda raide I;
'58'H .. '5F'H	rezervuota gamintojams, kurių pavadinimai prasideda raide J;
'60'H .. '67'H	rezervuota gamintojams, kurių pavadinimai prasideda raide K;
'68'H .. '6F'H	rezervuota gamintojams, kurių pavadinimai prasideda raide L;
'70'H .. '77'H	rezervuota gamintojams, kurių pavadinimai prasideda raide M;
'78'H .. '7F'H	rezervuota gamintojams, kurių pavadinimai prasideda raide N;
'80'H	OSCARD;
'81'H .. '87'H	rezervuota gamintojams, kurių pavadinimai prasideda raide O;
'88'H .. '8F'H	rezervuota gamintojams, kurių pavadinimai prasideda raide P;
'90'H .. '97'H	rezervuota gamintojams, kurių pavadinimai prasideda raide Q;
'98'H .. '9F'H	rezervuota gamintojams, kurių pavadinimai prasideda raide R;
'A0'H	SETEC;
'A1'H	SIEMENS VDO;
'A2'H	STONERIDGE;
'A3'H .. 'A7'H	rezervuota gamintojams, kurių pavadinimai prasideda raide S;
'AA'H	TACHOCONTROL;
'AB'H .. 'AF'H	rezervuota gamintojams, kurių pavadinimai prasideda raide T;
'B0'H .. 'B7'H	rezervuota gamintojams, kurių pavadinimai prasideda raide U;
'B8'H .. 'BF'H	rezervuota gamintojams, kurių pavadinimai prasideda raide V;
'C0'H .. 'C7'H	rezervuota gamintojams, kurių pavadinimai prasideda raide W;
'C8'H .. 'CF'H	rezervuota gamintojams, kurių pavadinimai prasideda raide X;
'D0'H .. 'D7'H	rezervuota gamintojams, kurių pavadinimai prasideda raide Y;
'D8'H .. 'DF'H	rezervuota gamintojams, kurių pavadinimai prasideda raide Z.

2.68. MemberStateCertificate

Europos sertifikavimo institucijos išduotas valstybės narės atvirojo rakto pažymėjimas.

```
MemberStateCertificate ::= Certificate
```

2.69. MemberStatePublicKey

Valstybės narės atvirasis raktas.

`MemberStatePublicKey ::= PublicKey.`

2.70. Name

Pavadinimas (pavardė).

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

codePage – žymi ISO/IEC 8859 dalį, naudotą pavadinimui (pavardei) užkoduoti,

name – pagal ISO/IEC 8859-codePage užkoduotas pavadinimas (pavardė).

2.71. NationAlpha

Raidinis šalies žymuo pagal sąlyginę šalių pavadinimų kodavimo sistemą, naudojamą šalims nurodyti ant bamperių klijuojamuose lipdukuose ir (arba) tarp tarptautiniu mastu suderintuose transporto priemonių draudimo dokumentuose (žaliojoje kortelėje).

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

Priskiriamos vertės:

' '	neturima informacijos;
'A'	Austrija;
'AL'	Albanija;
'AND'	Andora;
'ARM'	Armėnija;
'AZ'	Azerbaidžanas;
'B'	Belgija;
'BG'	Bulgarija;
'BIH'	Bosnija ir Hercegovina;
'Bĭ'	Baltarusija;
'CH'	Šveicarija;
'CY'	Kipras;
'C2'	Čekija;
'D'	Vokietija;
'DK'	Danija;
'E'	Ispanija;
'EST'	Estija;
'F'	Prancūzija;
'FIN'	Suomija;
'FL'	Lichtenšteinas;
'FR'	Farerų salos;
'UK'	Jungtinė Karalystė, Aldernis, Gernsis, Džersis, Meno sala, Gibraltaras;
'GE'	Gruzija;
'GR'	Graikija;
'H'	Vengrija;
'HR'	Kroatija;
'I'	Italija;
'IRL'	Airija;
'IS'	Islandija;
'KZ'	Kazachstanas;
'L'	Liuksemburgas;
'LT'	Lietuva;
'LV'	Latvija;
'M'	Malta;
'MĆ'	Monakas;

'MD'	Moldovos Respublika;
'MK'	Makedonija;
'N'	Norvegija;
'NL'	Nyderlandai;
'P'	Portugalija;
'PL'	Lenkija;
'RĖ'	Rumunija;
'RSM'	San Marinas;
'RUS'	Rusijos Federacija;
'S'	Švedija;
'SK'	Slovakija;
'SLO'	Slovėnija;
'TM'	Turkmėnistanas;
'TR'	Turkija;
'UA'	Ukraina;
'V'	Vatikanas;
'YU'	Jugoslavija;
'UNK'	nežinoma;
'EĆ'	Europos Bendrija;
'EUR'	likusios Europos šalys;
'WLD'	likusios pasaulio šalys.

2.7.2. NationNumeric

Skaitmeninis šalies žymuo.

NationNumeric ::= INTEGER(0..255)

Priskiriamos vertės:

-- neturima informacijos	(00)H,
-- Austrija	(01)H,
-- Albanija	(02)H,
-- Andora	(03)H,
-- Armėnija	(04)H,
-- Azerbaidžanas	(05)H,
-- Belgija	(06)H,
-- Bulgarija	(07)H,
-- Bosnija ir Hercegovina	(08)H,
-- Baltarusija	(09)H,
-- Šveicarija	(0A)H,
-- Kipras	(0B)H,
-- Čekija	(0C)H,
-- Vokietija	(0D)H,
-- Danija	(0E)H,
-- Ispanija	(0F)H,
-- Estija	(10)H,
-- Prancūzija	(11)H,
-- Suomija	(12)H,
-- Lichtenšteinas	(13)H,
-- Farerų salos	(14)H,
-- Jungtinė Karalystė	(15)H,
-- Gruzija	(16)H,
-- Graikija	(17)H,
-- Vengrija	(18)H,
-- Kroatija	(19)H,
-- Italija	(1A)H,
-- Airija	(1B)H,
-- Islandija	(1C)H,

- - Kazachstanas	(1D) H,
- - Liuksemburgas	(1E) H,
- - Lietuva	(1F) H,
- - Latvija	(20) H,
- - Malta	(21) H,
- - Monakas	(22) H,
- - Moldovos Respublika	(23) H,
- - Makedonija	(24) H,
- - Norvegija	(25) H,
- - Nyderlandai	(26) H,
- - Portugalija	(27) H,
- - Lenkija	(28) H,
- - Rumunija	(29) H,
- - San Marinas	(2A) H,
- - Rusijos Federacija	(2B) H,
- - Švedija	(2C) H,
- - Slovakija	(2D) H,
- - Szlovénia	(2E) H,
- - Turkmėnistanas	(2F) H,
- - Turkija	(30) H,
- - Ukraina	(31) H,
- - Vatikanas	(32) H,
- - Jugoslavija	(33) H,
- - RFU	(34 . . FC) H,
- - Europos bendrija	(FD) H,
- - likusios Europos šalys	(FE) H,
- - likusios pasaulio šalys	(FF) H.

2.73. NoOfCalibrationRecords

Dirbtuvių kortelės atmintyje galinčių tilpti įrašų apie kalibravimą skaičius.

NoOfCalibrationRecords ::= INTEGER(0..255)

Priskiriamos vertės: žr. 3 skyrių.

2.74. NoOfCalibrationsSinceDownload

Skaitiklis, rodantis, kiek kalibravimų atlikta su dirbtuvių kortele nuo paskutinio duomenų perkėlimo iš jos (230 reikavimas).

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

Priskiriamos vertės: tiksliau nenustatyta.

2.75. NoOfCardPlaceRecords

Vairuotojo arba dirbtuvių kortelės atmintyje galinčių tilpti įrašų apie vietas skaičius.

NoOfCardPlaceRecords ::= INTEGER(0..255)

Priskiriamos vertės: žr. 3 skyrių.

2.76. NoOfCardVehicleRecords

Vairuotojo arba dirbtuvių kortelės atmintyje galinčių tilpti įrašų apie naudotas transporto priemones skaičius.

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

Priskiriamos vertės: žr. 3 skyrių.

2.77. NoOfCompanyActivityRecords

Įmonės kortelės atmintyje galinčių tilpti įrašų apie įmonės veiklą skaičius.

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

Priskiriamos vertės: žr. 3 skyrių.

2.78. NoOfControlActivityRecords

Kontrolės kortelės atmintyje galinčių tilpti įrašų apie kontrolės veiklą skaičius.

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

Priskiriamos vertės: žr. 3 skyrių.

2.79. NoOfEventsPerType

Kortelės atmintyje galinčių tilpti įrašų apie tam tikros rūšies įvykius skaičius.

NoOfEventsPerType ::= INTEGER(0..255)

Priskiriamos vertės: žr. 3 skyrių.

2.80. NoOfFaultsPerType

Kortelės atmintyje galinčių tilpti įrašų apie tam tikros rūšies gedimus skaičius.

NoOfFaultsPerType ::= INTEGER(0..255)

Priskiriamos vertės: žr. 3 skyrių.

2.81. OdometerValueMidnight

Transporto priemonės hodometro rodmens vertė tam tikros dienos vidurnaktį (090 reikalavimas).

OdometerValueMidnight ::= OdometerShort

Priskiriamos vertės: tiksliau nenustatyta.

2.82. OdometerShort

Transporto priemonės hodometro rodmens vertė trumpąja forma.

OdometerShort ::= INTEGER(0..2²⁴-1)

Priskiriamos vertės: Priskiriamos vertės: Dvinariai be ženklų. Vertė kilometrais nuo 0 iki 9 999 999 km.

2.83. OverspeedNumber

Greičio viršijimo įvykių skaičius nuo paskutinės greičio viršijimo kontrolės.

OverspeedNumber ::= INTEGER(0..255)

Priskiriamos vertės: 0 reiškia, kad nuo paskutinės greičio viršijimo kontrolės daugiau greičio viršijimo įvykių nebuvo, 1 reiškia, kad nuo paskutinės greičio viršijimo kontrolės buvo vienas greičio viršijimo įvykis, 255 – kad nuo paskutinės greičio viršijimo kontrolės buvo 255 ar daugiau greičio viršijimo įvykių.

2.84. PlaceRecord

Informacija apie vietą, kurioje prasideda arba baigiasi dienos darbo laikotarpis (087, 202, 221 reikalavimai).

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

entryTime – įrašo data ir laikas.

entryTypeDailyWorkPeriod – įrašo rūšis.

dailyWorkPeriodCountry – nurodyta šalis.

dailyWorkPeriodRegion – nurodytas regionas.

vehicleOdometerValue – hodometro rodmens vertė įrašo apie vietą momentu.

2.85. PreviousVehicleInfo

Informacija apie vairuotojo, įkišančio savo kortelę į transporto priemonės bloką, pirmiau naudotas transporto priemonės (081 reikalavimas).

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

vehicleRegistrationIdentification – TPRN ir registruojančioji valstybė narė.

cardWithdrawalTime – kortelės ištraukimo data ir laikas.

2.86. PublicKey

Atvirasis RSA raktas.

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

rsaKeyModulus – rakto poros modulis.

rsaKeyPublicExponent – rakto poros atvirasis laipsnio rodiklis.

2.87. RegionAlpha

Tam tikros šalies regiono raidinis žymuo.

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

Priskiriamos vertės:

' ' neturima informacijos;

Ispanija:

'AN'	Andalucía;
'AR'	Aragón;
'AST'	Asturias;
'C'	Cantabria;
'CAT'	Cataluña;
'CL'	Castilla-León;
'CM'	Castilla-La-Mancha;
'CV'	Valencia;
'EXT'	Extremadura;
'G'	Galicia;
'IB'	Baleares;
'IC'	Canarias;
'LR'	La Rioja;
'M'	Madrid;
'MU'	Murcia;
'NA'	Navarra;
'PV'	País Vasco.

2.88. RegionNumeric

Tam tikros šalies regiono skaitmeninis žymuo.

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

Priskiriamos vertės:

'00'H neturima informacijos;

Ispanija:

'01'H Andalucía;
 '02'H Aragón;
 '03'H Asturias;
 '04'H Cantabria;
 '05'H Cataluña;
 '06'H Castilla-León;
 '07'H Castilla-La-Mancha;
 '08'H Valencia;
 '09'H Extremadura;
 '0A'H Galicia;
 '0B'H Baleares;
 '0C'H Canarias;
 '0D'H La Rioja;
 '0èH Madrid;
 '0F'H Murcia;
 '10'H Navarra;
 '11'H País Vasco.

2.89. RSAKeyModulus

RSA rakto poros modulis.

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

Priskiriamos vertės: nenustatyta.

2.90. RSAKeyPrivateExponent

RSA rakto poros slaptasis laipsnio rodiklis.

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

Priskiriamos vertės: nenustatyta.

2.91. RSAKeyPublicExponent

RSA rakto poros atvirasis laipsnio rodiklis.

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

Priskiriamos vertės: nenustatyta.

2.92. SensorApprovalNumber

Jutiklio tipo patvirtinimo numerius.

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

Priskiriamos vertės: nenustatyta.

2.93. SensorIdentification

Judesio jutiklio atmintyje laikomi jo identifikacijos duomenys (077 reikalavimas).

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

sensorSerialNumber – judesio jutiklio pailgintas serijos numeris (susideda iš komponento šifro ir gamintojo kodo).

sensorApprovalNumber – judesio jutiklio patvirtinimo numeris.

sensorSCIdentifier – judesio jutiklio apsaugos komponento vardas.

sensorOSIdentifier – judesio jutiklio operacinės sistemos vardas.

2.94. SensorInstallation

Judesio jutiklio atmintyje laikoma informacija apie judesio jutiklio įrengimą (099 reikalavimas).

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

sensorPairingDateFirst – judesio jutiklio pirmojo sujungimo su transporto priemonės bloku data.

firstVuApprovalNumber – su judesio jutikliu sujungto pirmojo transporto priemonės bloko patvirtinimo numeris.

firstVuSerialNumber – su judesio jutikliu sujungto pirmojo transporto priemonės bloko serijos numeris.

sensorPairingDateCurrent – judesio jutiklio esamo sujungimo su transporto priemonės bloku data.

currentVuApprovalNumber – esamu metu su judesio jutikliu sujungto transporto priemonės bloko patvirtinimo numeris.

currentVUSerialNumber – esamu metu su judesio jutikliu sujungto transporto priemonės bloko serijos numeris.

2.95. SensorInstallationSecData

Dirbtuvių kortelės atmintyje laikoma informacija apie apsaugos duomenis, reikalingus judesio jutikliams jungti su transporto priemonės blokais (214 reikalavimas).

```
SensorInstallationSecData ::= TDesSessionKey
```

Priskiriamos vertės: pagal ISO 16844-3.

2.96. SensorOSIdentifier

Judesio jutiklio operacinės sistemos vardas.

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

Priskiriamos vertės: nustato gamintojas.

2.97. SensorPaired

Transporto priemonės bloko atmintyje laikomi su juo sujungto judesio jutiklio identifikacijos duomenys (079 reikalavimas).

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

sensorSerialNumber – esamu metu su transporto priemonės bloku sujungto judesio jutiklio serijos numeris.

sensorApprovalNumber – esamu metu su transporto priemonės bloku sujungto judesio jutiklio patvirtinimo numeris.

sensorPairingDateFirst – esamu metu su transporto priemonės bloku sujungto judesio jutiklio pirmojo sujungimo su transporto priemonės bloku data.

2.98. **SensorPairingDate**

Judesio jutiklio sujungimo su transporto priemonės bloku data.

`SensorPairingDate ::= TimeReal`

Priskiriamos vertės: nenustatyta.

2.99. **SensorSerialNumber**

Judesio jutiklio serijos numeris.

`SensorSerialNumber ::= ExtendedSerialNumber:`

2.100. **SensorSCIdentifier**

Judesio jutiklio apsauginio komponento vardas.

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

Priskiriamos vertės: nustato komponento gamintojas.

2.101. **Signature**

Skaitmeninis parašas.

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

Priskiriamos vertės: pagal 11 priedėlį „Bendrieji apsaugos mechanizmai“.

2.102. **SimilarEventsNumber**

Panašių įvykių tam tikrą dieną skaičius (094 reikalavimas).

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

Priskiriamos vertės: 0 nenaudojamas, 1 reiškia, kad tą dieną įvyko ir buvo užregistruotas vienas tos rūšies įvykis, 2 reiškia, kad tą dieną įvyko du įvykiai (užregistruotas tik vienas), ... 255 reiškia, kad tą dieną įvyko 255 ar daugiau tos rūšies įvykių.

2.103. **SpecificConditionType**

Ypatingą būseną žymintis kodas (050b, 105a, 212a ir 230a reikalavimai).

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

Priskiriamos vertės:

'00'H	RFU;
'01'H	nekontroliuojama – pradžia;
'02'H	nekontroliuojama – pabaiga;
'03'H	kelto perkėla/geležinkelio pervažis;
'04'H .. 'FF'H	RFU.

2.104. **SpecificConditionRecord**

Vairuotojo, dirbtuvių kortelės arba transporto priemonės bloko atmintyje laikoma informacija apie ypatingą būseną (105a, 212a ir 230a reikalavimai).

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

entryTime – įrašo data ir laikas.

specificConditionType – ypatingą būseną identifikuojantis kodas.

2.105. **Speed**

Transporto priemonės greitis (km/h).

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

Priskiriamos vertės: kilometrais per valandą nuo 0 iki 220 km/h.

2.106. **SpeedAuthorised**

Didžiausias leistinas transporto priemonės greitis (bb apibrėžimas).

```
SpeedAuthorised ::= Speed.
```

2.107. **SpeedAverage**

Vidutinis greitis per anksčiau nustatytą laikotarpį (km/h).

```
SpeedAverage ::= Speed.
```

2.108. **SpeedMax**

Didžiausias greitis, išmatuotas per anksčiau nustatytą laikotarpį.

```
SpeedMax ::= Speed.
```

2.109. **TDesSessionKey**

Trigubo DES panaudos raktas.

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

Priskiriamos vertės: tiksliau nenustatyta.

2.110. **TimeReal**

Bendrojo datos ir laiko laukelio kodas, kuriuo data ir laikas išreiškiami sekundėmis po 1970 m. sausio 1 d. 00 val. 00 min. 00 sek. GMT laiku.

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

Priskiriamos vertės – Synchronizavimas pagal okteta: sekundžių sakičius po 1970 m. sausio 1 d. vidurnakčio GMT laiku

Vėliausia galima data/laikas yra 2106 m.

2.111. **TyreSize**

Padangų matmenų žymuo.

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

Priskiriamos vertės: Priskiriamos vertės: pagal 1992 3 31 Direktyvą 92/23 (EEB), OL L 129, p. 95.

2.112. VehicleIdentificationNumber

Visą transporto priemonę žymintis Transporto priemonės identifikacijos numeris (TPIN) – paprastai važiuoklės serijos numeris arba rėmo numeris.

VehicleIdentificationNumber ::= IA5String(SIZE(17))

Priskiriamos vertės: kaip nustatyta ISO 3779.

2.113. VehicleRegistrationIdentification

Transporto priemonės unikali europinė identifikacija (TPRN ir valstybė narė).

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

vehicleRegistrationNation – transporto priemonės registracijos šalis.

vehicleRegistrationNumber – transporto priemonės registracijos numeris (TPRN).

2.114. VehicleRegistrationNumber

Transporto priemonės registracijos numeris (TPRN). Registracijos numerį priskiria transporto priemonių licencijavimo institucija.

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

codePage – nurodo ISO/IEC 8859 dalį, kuri buvo naudota TPRN užkoduoti.

vehicleRegNumber – pagal ISO/IEC 8859-codePage užkoduotas TPRN.

Priskiriamos vertės: nustato šalis.

2.115. VuActivityDailyData

TPB laikoma informacija apie veiklos ir (arba) važiavimo būsenos ir (arba) kortelės būsenos pasikeitimus tam tiką kalendorinę dieną (084 reikalavimas) ir plyšių kortelėms būseną tos dienos 00.00 val.

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

noOfActivityChanges – ActivityChangeInfo žodžių skaičius activityChangeInfos rinkinyje.

activityChangeInfos – TPB laikomų ActivityChangeInfo žodžių apie tą dieną rinkinys. Jame visuomet yra du ActivityChangeInfo žodžiai, nusakantys dviejų plyšių būseną tos dienos 00.00 val.

2.116. VuApprovalNumber

Transporto priemonės bloko tipo patvirtinimo numeris.

VuApprovalNumber ::= IA5String(SIZE(8))

Priskiriamos vertės: nenustatyta.

2.117. VuCalibrationData

Transporto priemonės bloko atmintyje laikoma informacija apie tachografo kalibravimus (098 reikalavimas).

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

noOfVuCalibrationRecords – rinkinyje vuCalibrationRecords esančių įrašų skaičius.

vuCalibrationRecords – įrašų apie kalibravimą rinkinys.

2.118. VuCalibrationRecord

Transporto priemonės bloko atmintyje laikoma informacija apie vieną tachografo kalibravimą (098 reikalavimas).

```
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 – kalibravimo tikslas.

workshopName, **workshopAddress** – dirbtuvių pavadinimas ir adresas.

workshopCardNumber – nurodo kalibruojant naudotą dirbtuvių kortelę.

workshopCardExpiryDate – kortelės galiojimo pabaigos data.

vehicleIdentificationNumber – TPIN.

vehicleRegistrationIdentification – nurodo TPRN ir registruojančiąją valstybę narę.

wVehicleCharacteristicConstant – transporto priemonės būdingasis koeficientas.

kConstantOfRecordingEquipment – tachografo konstanta.

lTyreCircumference – ratų padangų efektyvusis apskritimo ilgis.

tyreSize – transporto priemonėje sumontuotų padangų matmens žymuo.

authorisedSpeed – leistinas transporto priemonės greitis.

oldOdometerValue, **newOdometerValue** – senoji ir naujoji hodometro rodmens vertės.

oldTimeValue, **newTimeValue** – senoji ir naujoji datos ir laiko vertės.

nextCalibrationDate – kalibravimo tikslo parametru CalibrationPurpose nurodytos rūšies kito kalibravimo, kurį turi atlikti įgaliota tikrinimo institucija, data.

2.119. VuCardIWData

Transporto priemonės bloko atmintyje laikoma informacija apie vairuotojo arba dirbtuvių kortelių įkišimo ir ištraukimo ciklus transporto priemonės bloke (081 reikalavimas).

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

noOfIWRecords – tai įrašų rinkinyje vuCardIWRecords skaičius.

vuCardIWRecords – įrašų apie kortelių įkišimo ir ištraukimo ciklus rinkinys.

2.120. VuCardIWRecord

Transporto priemonės bloko atmintyje laikoma informacija apie vieną vairuotojo arba dirbtuvių kortelių įkišimo ir ištraukimo ciklą transporto priemonės bloke (081 reikalavimas).

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

cardHolderName – kortelės atmintyje laikoma vairuotojo pavardė ir vardas (-ai) arba dirbtuvių pavadinimas.

fullCardNumber – kortelės rūšis, išduodančioji valstybė narė ir kortelės atmintyje laikomas kortelės numeris.

cardExpiryDate – kortelės atmintyje laikoma jos galiojimo pabaigos data.

cardInsertionTime – įkišimo data ir laikas.

vehicleOdometerValueAtInsertion – transporto priemonės hodometro rodmens vertė įkišant kortelę.

cardSlotNumber – plyšys, į kurį kortelės įkišta.

cardWithdrawalTime – ištraukimo data ir laikas.

vehicleOdometerValueAtWithdrawal – transporto priemonės hodometro rodmens vertė ištraukiant kortelę.

previousVehicleInfo – kortelės atmintyje laikoma informacija apie ankstesnę vairuotojo naudotą transporto priemonę.

manualInputFlag – ženklas, nurodantis, ar įkišęs kortelę jos turėtojas rankomis įvedė informaciją apie savo veiklos rūšis, ar ne.

2.121. VuCertificate

Transporto priemonės bloko atvirojo rakto pažymėjimas.

```
VuCertificate ::= Certificate
```

2.122. VuCompanyLocksData

Transporto priemonės bloko atmintyje laikoma informacija apie įmonės užraktus (104 reikalavimas).

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

noOfLocks – vuCompanyLocksRecords išvardytų užraktų skaičius.

vuCompanyLocksRecords – įrašų apie įmonės užraktus rinkinys.

2.123. VuCompanyLocksRecord

Transporto priemonės bloko atmintyje laikoma informacija apie vieną įmonės užraktą (104 reikalavimas).

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

lockInTime, lockOutTime – užrakinimo ir atrakinimo data ir laikas.

companyName, companyAddress – su užrakinimu susijusios įmonės pavadinimas ir adresas.

companyCardNumber – identifikuoja užrakinant naudotą kortelę.

2.124. VuControlActivityData

Transporto priemonės bloko atmintyje laikoma informacija apie naudojant ją atliktas kontroles (102 reikalavimas).

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

noOfControls – vuControlActivityRecords išvardytų kontrolių skaičius.

vuControlActivityRecords – įrašų apie kontrolės veiklą rinkinys.

2.125. VuControlActivityRecord

Transporto priemonės bloko atmintyje laikoma informacija apie naudojant ją atliktą vieną kontrolę (102 reikalavimas).

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

controlType – kontrolės rūšis.

controlTime – kontrolės data ir laikas.

ControlCardNumber – identifikuoja kontrolės kortelę, su kuria buvo atlikta kontrolė.

downloadPeriodBeginTime – duomenų perkėlimo pradžia (jei buvo perkeliama duomenys).

downloadPeriodEndTime – duomenų perkėlimo pradžia (jei buvo perkeliama duomenys).

2.126. VuDataBlockCounter

Kortelės atmintyje laikomas skaitiklis, identifikuojantis kortelės įkišimo ir ištraukimo ciklą transporto priemonės bloke seką.

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

Priskiriamos vertės: eilės tvarka didėjantis skaičius, kurio didžiausia vertė yra 9 999; pasiekus didžiausią vertę vėl pradedama skaičiuoti nuo 0.

2.127. VuDetailedSpeedBlock

Transporto priemonės bloko atmintyje laikoma informacija apie tikslų transporto priemonės greitį tą minutę, kai transporto priemonė važiavo (093 reikalavimas).

```

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

```

speedBlockBeginDate – pirmosios greičio vertės bloke data ir laikas.

speedsPerSecond – kiekvieną tos minutės sekundę išmatuoto greičio verčių chronologinė seka pradedant nuo momento speedBlockBeginDate (įskaitant).

2.128. VuDetailedSpeedData

Transporto priemonės bloko atmintyje laikoma išsami informacija tikslų transporto priemonės greitį.

```

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

```

noOfSpeedBlocks – blokų skaičius rinkinyje vuDetailedSpeedBlocks.

vuDetailedSpeedBlocks – išsamios informacijos apie greitį blokų rinkinys.

2.129. VuDownloadablePeriod

Seniausia ir naujausia datos, kurių duomenys apie vairuotojo veiklą laikomi transporto priemonės bloko atmintyje. (081, 084 arba 087 reikalavimai).

```

VuDownloadablePeriod ::= SEQUENCE {
    minDownloadableTime          TimeReal
    maxDownloadableTime          TimeReal
}

```

minDownloadableTime – seniausio transporto priemonės bloko atmintyje laikomo įrašo apie kortelės įkišimą, veiklos rūšies pasikeitimą arba vietą data ir laikas.

maxDownloadableTime – naujausio transporto priemonės bloko atmintyje laikomo įrašo apie kortelės įkišimą, veiklos rūšies pasikeitimą arba vietą data ir laikas.

2.130. VuDownloadActivityData

Transporto priemonės bloko atmintyje laikoma informacija apie paskutinį duomenų perkėlimą iš jo (105 reikalavimas).

```

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

```

downloadingTime – duomenų perkėlimo data ir laikas.

fullCardNumber – nurodo duomenims perkelti naudotą kortelę.

companyOrWorkshopName – įmonės arba dirbtuvių pavadinimas.

2.131. VuEventData

Transporto priemonės bloko atmintyje laikoma informacija apie įvykius (094 reikalavimas, išskyrus greičio viršijimo įvyki).

```

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

```

noOfVuEvents – rinkinyje vuEventRecords išvardytų įvykių skaičius.

vuEventRecords – įrašų apie įvykius rinkinys.

2.132. VuEventRecord

Transporto priemonės bloko atmintyje laikoma informacija apie vieną įvykį (094 reikalavimas, išskyrus greičio viršijimo įvykį).

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

eventType – įvykio rūšis.

eventRecordPurpose – įvykio užregistravimo tikslas.

eventBeginTime – įvykio pradžios data ir laikas.

eventEndTime – įvykio pabaigos data ir laikas.

cardNumberDriverSlotBegin – identifikuoja prasidedant įvykiui vairuotojo plyšyje įkištą kortelę.

cardNumberCodriverSlotBegin – identifikuoja prasidedant įvykiui vairuotojo porininko plyšyje įkištą kortelę.

cardNumberDriverSlotEnd – identifikuoja baigiantis įvykiui vairuotojo plyšyje įkištą kortelę.

cardNumberCodriverSlotEnd – identifikuoja baigiantis įvykiui vairuotojo porininko plyšyje įkištą kortelę.

similarEventsNumber – panašių įvykių skaičius tą dieną.

Ši seka gali būti naudojama visiems įvykiams, išskyrus greičio viršijimą.

2.133. VuFaultData

Transporto priemonės bloko atmintyje laikoma informacija apie gedimus (096 reikalavimas).

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

noOfVuFaults – rinkinyje vuFaultRecords išvardytų gedimų skaičius.

vuFaultRecords – įrašų apie gedimus rinkinys.

2.134. VuFaultRecord

Transporto priemonės bloko atmintyje laikoma informacija apie vieną gedimą (096 reikalavimas).

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

faultType – tachografo gedimo rūšis.

faultRecordPurpose – gedimo užregistravimo tikslas.

faultBeginTime – gedimo pradžios data ir laikas.

faultEndTime – gedimo pabaigos data ir laikas.

cardNumberDriverSlotBegin – identifikuoja prasidedant gedimui vairuotojo plyšyje įkištą kortelę.

cardNumberCofdriverSlotBegin – identifikuoja prasidedant gedimui vairuotojo porininko plyšyje įkištą kortelę.

cardNumberDriverSlotEnd – identifikuoja baigiantis gedimui vairuotojo plyšyje įkištą kortelę.

cardNumberCofdriverSlotEnd – identifikuoja baigiantis gedimui vairuotojo porininko plyšyje įkištą kortelę.

2.135. VuIdentification

Transporto priemonės bloko atmintyje laikomi jo identifikacijos duomenys (075 reikalavimas).

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

vuManufacturerName – transporto priemonės bloko gamintojo pavadinimas.

vuManufacturerAddress – transporto priemonės bloko gamintojo adresas.

vuPartNumber – transporto priemonės bloko komponento šifras.

vuSerialNumber – transporto priemonės bloko serijos numeris.

vuSoftwareIdentification – identifikuoja transporto priemonės bloke įdiegtą programinę įrangą.

vuManufacturingDate – transporto priemonės bloko pagaminimo data.

vuApprovalNumber – transporto priemonės bloko tipo patvirtinimo numeris.

2.136. VuManufacturerAddress

Transporto priemonės bloko gamintojo adresas.

```
VuManufacturerAddress ::= Address
```

Priskiriamos vertės: nenustatyta.

2.137. VuManufacturerName

Transporto priemonės bloko gamintojo pavadinimas.

```
VuManufacturerName ::= Name
```

Priskiriamos vertės: nenustatyta.

2.138. VuManufacturingDate

Transporto priemonės bloko pagaminimo data.

```
VuManufacturingDate ::= TimeReal
```

Priskiriamos vertės: nenustatyta.

2.139. VuOverSpeedingControlData

Transporto priemonės bloko atmintyje laikoma informacija apie greičio viršijimo įvykius nuo paskutinės greičio viršijimo kontrolės (095 reikalavimas).

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

lastOverspeedControlTime – paskutinės greičio viršijimo kontrolės data ir laikas.

firstOverspeedSince – pirmojo greičio viršijimo po tos kontrolės data ir laikas.

numberOfOverspeedSince – greičio viršijimo įvykių skaičius nuo paskutinės greičio viršijimo kontrolės.

2.140. VuOverSpeedingEventData

Transporto priemonės bloko atmintyje laikoma informacija apie greičio viršijimo įvykius (094 reikalavimas).

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

noOfVuOverSpeedingEvents – rinkinyje vuOverSpeedingEventRecords išvardytų įvykių skaičius.

vuOverSpeedingEventRecords – įrašų apie greičio viršijimo įvykius rinkinys.

2.141. VuOverSpeedingEventRecord

Transporto priemonės bloko atmintyje laikoma informacija apie vieną greičio viršijimo įvykį (094 reikalavimas).

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

eventType – įvykio rūšis.

eventRecordPurpose – įvykio užregistravimo tikslas.

eventBeginTime – įvykio pradžios data ir laikas.

eventEndTime – įvykio pabaigos data ir laikas.

maxSpeedValue – didžiausias įvykio metu išmatuotas greitis.

averageSpeedValue – įvykio išmatuoto greičio aritmetinis vidurkis.

cardNumberDriverSlotBegin – identifikuoja kortelę, kuri buvo vairuotojo plyšyje, kai prasidėjo įvykis.

similarEventsNumber – panašių įvykių skaičius tą dieną.

2.142. VuPartNumber

Transporto priemonės bloko komponento šifras.

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

Priskiriamos vertės: nustato TPB gamintojas.

2.143. VuPlaceDailyWorkPeriodData

Transporto priemonės bloko atmintyje laikoma informacija apie vietas, kur vairuotojai pradeda arba baigia dienos darbo laikotarpį (087 reikalavimas).

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

noOfPlaceRecords – rinkinyje vuPlaceDailyWorkPeriodRecords išvardytų įrašų skaičius.

vuPlaceDailyWorkPeriodRecords – įrašų apie vietas rinkinys.

2.144. VuPlaceDailyWorkPeriodRecord

Transporto priemonės bloko atmintyje laikoma informacija apie vietas, kur vairuotojas pradeda arba baigia dienos darbo laikotarpį (087 reikalavimas).

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

fullCardNumber – vairuotojo kortelės rūšis, išduodančioji valstybė narė ir kortelės numeris.

placeRecord – informacija apie nurodytą vietą.

2.145. VuPrivateKey

Transporto priemonės bloko slaptasis raktas.

```
VuPrivateKey ::= RSAKeyPrivateExponent
```

2.146. VuPublicKey

Transporto priemonės bloko atvirasis raktas.

```
VuPublicKey ::= PublicKey
```

2.147. VuSerialNumber

Transporto priemonės bloko serijos numeris (075 reikalavimas).

```
VuSerialNumber ::= ExtendedSerialNumber
```

2.148. VuSoftInstallationDate

Transporto priemonės bloko programinės įrangos versijos įdiegimo data.

```
VuSoftInstallationDate ::= TimeReal
```

Priskiriamos vertės: nenustatyta.

2.149. VuSoftwareIdentification

Transporto priemonės bloko atmintyje laikomi duomenys apie įdiegtą programinę įrangą.

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

vuSoftwareVersion – transporto priemonės bloko programinės įrangos versijos numeris.

vuSoftInstallationDate – programinės įrangos versijos įdiegimo data.

2.150. VuSoftwareVersion

Transporto priemonės bloko programinės įrangos versijos numeris.

VuSoftwareVersion ::= IA5String(SIZE(4))

Priskiriamos vertės: nenustatyta.

2.151. VuSpecificConditionData

Transporto priemonės bloko atmintyje laikoma informacija apie ypatingas būsenas.

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

noOfSpecificConditionRecords – rinkinyje specificConditionRecords išvardytų įrašų skaičius.

specificConditionRecords – įrašų apie ypatingas būsenas rinkinys.

2.152. VuTimeAdjustmentData

Transporto priemonės bloko atmintyje laikoma informacija apie neįprasto kalibravimo metu atliktus laiko koregavimus (101 reikalavimas).

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

noOfVuTimeAdjRecords – įrašų rinkinyje vuTimeAdjustmentRecords skaičius.

vuTimeAdjustmentRecords – įrašų apie laiko koregavimą rinkinys.

2.153. VuTimeAdjustmentRecord

Transporto priemonės bloko atmintyje laikoma informacija apie neįprasto kalibravimo metu atliktą laiko koregavimą (101 reikalavimas).

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

oldTimeValue, newTimeValue – senoji ir naujoji datos ir laiko vertės.

workshopName, workshopAddress – dirbtuvių pavadinimas ir adresas.

workshopCardNumber – identifikuoja laikui koreguoti naudotą dirbtuvių kortelę.

2.154. W-VehicleCharacteristicConstant

Transporto priemonės būdingasis koeficientas (k apibrėžimas).

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

Priskiriamos vertės: Priskiriamos vertės: impulsais per kilometrą, nuo 0 iki 64 255 imp./km.

2.155. WorkshopCardApplicationIdentification

Dirbtuvių kortelės atmintyje laikoma informacija apie kortelės naudojimą (190 reikalavimas).

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

typeOfTachographCardId – nurodo naudojamos kortelės rūšį.

cardStructureVersion – nurodo kortelės struktūros versiją.

noOfEventsPerType – nurodo, kiek vienos rūšies įvykių gali būti užregistruota kortelės atmintyje.

noOfFaultsPerType – nurodo, kiek vienos rūšies gedimų gali būti užregistruota kortelės atmintyje.

activityStructureLength – nurodo laisvų baitų skaičių įrašams apie veiklą.

noOfCardVehicleRecords – nurodo, kiek įrašų apie transporto priemonę gali tilpti kortelės atmintyje.

noOfCardPlaceRecords – nurodo, kiek įrašų apie vietas gali tilpti kortelės atmintyje.

noOfCalibrationRecords – nurodo, kiek įrašų apie kalibravimą gali tilpti kortelės atmintyje.

2.156. WorkshopCardCalibrationData

Dirbtuvių kortelėje laikoma informacija apie su kortele atliktą dirbtuvių veiklą (227 ir 229 reikalavimai).

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

calibrationTotalNumber – bendras su kortele atliktų kalibravimų skaičius.

calibrationPointerNewestRecord – paskutinio atnaujinto įrašo apie kalibravimą indeksas.

Priskiriamos vertės: numeris, atitinkantis įrašų apie kalibravimą skaitiklio vertę, pirmojo struktūros įrašo apie kalibravimą vertė yra 0.

calibrationRecords – informacijos apie kalibravimą ir (arba) laiko koregavimą įrašų rinkinys.

2.157. WorkshopCardCalibrationRecord

Dirbtuvių kortelėje laikoma informacija apie su kortele atliktą kalibravimą (227 reikalavimas).

```
WorkshopCardCalibrationRecord ::= SEQUENCE {
    calibrationPurpose               CalibrationPurpose,
    vehicleIdentificationNumber      VehicleIdentificationNumber,
    vehicleRegistration              VehicleRegistrationIdentification,
    wVehicleCharacteristicConstant   W-VehicleCharacteristicConstant,
    kConstantOfRecordingEquipment    K-ConstantOfRecordingEquipment,
    lTyreCircumference              L-TyreCircumference,
    tyreSize                        TyreSize,
```

<code>authorisedSpeed</code>	<code>SpeedAuthorised,</code>
<code>oldOdometerValue</code>	<code>OdometerShort,</code>
<code>newOdometerValue</code>	<code>OdometerShort,</code>
<code>oldTimeValue</code>	<code>TimeReal,</code>
<code>newTimeValue</code>	<code>TimeReal,</code>
<code>nextCalibrationDate</code>	<code>TimeReal,</code>
<code>vuPartNumber</code>	<code>VuPartNumber,</code>
<code>vuSerialNumber</code>	<code>VuSerialNumber,</code>
<code>sensorSerialNumber</code>	<code>SensorSerialNumber</code>

}

calibrationPurpose – kalibravimo tikslas.

vehicleIdentificationNumber – TPIN.

vehicleRegistration – TPRN ir registruojančioji valstybė narė.

wVehicleCharacteristicConstant – transporto priemonės būdingasis koeficientas.

kConstantOfRecordingEquipment – tachografo konstanta.

lTyreCircumference – ratų padangų efektyvusis apskritimo ilgis.

tyreSize – transporto priemonėje sumontuotų padangų matmens žymuo.

authorisedSpeed – didžiausias leistinas transporto priemonės greitis.

oldOdometerValue, newOdometerValue – senoji ir naujoji hodometro rodmens vertės.

oldTimeValue, newTimeValue – senoji ir naujoji datos ir laiko vertės.

nextCalibrationDate – kalibravimo tikslo parametru CalibrationPurpose nurodytos rūšies kito kalibravimo, kurį turi atlikti įgaliota tikrinimo institucija.

vuPartNumber, vuSerialNumber ir **sensorSerialNumber** – tachografo identifikacijos duomenų elementai.

2.158. WorkshopCardHolderIdentification

Dirbtuvių kortelės atmintyje laikoma informacija apie kortelės turėtoją (216 reikalavimas).

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

workshopName – kortelės turėtojo dirbtuvių pavadinimas.

workshopAddress – kortelės turėtojo dirbtuvių adresas.

cardHolderName – turėtojo pavardė ir vardas (-ai) (pvz., mechaniko pavardė).

cardHolderPreferredLanguage – kortelės turėtojo pageidaujama kalba.

2.159. WorkshopCardPIN

Dirbtuvių kortelės asmeninės identifikacijos numeris (213 reikalavimas).

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

Priskiriamos vertės: kortelės turėtoji žinomas PIN kodas, papildytas dešinėje prirašant iki 8 'FF' baitų.

3. VERČIŲ IR DYDŽIŲ RIBOS

2 dalies sąvokose naudojamų kintamųjų verčių ribos.

TimeRealRange ::= 2³²-1

3.1. Vairuotojo kortelės verčių ribos:

Kintamosios vertės	Mažiausia	Didžiausia
CardActivityLengthRange	5 544 baitai (28 dienos, 93 veiklos rūšių pasikeitimai per dieną)	13 776 baitai (28 dienos, 240 veiklos rūšių pasikeitimų per dieną)
NoOfCardPlaceRecords	84	112
NoOfCardVehicleRecords	84	200
NoOfEventsPerType	6	12
NoOfFaultsPerType	12	24

3.2. Dirbtuvių kortelės verčių ribos:

Kintamosios vertės	Mažiausia	Didžiausia
CardActivityLengthRange	198 baitai (1 diena, 93 veiklos rūšių pasikeitimai)	492 baitai (1 diena, 240 veiklos rūšių pasikeitimų)
NoOfCardPlaceRecords	6	8
NoOfCardVehicleRecords	4	8
NoOfEventsPerType	3	3
NoOfFaultsPerType	6	6
NoOfCalibrationRecords	88	255

3.3. Kontrolės kortelės verčių ribos:

Kintamosios vertės	Mažiausia	Didžiausia
NoOfControlActivityRecords	230	520

3.4. Įmonės kortelės verčių ribos:

Kintamosios vertės	Mažiausia	Didžiausia
NoOfCompanyActivityRecords	230	520

4. RAŠMENŲ RINKINIAI

Eilutėse **IA5Strings** naudojami ISO/IEC 8824-1 nustatyti ASCII rašmenys. Kad būtų aiškiau, jie pateikti toliau. Atsiradus neatitikimų viršenybė turi rašmenys pagal standartą ISO/IEC 8824-1.

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

Kitose rašmenų eilutėse (**Address**, **Name**, **VehicleRegistrationNumber**) papildomai naudojami nuo 192 iki 255 kodais koduojami rašmenys pagal ISO/IEC 8859-1 (Lotynų 1 rašmenų rinkinys) arba ISO/IEC 8859-7 (Graikų rašmenų rinkinys).

5. KODAVIMAS

Koduoiant pagal ASN.1 kodavimo taisykles, visi nustatyti duomenų tipai koduojami pagal ISO/IEC 8825-2 nurodytą sulgiuotąjį variantą.

2 priedėlis

TACHOGRAFO KORTELIŲ SPECIFIKACIJA

Turinys

1.	Įvadas	377
1.1.	Santrumpos.	377
1.2.	Nuorodos	378
2.	Elektrinės ir fizinės savybės	378
2.1.	Maitinimo įtampa ir imamos srovės stiprumas	378
2.2.	Programavimo įtampa V_{pp}	379
2.3.	Laikrodžio signalo generavimas ir dažnis	379
2.4.	Įvesties ir išvesties (I/O) kontaktas	379
2.5.	Kortelės būsenos	379
3.	Techninė įranga ir informacijos perdavimas	379
3.1.	Įvadas	379
3.2.	Siuntimo protokolas	379
3.2.1.	Protokoliai	379
3.2.2.	ATR	380
3.2.3.	PTS	381
3.3.	Prieigos sąlygos (AC)	381
3.4.	Duomenų kodavimas	382
3.5.	Komandos ir klaidų kodų apžvalga	382
3.6.	Komandų aprašymas	383
3.6.1.	SELECT_FILE [pasirinkti rinkmeną]	383
3.6.1.1.	Pasirinkimas pagal pavadinimą (AID)	383
3.6.1.2.	Elementariosios rinkmenos pasirinkimas naudojantis jos vardu	384
3.6.2.	READ_BINARY [nuskaityti dvinarį]	384
3.6.2.1.	Komanda be saugaus keitimosi duomenimis	385
3.6.2.2.	Komanda be saugaus keitimosi duomenimis	385
3.6.3.	UPDATE_BINARY [atnaujinti dvinarį]	387
3.6.3.1.	Komanda be saugaus keitimosi duomenimis	387
3.6.3.2.	Komanda su saugiu keitimusi duomenimis	388
3.6.4.	GET_CHALLENGE [reikalauti slaptažodžio]	389
3.6.5.	VERIFY [patikrinti]	389
3.6.6.	GET_RESPONSE [gauti atsakymą]	390
3.6.7.	PSO: VERIFY_CERTIFICATE [PSO: patikrinti pažymėjimą]	390
3.6.8.	INTERNAL_AUTHENTICATE [vidinis autentiškumo tikrinimas]	391

3.6.9.	EXTERNAL_AUTHENTICATE [išorinis autentiškumo tikrinimas]	392
3.6.10.	MANAGE_SECURITY_ENVIRONMENT (MSE) [valdyti apsaugos aplinką]	393
3.6.11.	PSO: HASH [PSO: maiša]	394
3.6.12.	PERFORM_HASH_OF_FILE [atlikti rinkmenos maišą]	394
3.6.13.	PSO: COMPUTE_DIGITAL_SIGNATURE [PSO: apskaičiuoti skaitmeninį parašą]	395
3.6.14.	PSO: VERIFY_DIGITAL_SIGNATURE [PSO: patikrinti skaitmeninį parašą]	396
4.	Tachografo kortelių struktūra	396
4.1.	Vairuotojo kortelės struktūra	397
4.2.	Dirbtuvių kortelės struktūra	399
4.3.	Kontrolės kortelės struktūra	401
4.4.	Įmonės kortelės struktūra	403

1. ĮVADAS

1.1. Santrumpos

Šiame priedėlyje naudojamos tokios santrumpos:

AC	prieigos sąlygos;
AID	taikomosios programos vardas;
ALW	visuomet;
APDU	taikomosios programos protokolo duomenų vienetas (komandos struktūra);
ATR	atsakymas į perkrovimą;
AUT	autentiškumas patikrintas;
C6, C7	kortelės kontaktai Nr. 6 ir 7, kaip aprašyta ISO/IEC 7816-2;
cc	laikrodžio ciklai;
CHV	kortelės turėtojo patikrinimo informacija;
CLA	APDU komandos klasės baitas;
DF	paskirtoji rinkmena. Joje negali būti kitų rinkmenų (EE arba DF);
EF	elementarioji rinkmena;
ENC	užkoduota: prieiga galima tik užkoduojant duomenis;
etu	elementarus laiko vienetas;
IC	integrinis grandynas;
ICC	kortelė su integriniu grandynu;
ID	vardas;
IFD	sąsajos įtaisas;
IFS	informacijos lauko dydis;
IFSC	informacijos lauko dydis kortelei;
IFSD	informacijos lauko dydžio įtaisas (terminalui);
INS	APDU komandos nurodymo baitas;
Lc	APDU komandos įvesties duomenų ilgis;
Le	laukiamų duomenų dydis (komandos išvesties duomenys);
MF	pagrindinė rinkmena (esminė DF);
P1-P2	parametrų rinkmenos;
NAD	protokole T=1 naudojamas mazginių taškų adresas;
NEV	niekada;
PIN	asmeninės identifikacijos numeris;
PRO SM	apsaugota saugiu keitimusi pranešimais;
PTS	protokolo siuntimo pasirinkimas;
RFU	rezervuota panaudoti vėliau;

RST	(kortelės) perkrovimas;
SM	saugusis keitimasis pranešimais;
SW1-SW2	būsenos baitai;
TS	pirmasis ATR rašmuo;
VPP	programavimo įtampa;
XXh	vertė XX šešioliktaine skaičiavimo sistema;
	sąryšio simbolis 03 04=0304.

1.2. Nuorodos

Šiame priedėlyje naudoti tokie šaltiniai:

EN 726-3	Identifikacijos kortelių sistemos. Telekomunikacijų kortelės su integriniais grandynais ir terminalai. 3 dalis. Nuo programos nepriklausomų kortelių reikalavimai. 1994 m. gruodžio mėn.
ISO/IEC 7816-2	Informacinė technologija. Identifikacijos kortelės. Kortelės su integriniais grandynais ir kontaktais. 2 dalis. Matmenys ir kontaktų vieta. Pirmasis leidimas: 1999 m.
ISO/IEC 7816-3	Informacinė technologija. Identifikacijos kortelės. Kortelės su integriniais grandynais ir kontaktais. 3 dalis. Elektroniniai signalai ir siuntimo protokolas. 2 leidimas: 1997 m.
ISO/IEC 7816-4	Informacinė technologija. Identifikacijos kortelės. Kortelės su integriniais grandynais ir kontaktais. 4 dalis. Tarpusavio keitimosi tarpšakinės komandos. Pirmasis leidimas: 1995 m. + 1 pataisa: 1997 m.
ISO/IEC 7816-6	Informacinė technologija. Identifikacijos kortelės. Kortelės su integriniais grandynais ir kontaktais. 6 dalis. Tarpšakiniai duomenų elementai. Pirmasis leidimas: 1996 m. + 1 pataisa: 1998 m.
ISO/IEC 7816-8	Informacinė technologija. Identifikacijos kortelės. Kortelės su integriniais grandynais ir kontaktais. 8 dalis. Apsauginės tarpšakinės komandos. Pirmasis leidimas: 1999 m.
ISO/IEC 9797	Informacinė technologija. Apsaugos metodika. Duomenų nepažeistumo mechanizmas naudojant kriptografinę kontrolės funkciją su blokinių šifro algoritmu. 2 leidimas: 1994 m.

2. ELEKTRINĖS IR FIZINĖS SAVYBĖS

TCS_200 Jei nenurodyta kitaip, visi elektroniniai signalai turi būti pagal ISO/IEC 7816-3.

TCS_201 Kortelės kontaktų vieta ir matmenys turi atitikti ISO/IEC 7816-2.

2.1. Maitinimo įtampa ir imamos srovės stiprumas

TCS_202 Kortelė turi veikti pagal specifikacijas neviršydamą ISO/IEC 7816-3 nurodytą sąnaudų ribų.

TCS_203 Kortelės naudojama įtampa $V_{cc} = 3 \text{ V} (\pm 0,3 \text{ V})$ arba $V_{cc} = 5 \text{ V} (\pm 0,5 \text{ V})$.

Įtampa turi būti parinkta pagal ISO/IEC 7816-3.

2.2. Programavimo įtampa V_{pp}

- TCS_204 Kortelei neturi reikėti programavimo įtamos kontakte C6. Numatyta, kad C6 nejungiamas į IFD. Kontaktas C6 gali būti prijungtas prie V_{cc} kortelėje, tačiau neturi būti įžemintas. Ši įtampa bet kuriuo atveju neturi būti ignoruojama.

2.3. Laikrodžio signalo generavimas ir dažnis

- TCS_205 Kortelė turi veikti 1–5 MHz dažnio diapazonu. Vienos kortelės panaudos metu laikrodžio dažnis negali keistis daugiau kaip $\pm 2\%$. Laikrodžio dažnį generuoja transporto priemonės blokas, o ne pati kortelė. Darbinis ciklas gali trukti nuo 40 iki 60 %.
- TCS_206 Pagal kortelės rinkmenoje EF_{ICC} esančias sąlygas išorinį laikrodį galima sustabdyti. Pirmasis rinkmenos EF_{ICC} baitas koduoja laikrodžio sustabdymo režimo sąlygas (išsamiau nurodyta EN 726-3):

Žemas	Aukštas		
3 bitas	2 bitas	1 bitas	
0	0	1	Laikrodį sustabdyti leidžiama, lygis nenustatytas
0	1	1	Laikrodį sustabdyti leidžiama, pageidaujamas aukštas lygis
1	0	1	Laikrodį sustabdyti leidžiama, pageidaujamas žemas lygis
0	0	0	Laikrodį sustabdyti draudžiama
0	1	0	Laikrodį sustabdyti leidžiama tik aukštu lygiu
1	0	0	Laikrodį sustabdyti leidžiama tik žemu lygiu

4 ir 8 bitai nenaudojami.

2.4. Įvesties ir išvesties (I/O) kontaktas

- TCS_207 Įvesties ir išvesties kontaktas C7 naudojamas duomenims priimti ir nusiųsti į IFD. Veikiant tik kortelė arba IFD turi veikti siuntimo režimu. Jei abu įtaisai veiktų siuntimo režimu, kortelė neturi būti sugadinta. Jei kortelė nesiunčia, ji turi veikti priėmimo režimu.

2.5. Kortelės būsenos

- TCS_208 Esant maitinimo įtampai kortelė veikia dviem būsenomis:

- darbine būsena, kai vykdo komandas arba sąveikauja su skaitmeniniu bloku,
- budėjimo būsena visais kitais atvejais; šiai būsenai esant kortelė turi išlaikyti visus duomenis.

3. TECHNINĖ ĮRANGA IR INFORMACIJOS PERDAVIMAS

3.1. Įvadas

Šiame poskyryje aprašytos būtinausios tachografo kortelių ir TPB funkcinės savybės, reikalingos, kad jie tinkamai veiktų ir būtų funkciškai suderinami tarpusavyje.

Tachografo kortelės turi būti kiek įmanoma sudėtingesnės pagal taikytinas ISO/IEC normas (ypač ISO/IEC 7816). Tačiau komandos ir protokolai yra išsamiai aprašyti, nurodant tam tikrus naudojimo apribojimus ar galimus skirtumus. Nurodytos komandos visiškai atitinka minėtas normas (jei nenurodyta kitaip).

3.2. Siuntimo protokolai

- TCS_300 Siuntimo protokolai turi atitikti ISO/IEC 7816-3. Pažymėtina, kad TPB turi atpažinti kortelės siunčiamus laukimo laiko plėtimus.

3.2.1. Protokoliai

- TCS_301 Kortelė turi naudoti tiek protokolą T=0, tiek protokolą T=1.

TCS_302 T=0 yra numatytasis protokolas, todėl norint jį pakeisti į protokolą T=1, reikia PTS komandos.

TCS_303 Įtaisai turi gebėti taikyti tiesioginį susitarimą abiem protokolais: taigi tiesioginio susitarimo funkcija yra privaloma kortelei.

TCS_304 Kortelės informacijos lauko dydžio baitą ATR turi žymėti simbolis TA3. Ši vertė turi būti ne mažesnė kaip F0h (= 240 baitų).

Protokolams galioja tokie apribojimai:

TCS_305 T=0

- Sąsajos įtaisas turi gebėti atsakyti į I/O po signalo kylančios kraštinės RST momentu nuo 400cc.
- Sąsajos įtaisas turi gebėti nuskaityti 12 etu atskirtus rašmenis.
- Sąsajos įtaisas turi nuskaityti klaidingą rašmenį ir jo pakartojimą, jei juos skiria 13 etu. Jei klaidingas rašmuo aptinkamas, klaidingas atsakymas I/O gali atsirasti tarp 1 etu ir 2 etu. Įtaisas turi gebėti taikyti 1 etu vėlavimą.
- Sąsajos įtaisas turi priimti 33 baitų ATR (TS+32).
- Jei ATR sudėtyje yra TC1, sąsajos įtaiso siunčiamiems rašmenims turi būti taikomas Papildomas apsauginis laikas, tačiau kortelės siunčiami rašmenys gali tebebūti atskiriami 12 etu. Tai galioja ir kortelės siunčiamam ACK rašmeniui, kai sąsajos įtaisas išsiunčia rašmenį P3.
- Sąsajos įtaisas turi atsižvelgti į kortelės siunčiamą rašmenį NUL.
- Sąsajos įtaisas turi priimti papildomą režimą, skirtą ACK.
- Grupavimo režimu ilgesniems kaip 255 baitai duomenims priimti negalima naudoti komandos GET-RESPONSE.

TCS_306 T=1

- Baitas NAD: nenaudojamas (NAD turi būti nustatytas į „00„).
- S-bloko ABORT: nenaudojama.
- S-bloko VPP būsenos klaida: nenaudojama.
- Visas duomenų laukelio grupavimo ilgis neviršija 255 baitų (turi užtikrinti IFD).
- Informacijos lauko dydžio įtaisą (IFSD) IFD turi nurodyti tuoj po ATR: po ATR, IFD turi siųsti S-bloko IFS paklausimą, o kortelė turi atsiųsti atgal S-bloko IFS. Rekomenduojama IFSD vertė – 254 baitai.
- Kortelė neprašo pakartotinio IFS patikslinimo.

3.2.2. ATR

TCS_307 Įtaisas patikrina ATR baitus pagal ISO/IEC 7816-3. ATR istoriniai rašmenys netikrinami.

Bazinio biprotokolo ATR pagal ISO/IEC 7816-3 pavyzdys

Rašmuo	Vertė	Pastabos
TS	'3Bh'	Žymi tiesioginį susitarimą
T0	'85h'	Yra TD1; yra 5 istoriniai baitai
TD1	'80h'	Yra TD2; reikia naudoti T=0
TD2	'11h'	Yra TA3; reikia naudoti T=1
TA3	'XXh' (min. 'F0h')	Informacijos lauko dydis kortelei (IFSD)
TH1 bis TH5	'XXh'	Istoriniai rašmenys
TCK	'XXh'	Kontrolinis rašmuo (išskyrus OR)

TCS_308 Po atsakymo į perkrovimą (ATR), besąlygiškai parenkama pagrindinė rinkmena (MF), kuri tampa esamučiu katalogu.

3.2.3. PTS

TCS_309 Numatytasis protokolas yra T=0. Protokolui T=1 nustatyti, įtaisas turi nusiųsti į kortelę PTS (dar žinomą PPS pavadinimu).

TCS_310 Kadangi kortelei privalomas tiek T=0, tiek T=1 protokolas, jai privalomas protokolo pakeitimo bazinis PTS.

Kaip nurodyta ISO/IEC 7816-3, šį PTS galima naudoti perdavimo greičiui didinti iki aukštesnės už numatytąją vertę, kurią siūlo kortelė galimame ATR (baitas TA(1)).

TCS_311 Jei galimas naudoti tik numatytasis perdavimo greitis (arba jei pasirinktas greitis netinkamas), kortelė turi tinkamai atsakyti į PTS pagal ISO/IEC 7816-3, praleisdama baitą PPS1.

Bazinio PTS pavyzdžiai yra tokie:

Rašmuo	Vertė	Pastabos
PPSS	'FFh'	Pirmasis rašmuo
PPS0	'00h' arba '01h'	Nuo PPS1 iki PPS3 nėra; T0 pasirinkti – '00h', T1 pasirinkti – '01h'
PK	'XXh'	Kontrolinis rašmuo: jei PPS0 = '00h', 'XXh' = 'FFh' jei PPS0 = '01h', 'XXh' = 'FEh'

3.3. Prieigos sąlygos (AC)

Kiekvienai elementariajai rinkmenai nustatomos komandų UPDATE_BINARY ir READ_BINARY komandų prieigos sąlygos (AC).

TCS_312 Norint prieiti prie esamosios rinkmenos naudojantis šiomis komandomis, reikia įvykdyti jos AC.

Galimų prieigos sąlygų apibrėžimai yra tokie:

- ALW: veiksmas visuomet galimas ir jį galima atlikti be jokių apribojimų.
- NEV: veiksmas niekada negalimas.
- AUT: turi būti suteikta teisė, atitinkanti sėkmingą išorinį autentiškumo tikrinimą (atliekama komanda EXTERNAL_AUTHENTICATE).
- PRO SM: komanda saugaus keitimosi pranešimais būdu turi būti siunčiama kartu su kriptografinė kontroline suma (žr. 11 priedėlį).
- AUT ir PRO SM (kartu).

Kortelėje galima nustatyti tokias apdorojimo komandų (UPDATE_BINARY ir READ_BINARY) prieigos sąlygas:

	UPDATE_BINARY	READ_BINARY
ALW	Taip	Taip
NEV	Taip	Taip
AUT	Taip	Taip
PRO SM	Taip	Ne
AUT ir PRO SM	Taip	Ne

Prieigos sąlyga PRO SM negalima komandai READ_BINARY. Tai reiškia, kad komandai READ kriptografinė kontrolinė suma niekuomet nėra privaloma. Tačiau šioje klasėje naudojant vertę !!!OČ įmanoma naudoti komandą READ_BINARY saugiu būdu keičiantis pranešimais, kaip aprašyta 3.6.2 punkte.

3.4. Duomenų kodavimas

Kai reikia apsaugoti iš rinkmenos nuskaitytų duomenų konfidencialumą, rinkmena pažymima kaip „užkoduota“. Koduojama taikant saugaus keitimosi pranešimais būdą (žr. 11 priedėlį).

3.5. Komandos ir klaidų kodų apžvalga

Naudojamos komandos ir rinkmenų struktūra iš ISO/IEC 7816-4.

TCS_313 Šiame poskyryje aprašytos tokios APDU komandų ir atsakymų poros:

Komanda	INS
SELECT_FILE	A4
READ_BINARY	B0
UPDATE_BINARY	D6
GET_CHALLENGE	84
VERIFY	20
GET_RESPONSE	C0
PERFORM_SECURITY_OPERATION: VERIFY_CERTIFICATE COMPUTE_DIGITAL_SIGNATURE VERIFY_DIGITAL_SIGNATURE HASH	2A
INTERNAL_AUTHENTICATE	88
EXTERNAL_AUTHENTICATE	82
MANAGE_SECURITY_ENVIRONMENT: SETTING_A_KEY	22
PERFORM_HASH_OF_FILE	2A

TCS_314 Būsenos žodžiai SW1 ir SW2 grąžinami bet kokiame atsakymo pranešime ir žymi komandos apdorojimo būseną.

SW1	SW2	Reikšmė
90	00	Įprastas apdorojimas.
61	XX	Įprastas apdorojimas. XX = galimų atsakymo baitų skaičius.
62	81	Perspėjamas apdorojimas. Dalis grąžinamų duomenų gali būti sugadinti.
63	CX	Neteisingas CHV (PIN). Likusių bandymų skaitiklio vertė pateikiama kaip 'X'.
64	00	Vykdyto klaida. Ilgalaiškės atminties būseną nepakitusi. Nepažeistumo klaida.
65	00	Vykdyto klaida. Ilgalaiškės atminties būseną pakitusi.
65	81	Vykdyto klaida. Ilgalaiškės atminties būseną pakitusi. Atminties sutrikimas.
66	88	Apsaugos klaida: neteisinga kriptografinė kontrolinė suma (vykstant saugiam keitimuisi duomenimis); neteisingas pažymėjimas (tikrinant pažymėjimą); neteisinga kriptograma (išoriškai tikrinant autentiškumą); neteisingas parašas (tikrinant parašą).
67	00	Neteisingas ilgis (neteisingas Lc arba Le).
69	00	Uždrausta komanda (kai T=0, atsakymas negalimas).
69	82	Neįvykdyti apsaugos būsenos reikalavimai.
69	83	Autentiškumo tikrinimo būdas užblokuotas.
69	85	Neįvykdyti naudojimo reikalavimai.
69	86	Komanda neleidžiama (nėra esamojo EF).
69	87	Nėra lauktų saugaus keitimosi pranešimais duomenų objektų.
69	88	Neteisingi saugaus keitimosi pranešimais duomenų objektai.
6A	82	Rinkmena nerasta.
6A	86	Neteisingi parametrai P1-P2.
6A	88	Nurodyti duomenys nerasti.
6B	00	Neteisingi parametrai (nuokrypys už EF rinkmenos ribų).

SW1	SW2	Reikšmė
6C	XX	Neteisingas ilgis; teisingą ilgį rodo SW2. Duomenų laukelis atsakyme negražinamas.
6D	00	Instrukcijos kodas netinkamas arba neteisingas.
6E	00	Klasė netinkama.
6F	00	Kitos tikrinimo klaidos.

3.6. Komandų aprašymas

Šiame poskyryje aprašytos tachografo kortelių privalomosios komandos.

Papildoma išsamesnė informacija apie naudojamas kriptografines operacijas pateikta 11 priedėlyje „Bendrieji apsaugos mechanizmai“.

Visos komandos aprašytos nepriklausomai nuo naudojamo protokolo ($T=0$ ar $T=1$). Visuomet nurodyti APDU baitai CLA, INS, P1, P2, Lc ir Le. Jei komandai apibūdinti Lc ir Le nereikalingi, atitinkamos ilgio, vertės ir aprašymo pozicijos lieka tuščios.

TCS_315 Jei reikalaujami abu ilgio baitai (Lc ir Le) ir IFD naudoja protokolą $T=0$, aprašyta komanda turi būti padalyta į dvi dalis: IFD siunčia komandą, kaip aprašyta su $P3=Lc$ + duomenys, o tuomet siunčia komandą GET_RESPONSE (žr. 3.6.6 punktą) su $P3=Le$.

TCS_316 Jei reikalaujami abu ilgio baitai ir $Le=0$ (saugus keitimasis pranešimais):

- kai naudojamas protokolas $T=1$, kortelė turi atsakyti į $Le=0$ išsiųsdama visus turimus išvesties duomenis,
- kai naudojamas protokolas $T=0$, IFD siunčia pirmąją komandą, kurioje $P3=Lc$ + duomenys, kortelė atsako (čia numanoma $Le=0$) būsenos baitais „61La“ (čia La yra galimų atsakymo baitų skaičius). Tuomet, kad galėtų nuskaityti duomenis, IFD turi sugeneruoti komandą GET_RESPONSE su $P3=La$.

3.6.1. SELECT_FILE [pasirinkti rinkmeną]

Ši komanda atitinka ISO/IEC 7816-4, tačiau jos naudojimas, palyginti su standarte nustatyta komanda, yra labiau apribotas.

Komanda SELECT_FILE naudojama:

- taikomosios programos DF pasirinkti (reikia naudoti pasirinkimą pagal pavadinimą),
- pateiktos rinkmenos ID atitinkančiai elementariajai rinkmenai pasirinkti.

3.6.1.1. Pasirinkimas pagal pavadinimą (AID)

Ši komanda leidžia pasirinkti kortelėje taikomosios programos DF.

TCS_317 Šią komandą galima atlikti iš bet kurios rinkmenos struktūros vietos (po ATR ar bet kada).

TCS_318 Pasirinkus pritaikymą, esama apsaugos aplinka perkraunama. Pasirinkus pritaikymą daugiau nebeparenkamas joks esamas atvirasis raktas, o buvusios panaudos rakto nebegalima naudoti saugiu būdu keičiantis pranešimais. Taip pat prarandama prieigos sąlyga AUT.

TCS_319 Komandos pranešimas

Baitas	Ilgis	Vertė	Aprašymas
CLA	1	'00h'	
INS	1	'A4h'	
P1	1	'04h'	Pasirinkimas pagal pavadinimą (AID).
P2	1	'0Ch'	Atsakymo nelaukiama.
Lc	1	'NNh'	Į kortelę nusiųstų baitų skaičius (AID ilgis): tachografo programa '06h'
#6-#(5+NN)	NN	'XX..XXh'	AID: tachografo programa – 'FF 54 41 43 48 4F'

Į komandą SELECT_FILE atsakyti nereikia (T=1 Le nėra, o T=0 atsakyti neprašoma).

TCS_320 Atsakymo pranešimas (atsakyti neprašoma)

Baitas	Ilgis	Vertė	Aprašymas
SW	2	'XXXXh'	Būsenos žodžiai (SW1, SW2).

- Jei komanda sėkmingai įvykdoma, kortelė atsako '9000'.
- Jei AID atitinkanti programa nerandama, atsakyme nurodoma apdorojimo būseną '6A82'.
- Jei protokole T=1 yra Le, atsakyme nurodoma būseną '6700'.
- Jei protokole T=0 po komandos SELECT_FILE prašoma atsakyti, atsakyme nurodoma būseną '6900'.
- Jei pasirinkta programa laikoma sugadinta (rinkmenos atributuose randama nepažeistumo klaida), atsakyme nurodoma apdorojimo būseną '6400' arba '6581'.

3.6.1.2. Elementariosios rinkmenos pasirinkimas naudojantis jos vardu

TCS_321 Komandos pranešimas

Baitas	Ilgis	Vertė	Aprašymas
CLA	1	'00h'	
INS	1	'A4h'	
P1	1	'04h'	EF pasirinkimas pagal esamą DF.
P2	1	'0Ch'	Atsakymo nelaukiama.
Lc	1	'02h'	Į kortelę nusiųstų baitų skaičius.
#6-#7	2	'XXXXh'	Rinkmenos vardas.

Į komandą SELECT_FILE atsakyti nereikia (T=1 Le nėra, o T=0 atsakyti neprašoma).

TCS_322 Atsakymo pranešimas (atsakyti neprašoma)

Baitas	Ilgis	Vertė	Aprašymas
SW	2	'XXXXh'	Būsenos žodžiai (SW1, SW2).

- Jei komanda sėkmingai įvykdoma, kortelė atsako '9000'.
- Jei AID atitinkanti programa nerandama, atsakyme nurodoma apdorojimo būseną '6A82'.
- Jei protokole T=1 yra Le, atsakyme nurodoma būseną '6700'.
- Jei protokole T=0 po komandos SELECT_FILE prašoma atsakyti, atsakyme nurodoma būseną '6900'.
- Jei pasirinkta programa laikoma sugadinta (rinkmenos atributuose randama nepažeistumo klaida), atsakyme nurodoma apdorojimo būseną '6400' arba '6581'.

3.6.2. READ_BINARY [nuskaityti dvinarį]

Ši komanda atitinka ISO/IEC 7816-4, tačiau jos naudojimas, palyginti su standarte nustatyta komanda, yra labiau apribotas.

Komanda READ_BINARY naudojama duomenims nuskaityti iš atvirosios rinkmenos.

Kortelės atsakymą sudaro grąžinami nuskaityti duomenys, kurie gali būti įterpti į saugaus keitimosi pranešimų struktūrą.

TCS_323 Komandą galima atlikti tik tuomet, jei apsaugos būseną atitinka nustatytus EF funkcijos READ apsaugos atributus.

3.6.2.1. Komanda be saugaus keitimosi duomenimis

Ši komanda leidžia IFD nuskaityti duomenis iš tuo metu pasirinkto EF nenaudojant saugaus keitimosi pranešimais būdo.

TCS_324 Šia komanda turi būti neįmanoma nuskaityti duomenis iš rinkmenos, pažymėtos kaip „užkoduota“.

TCS_325 Komandos pranešimas

Baitas	Ilgis	Vertė	Aprašymas
CLA	1	'00h'	Saugus keitimasis pranešimais neprašomas.
INS	1	'B0h'	
P1	1	'XXh'	Poslinkis baitais nuo rinkmenos pradžios: pats svarbiausias baitas.
P2	1	'XXh'	Poslinkis baitais nuo rinkmenos pradžios: mažiausiai svarbus baitas.
Le	1	'XXh'	Laukiamų duomenų ilgis. Nuskaitytinų baitų skaičius.

Pastaba: P1 8 bitas turi būti nustatytas į 0.

TCS_326 Atsakymo pranešimas (atsakyti neprašoma)

Baitas	Ilgis	Vertė	Aprašymas
#1-#X	X	'XX...XXh'	Nuskaityti duomenys.
SW	2	'XXXXh'	Būsenos žodžiai (SW1, SW2).

- Jei komanda sėkmingai įvykdoma, kortelė atsako '9000'.
- Jei nepasirinktas joks EF, atsakyme nurodoma apdorojimo būseną '6986'.
- Jei pasirinktos rinkmenos prieigos kontrolės reikalavimai neįvykdyti, atsakyme nurodoma apdorojimo būseną '6982'.
- Jei poslinkis neatitinka EF dydžio (poslinkis > EF dydis), atsakyme nurodoma apdorojimo būseną '6B00'.
- Jei nuskaitytinų duomenų dydis neatitinka EF dydžio (poslinkis + Le > EF dydis), atsakyme nurodoma apdorojimo būseną '6700' arba '6Cxx' (čia 'xx' nurodo tikslų ilgį).
- Jei rinkmenos atributuose randama nepažeistumo klaida, kortelė turi laikyti rinkmeną sugadintą ir neatkuriama, o atsakyme nurodoma apdorojimo būseną '6400' arba '6581'.
- Jei atmintyje laikomuose duomenyse randama nepažeistumo klaida, kortelė turi grąžinti pareikalautus duomenis, o atsakyme nurodoma apdorojimo būseną '6281'.

3.6.2.2. Komanda be saugaus keitimosi duomenimis

Ši komanda leidžia IFD nuskaityti duomenis iš tuo metu pasirinkto EF naudojant saugaus keitimosi pranešimais būdą, kad būtų patikrintas gautų duomenų nepažeistumas ir apsaugotas konfidencialumas, jei EF pažymėtas kaip „užkoduotas“.

TCS_327 Parancsüzenet

Baitas	Ilgis	Vertė	Aprašymas
CLA	1	'0Ch'	Saugus keitimasis pranešimais prašomas.
INS	1	'B0h'	INS
P1	1	'XXh'	P1 (poslinkis baitais nuo rinkmenos pradžios): pats svarbiausias baitas.
P2	1	'XXh'	P2 (poslinkis baitais nuo rinkmenos pradžios): mažiausiai svarbus baitas.
Lc	1	'09h'	Saugaus keitimosi pranešimais įvesties duomenų ilgis.
#6	1	'97h'	T _{LE} : laukiamo ilgio specifikacijos žymena.
#7	1	'01h'	L _{LE} : laukiamas ilgis.
#8	1	'NNh'	Laukiamo ilgio specifikacija (pradinis Le): nuskaitytinų baitų skaičius.

Baitas	Ilgis	Vertė	Aprašymas
#9	1	'8Eh'	T _{CC} : kriptografinės kontrolinės sumos žymena.
#10	1	'04h'	L _{CC} : kitos iš eilės kriptografinės kontrolinės sumos ilgis.
#11-#14	4	'XX..XXh'	Kriptografinė kontrolinė suma (4 svarbiausieji baitai).
Le	1	'00h'	Kaip nurodyta ISO/IEC 7816-4.

TCS_328 Atsakymo pranešimas, jei EF nepažymėtas kaip „užkoduotas“ ir jei saugaus keitimosi pranešimais įvesties formatas yra tinkamas:

Baitas	Ilgis	Vertė	Aprašymas
#1	1	'81h'	T _{PV} : paprastųjų verčių duomenų žymena.
#2	L	'NNh' arba '81 NNh'	L _{PV} : grąžinamų duomenų ilgis (= pradiniam Le). Jei L _{PV} > 127 baitai, L yra 2 baitai.
#(2+L)-#(1+L+NN)	NN	'XX..XXh'	Paprastųjų verčių duomenys.
#(2+L+NN)	1	'8Eh'	T _{CC} : kriptografinės kontrolinės sumos žymena.
#(3+L+NN)	1	'04h'	L _{CC} : kitos iš eilės kriptografinės kontrolinės sumos ilgis.
#(4+L+NN)-#(7+L+NN)	4	'XX..XXh'	Kriptografinė kontrolinė suma (4 svarbiausieji baitai).
SW	2	'XXXXh'	Būsenos žodžiai (SW1, SW2).

TCS_329 Atsakymo pranešimas, jei EF pažymėtas kaip „užkoduotas“ ir jei saugaus keitimosi pranešimais įvesties formatas yra tinkamas:

Baitas	Ilgis	Vertė	Aprašymas
#1	1	'87h'	T _{PI CG} : užkoduotų duomenų (kriptogramos) žymena.
#2	L	'MMh' arba '81 MMh'	L _{PI CG} : grąžinamų užkoduotų duomenų ilgis (skiriasi nuo komandos pradinio Le dėl išplėtimo). Jei L _{PI CG} > 127 baitai, L yra 2 baitai.
#(2+L)-#(1+L+MM)	MM	'01XX..XXh'	Užkoduoti duomenys: išplėtimo indikatorius ir kriptograma.
#(2+L+MM)	1	'8Eh'	T _{CC} : kriptografinės kontrolinės sumos žymena.
#(3+L+MM)	1	'04h'	L _{CC} : kitos iš eilės kriptografinės kontrolinės sumos ilgis.
#(4+L+MM)-#(7+L+MM)	4	'XX..XXh'	Kriptografinė kontrolinė suma (4 svarbiausieji baitai).
SW	2	'XXXXh'	Būsenos žodžiai (SW1, SW2).

Grąžinamų užkoduotų duomenų pirmasis baitas nurodo išplėtimo režimą. Tachografo programoje išplėtimo indikatorius vertė visuomet būna '01h', kas reiškia, jog naudotas ISO/IEC 7816-4 nustatytas išplėtimo režimas (vienas '80h' vertės baitas, po kurio yra keletas nulinių baitų: ISO/IEC 9797 2 metodas).

Aprašytos komandos READ_BINARY „įprastos“ apdorojimo būsenos, nenaudojant saugaus keitimosi pranešimais (žr. 3.6.2.1 papunktį), atsakyme gali būti nurodytos naudojant pirmiau aprašytą atsakymo pranešimų struktūrą su žymena !!!99h!!! (kaip aprašyta TCS 335).

Be to, gali įvykti tam tikrų vien tik su saugiu keitimusi pranešimais susijusių klaidų. Tokiais atvejais apdorojimo būsenos nuoroda paprasčiausiai grąžinama nenaudojant saugaus keitimosi pranešimais struktūros.

TCS_330 Atsakymo pranešimas, jei saugaus keitimosi pranešimais įvesties formatas netinkamas:

Baitas	Ilgis	Vertė	Aprašymas
SW	2	'XXXXh'	Būsenos žodžiai (SW1, SW2).

— Jei nėra jokio esamos panaudos rakto, atsakyme nurodoma apdorojimo būsena „6A88“. Taip atsitinka, jei panaudos raktas dar nesugeneruotas arba baigėsi jo galiojimo laikas (šiuo atveju IFD turi pakartoti abipusio autentiškumo patvirtinimo procesą naujam panaudos raktui nustatyti).

— Jei saugaus keitimosi pranešimais formate nerandama kai kurių laukiamų duomenų objektų (kaip nurodyta pirmiau), atsakyme nurodoma apdorojimo būsena „6987“: ši klaida įvyksta, jei nėra laukiamos žymenos, arba komandos pagrindinė dalis netinkamai sudaryta.

- Jei kai kurie duomenų objektai yra neteisingi, atsakyme nurodoma apdorojimo būsena „6988“: ši klaida įvyksta, jei yra visos reikiamos žymenos, tačiau kai kurie ilgiai skiriasi nuo lauktų.
- Jei kriptografinės kontrolinės sumos patikrinti nepavyksta, atsakyme nurodoma apdorojimo būsena „6688“.

3.6.3. UPDATE_BINARY [atnaujinti dvinarį]

Ši komanda atitinka ISO/IEC 7816-4, tačiau jos naudojimas, palyginti su standarte nustatyta komanda, yra labiau apribotas.

Komandos UPDATE_BINARY pranešimas pradeda EF dvinaryje jau esančių bitų atnaujinimą (trynimą + rašymą) komandoje APDU esančiais bitais.

TCS_331 Komandą galima atlikti tik tuomet, jei apsaugos būsena atitinka nustatytus EF funkcijos UPDATE apsaugos atributus (jei funkcijos UPDATE prieigos kontrolė naudoja PRO SM, komandą reikia papildyti saugiu keitimusi pranešimais).

3.6.3.1. Komanda be saugaus keitimosi duomenimis

Ši komanda leidžia IFD rašyti duomenis į tuo metu pasirinktą EF, kortelei netikrinant gautų duomenų nepažeistumo. Šis paprastas režimas leidžiamas tik tuomet, jei atitinkama rinkmena nepažymėta kaip „užkoduota“.

TCS_332 Komandos pranešimas

Baitas	Ilgis	Vertė	Aprašymas
CLA	1	'00h'	Saugus keitimasis pranešimais neprašomas.
INS	1	'D6h'	Poslinkis baitais nuo rinkmenos pradžios: pats svarbiausias baitas.
P1	1	'XXh'	
P2	1	'XXh'	
Lc	1	'NNh'	Poslinkis baitais nuo rinkmenos pradžios: mažiausiai svarbus baitas.
#6-#(5+NN)	NN	'XX..XXh'	Atnaujintųjų duomenų Lc ilgis. Rašytinų baitų skaičius.
			Rašytini duomenys.

Pastaba: P1 8 bitas turi būti nustatytas į 0.

TCS_333 Atsakymo pranešimas

Baitas	Ilgis	Vertė	Aprašymas
SW	2	'XXXXh'	Būsenos žodžiai (SW1, SW2).

- Jei komanda sėkmingai įvykdoma, kortelė atsako '9000'.
- Jei nepasirinktas joks EF, atsakyme nurodoma apdorojimo būsena '6986'.
- Jei pasirinktos rinkmenos prieigos kontrolės reikalavimai neįvykdyti, atsakyme nurodoma apdorojimo būsena '6982'.
- Jei poslinkis neatitinka EF dydžio (poslinkis > EF dydis), atsakyme nurodoma apdorojimo būsena '6B00'.
- Jei rašytinų duomenų dydis neatitinka EF dydžio (poslinkis + Le > EF dydis), atsakyme nurodoma apdorojimo būsena '6700'.
- Jei rinkmenos atributuose randama nepažeistumo klaida, kortelė turi laikyti rinkmeną sugadintą ir neatkuriama, o atsakyme nurodoma apdorojimo būsena '6400' arba '6500'.
- Jei rašyti nepavyksta, atsakyme nurodoma apdorojimo būsena '6581'.

3.6.3.2. Komanda be saugaus keitimosi duomenimis

Ši komanda leidžia IFD rašyti duomenis į tuo metu pasirinktą EF, kortelei tikrinant gautų duomenų nepažeistumą. Kadangi konfidencialumas nereikalaujamas, duomenys nėra užkoduoti.

TCS_334 Komandos pranešimas

Baitas	Ilgis	Vertė	Aprašymas
CLA	1	'0Ch'	Saugus keitimasis pranešimais prašomas.
INS	1	'D6h'	INS
P1	1	'XXh'	Poslinkis baitais nuo rinkmenos pradžios: pats svarbiausias baitas.
P2	1	'XXh'	Poslinkis baitais nuo rinkmenos pradžios: mažiausiai svarbus baitas.
Lc	1	'XXh'	Apsaugoto duomenų laukelio ilgis.
#6	1	'81h'	T _{PV} : paprastųjų verčių duomenų žymena.
#7	L	'NNh' arba '81 NNh'	L _{PV} : grąžinamų duomenų ilgis. Jei L _{PV} > 127 baitai, L yra 2 baitai.
#(7+L)-#(6+L+NN)	NN	'XX..XXh'	Paprastųjų verčių duomenys (rašytini duomenys).
#(7+L+NN)	1	'8Eh'	T _{CC} : kriptografinės kontrolinės sumos žymena.
#(8+L+NN)	1	'04h'	L _{CC} : kitos iš eilės kriptografinės kontrolinės sumos ilgis.
#(9+L+NN)-#(12+L+NN)	4	'XX..XXh'	Kriptografinė kontrolinė suma (4 svarbiausieji baitai).
Le	1	'00h'	Kaip nurodyta ISO/IEC 7816-4.

TCS_335 Atsakymo pranešimas, jei saugaus keitimosi pranešimais įvesties formatas yra tinkamas:

Baitas	Ilgis	Vertė	Aprašymas
#1	1	'99h'	T _{SW} : būsenos žodžių žymena (ją turi saugoti CC).
#2	1	'02h'	L _{SW} : grąžinamų būsenos žodžių ilgis.
#3-#4	2	'XXXXh'	Būsenos žodžiai (SW1, SW2).
#5	1	'8Eh'	T _{CC} : kriptografinės kontrolinės sumos žymena.
#6	1	'04h'	L _{CC} : kitos iš eilės kriptografinės kontrolinės sumos ilgis.
#7-#10	4	'XX..XXh'	Kriptografinė kontrolinė suma (4 svarbiausieji baitai).
SW	2	'XXXXh'	Būsenos žodžiai (SW1, SW2).

Aprašytos komandos UPDATE_BINARY „įprastos“ apdorojimo būsenos, nenaudojant saugaus keitimosi pranešimais (žr. 3.6.3.1 papunktį), atsakyme gali būti nurodytos naudojant pirmiau aprašytą atsakymo pranešimų struktūrą.

Be to, gali įvykti tam tikrų vien tik su saugiu keitimusi pranešimais susijusių klaidų. Tokiais atvejais apdorojimo būseną paprasčiausiai grąžinama nenaudojant saugaus keitimosi pranešimais struktūros.

TCS_336 Atsakymo pranešimas, jei saugaus keitimosi pranešimais įvesties formatas netinkamas:

Baitas	Ilgis	Vertė	Aprašymas
SW	2	'XXXXh'	Būsenos žodžiai (SW1, SW2).

- Jei nėra jokio esamos panaudos rakto, atsakyme nurodoma apdorojimo būseną „6A88“.
- Jei saugaus keitimosi pranešimais formate nerandama kai kurių laukiamų duomenų objektų (kaip nurodyta pirmiau), atsakyme nurodoma apdorojimo būseną „6987“: ši klaida įvyksta, jei nėra laukiamos žymenos, arba komandos pagrindinė dalis netinkamai sudaryta.
- Jei kai kurie duomenų objektai yra neteisingi, atsakyme nurodoma apdorojimo būseną „6988“: ši klaida įvyksta, jei yra visos reikiamos žymenos, tačiau kai kurie ilgiai skiriasi nuo lauktų.
- Jei kriptografinės kontrolinės sumos patikrinti nepavyksta, atsakyme nurodoma apdorojimo būseną „6688“.

3.6.4. GET_CHALLENGE [reikalauti slaptažodžio]

Ši komanda atitinka ISO/IEC 7816-4, tačiau jos naudojimas, palyginti su standarte nustatyta komanda, yra labiau apribotas.

Komanda GET_CHALLENGE paprašo kortelės duoti slaptažodį, kad jį galima būtų panaudoti apsaugos procedūroje, per kurią į kortelę nusiunčiama kriptograma arba tam tikri užšifruoti duomenys.

TCS_337 Kortelės duodamas slaptažodis galioja tik kitai komandai į kortelę siunčiamai komandai, kuri tą slaptažodį panaudoja.

TCS_338 Komandos pranešimas

Baitas	Ilgis	Vertė	Aprašymas
CLA	1	'00h'	CLA
INS	1	'84h'	INS
P1	1	'00h'	P1
P2	1	'00h'	P2
Le	1	'08h'	Le (laukiamas slaptažodžio ilgis)

TCS_339 Atsakymo pranešimas

Baitas	Ilgis	Vertė	Aprašymas
#1-#8	8	'XX..XXh'	Slaptažodis
SW	2	'XXXXh'	Būsenos žodžiai (SW1, SW2).

— Jei komanda sėkmingai įvykdoma, kortelė atsako '9000'.

— Jei Le yra ne '08h', apdorojimo būseną yra '6700'.

— Jei parametrai P1-P2 neteisingi, apdorojimo būseną yra '6A86'.

3.6.5. VERIFY [patikrinti]

Ši komanda atitinka ISO/IEC 7816-4, tačiau jos naudojimas, palyginti su standarte nustatyta komanda, yra labiau apribotas.

Komanda VERIFY nurodo kortelėje suliginti atsiųstus CHV (PIN) duomenis su kortelės atmintyje laikomu standartiniu CHV.

Pastaba: naudotojo įvestą PIN sąsajos įtaisas turi papildyti dešinėje prirašydamas iki 8 „FF“ baitų.

TCS_340 Jei komanda yra sėkmingai įvykdoma, atidaromos CHV pateikimą atitinkančios teisės ir iš naujo paleidžiamas CHV mėginimų skaitiklis.

TCS_341 Jei suliginimas nepavyksta, jis registruojamas kortelėje, kad būtų apribotas papildomų mėginimų panaudoti standartinį CHV skaičius.

TCS_342 Komandos pranešimas

Baitas	Ilgis	Vertė	Aprašymas
CLA	1	'00h'	CLA
INS	1	'20h'	INS
P1	1	'00h'	P1
P2	1	'00h'	P2 (patikrintas CHV netiesiogiai žinomas)
Lc	1	'08h'	Persiūsto CHV kodo ilgis.
#6-#13	8	'XX..XXh'	CHV

TCS_343 Atsakymo pranešimas

Baitas	Ilgis	Vertė	Aprašymas
SW	2	'XXXXh'	Būsenos žodžiai (SW1, SW2).

- Jei komanda sėkmingai įvykdoma, kortelė atsako '9000'.
- Jei standartinis CHV nerandamas, atsakyme nurodoma apdorojimo būseną '6A86'.
- Jei CHV užblokuotas (likusių mėginimų skaitiklio vertė lygi nuliui), atsakyme nurodoma apdorojimo būseną '6983'. Esant šiai būsenai CHV daugiau nebegalima pateikti.
- Jei sulyginimas nepavyksta, likusių mėginimų skaitiklio vertė sumažėja, o atsakyme nurodoma būseną '63CX' (X > 0, o X reiškia likusių CHV mėginimų skaitiklio vertę. X = 'F', CHV mėginimų skaitiklio vertė didesnė už 'F').
- Jei standartinis CHV laikomas sugadintu, atsakyme nurodoma būseną '6400' arba '6581'.

3.6.6. GET_RESPONSE [gauti atsakymą]

Ši komanda atitinka ISO/IEC 7816-4.

Ši komanda (ji būtina ir galima tik naudojant protokolą T=0) naudojama paruoštiems duomenims persiųsti iš kortelės į sąsajos įtaisą (atvejais, kai komandoje yra tiek Lc, tiek Le).

Komanda GET_RESPONSE turi būti duodama tuoj po duomenims paruošiančios komandos, priešingu atveju duomenys prarandami. Įvykdžius komandą GET_RESPONSE (išskyrus atvejus, kai įvyksta klaida '61xx' arba '6Cxx', žr. toliau), pirmiau paruošti duomenys tampa nebe prieinami.

TCS_344 Komandos pranešimas

Baitas	Ilgis	Vertė	Aprašymas
CLA	1	'00h'	
INS	1	'C0h'	
P1	1	'00h'	
P2	1	'00h'	
Le	1	'XXh'	Laukiamas baitų skaičius.

TCS_345 Atsakymo pranešimas

Baitas	Ilgis	Vertė	Aprašymas
#1-#X	X	'XX..XXh'	Duomenys
SW	2	'XXXXh'	Būsenos žodžiai (SW1, SW2).

- Jei komanda sėkmingai įvykdoma, kortelė atsako '9000'.
- Jei kortelei duomenų nebuvo paruošta, atsakyme nurodoma apdorojimo būseną '6900' arba '6F00'.
- Jei Le viršija galimų baitų skaičių arba lygus nuliui, atsakyme nurodoma apdorojimo būseną '6Cxx' (čia 'xx' nurodo tikslų galimų baitų skaičių). Tokiu atveju paruošti duomenys tebėra prieinami kitai komandai GET_RESPONSE.
- Jei Le nėra lygus nuliui ir yra mažesnis už galimų baitų skaičių, reikalaujamus duomenis kortelė išsiunčia įprastai, o atsakyme nurodoma apdorojimo būseną '61xx' (čia 'xx' nurodo dar galimų panaudoti su kita komanda GET_RESPONSE baitų skaičių).
- Jei komanda netinkama (protokolas T=1), kortelė atsako '6D00'.

3.6.7. PSO: VERIFY_CERTIFICATE [PSO: patikrinti pažymėjimą]

Ši komanda atitinka ISO/IEC 7816-8, tačiau jos naudojimas, palyginti su standarte nustatyta komanda, yra labiau apribotas.

Komandą VERIFY_CERTIFICATE kortelė naudoja atvirajam raktui iš išorės gauti ir jo galiojimui patikrinti.

TCS_346 Kai komanda VERIFY_CERTIFICATE yra sėkmingai įvykdoma, atvirasis raktas įrašomas į atmintį būsimam panaudojimui apsaugos aplinkoje. Šis raktas komanda MSE (žr. 3.6.10 punktą), naudojant jo rakto vardą, turi būti aiškiai nustatytas naudoti su apsaugos komandomis (INTERNAL_AUTHENTICATE, EXTERNAL_AUTHENTICATE arba VERIFY_CERTIFICATE).

TCS_347 Bet kuriuo atveju pažymėjimui atidaryti komanda VERIFY_CERTIFICATE naudoja atvirąjį raktą, kurį anksčiau parinko komanda MSE. Šis atvirasis raktas turi būti valstybės narės arba europinis.

TCS_348 Komandos pranešimas

Baitas	Ilgis	Vertė	Aprašymas
CLA	1	'00h'	CLA
INS	1	'2Ah'	Atlikti apsaugos operaciją.
P1	1	'00h'	P1
P2	1	'AEh'	P2: ne pagal BER-TLV užkoduoti duomenys (duomenų elementų sąryšis).
Lc	1	'CEh'	Lc: pažymėjimo ilgis, 194 baitai.
#6-#199	194	'XX.XXh'	Pažymėjimas: duomenų elementų sąryšis (kaip aprašyta 11 priedėlyje).

TCS_349 Atsakymo pranešimas

Baitas	Ilgis	Vertė	Aprašymas
SW	2	'XXXXh'	Būsenos žodžiai (SW1, SW2).

- Jei komanda sėkmingai įvykdoma, kortelė atsako '9000'.
- Jei pažymėjimo patikrinti nepavyksta, atsakyme nurodoma apdorojimo būseną '6688'. Pažymėjimo tikrinimo ir išnagrinėjimo procesas aprašytas 11 priedėlyje.
- Jei apsaugos aplinkoje nėra atvirojo rakto, atsakyme nurodoma apdorojimo būseną '6A88'.
- Jei pasirinktas atvirasis raktas (naudotas pažymėjimui išnagrinėti) laikomas sugadintu, atsakyme nurodoma apdorojimo būseną '6400' arba '6581'.
- Jei pasirinkto atvirojo rakto (naudoto pažymėjimui išnagrinėti) CHA.LSB (CertificateHolderAuthorisation.equipmentType) yra ne '00' (t. y. jis yra ne valstybės narės ir ne europinis), atsakyme nurodoma apdorojimo būseną '6985'.

3.6.8. INTERNAL_AUTHENTICATE [vidinis autentiškumo tikrinimas]

Ši komanda atitinka ISO/IEC 7816-4.

Naudodamasis komanda INTERNAL_AUTHENTICATE sąsajos įtaisas gali patikrinti kortelės autentiškumą.

Autentiškumo tikrinimo procesas aprašytas 11 priedėlyje. Jį sudaro tokios instrukcijos:

TCS_350 Autentiškumo tikrinimo duomenims, įskaitant K1 (pirmasis panaudos rakto sutarties elementas) ir RND1, pasirašyti komanda INTERNAL_AUTHENTICATE naudoja kortelės slaptaįjį raktą (netiesiogiai pasirinktą), o parašui užkoduoti ir autentiškumo tikrinimo leksemui suformuoti – esamu metu pasirinktą atvirąjį raktą (naudodamasi komanda MSE) (išsamiau aprašyta 11 priedėlyje).

TCS_351 Komandos pranešimas

Baitas	Ilgis	Vertė	Aprašymas
CLA	1	'00h'	CLA
INS	1	'88h'	INS
P1	1	'00h'	P1
P2	1	'00h'	P2
Lc	1	'10h'	I kortelę nusiųstų duomenų ilgis.
#6-#13	8	'XX..XXh'	Kortelės autentiškumui patikrinti naudotas slaptažodis.
#14-#21	8	'XX..XXh'	VU.CHR (žr. 11 priedėlį).
Le	1	'80h'	Iš kortelės laukiamų duomenų ilgis.

TCS_352 Atsakymo pranešimas

Baitas	Ilgis	Vertė	Aprašymas
#1-#128	128	'XX..XXh'	Kortelės autentiškumo tikrinimo leksema (žr. 11 priedėlį).
SW	2	'XXXXh'	Būsenos žodžiai (SW1, SW2).

- Jei komanda sėkmingai įvykdoma, kortelė atsako '9000'.
- Jei apsaugos aplinkoje nėra atvirojo rakto, atsakyme nurodoma apdorojimo būseną '6A88'.
- Jei apsaugos aplinkoje nėra slaptojo rakto, atsakyme nurodoma apdorojimo būseną '6A88'.
- Jei VU.CHR neatitinka esamo atvirojo rakto vardo, atsakyme nurodoma apdorojimo būseną '6A88'.
- Jei pasirinktas atvirasis raktas laikomas sugadintu, atsakyme nurodoma apdorojimo būseną '6400' arba '6581'.

TCS_353 Jei komanda INTERNAL_AUTHENTICATE yra sėkmingai įvykdoma, esamas panaudos raktas (jei yra) yra ištrinamas ir daugiau nenaudojamas. Tam, kad galima būtų gauti naują panaudos raktą, reikia sėkmingai įvykdyti komandą EXTERNAL_AUTHENTICATE.

3.6.9. EXTERNAL_AUTHENTICATE [išorinis autentiškumo tikrinimas]

Ši komanda atitinka ISO/IEC 7816-4.

Naudodamasi komanda EXTERNAL_AUTHENTICATE kortelė gali patikrinti IFD autentiškumą.

Autentiškumo tikrinimo procesas aprašytas 11 priedėlyje. Jį sudaro tokios instrukcijos:

TCS_354 Prieš pat komandą EXTERNAL_AUTHENTICATE turi būti duodama komanda GET_CHALLENGE. Kortelė suteikia slaptažodį (RND3).

TCS_355 Tikrinant kriptogramą naudojamas RND3 (kortelės suteiktas slaptažodis), kortelės slapstasis raktas (netiesiogiai pasirinktas) ir anksčiau komanda MSE pasirinktas atvirasis raktas.

TCS_356 Kortelė patikrina kriptogramą ir, jei ji tinkama, atidaroma prieigos sąlyga AUT.

TCS_357 Įvesties kriptogramoje yra antrasis panaudos rakto sutarties elementas K2.

TCS_358 Komandos pranešimas

Baitas	Ilgis	Vertė	Aprašymas
CLA	1	'00h'	CLA
INS	1	'82h'	INS
P1	1	'00h'	P1
P2	1	'00h'	P2 (naudotinas atvirasis raktas yra netiesiogiai žinomas ir anksčiau nustatytas komanda MSE).
Lc	1	'80h'	Lc (i kortelę nusiųstų duomenų ilgis).
#6-#133	128	'XX..XXh'	Kriptograma (žr. 11 priedėlį).

TCS_359 Atsakymo pranešimas

Baitas	Ilgis	Vertė	Aprašymas
SW	2	'XXXXh'	Būsenos žodžiai (SW1, SW2).

- Jei komanda sėkmingai įvykdoma, kortelė atsako '9000'.
- Jei apsaugos aplinkoje nėra atvirojo rakto, atsakyme nurodoma apdorojimo būseną '6A88<'.
- Jei esamu metu nustatyto atvirojo rakto CHA nėra tachografo programos AID ir TPB įrangos tipo sąryšis, atsakyme nurodoma apdorojimo būseną '6F00' (žr. 11 priedėlį).
- Jei apsaugos aplinkoje nėra slaptojo rakto, atsakyme nurodoma apdorojimo būseną '6A88'.
- Jei kriptogramos patikrinimas neteisingas, atsakyme nurodoma apdorojimo būseną '6688'.
- Jei prieš komandą nėra komandos GET_CHALLENGE, atsakyme nurodoma apdorojimo būseną '6985'.
- Jei pasirinktas atvirasis raktas laikomas sugadintu, atsakyme nurodoma apdorojimo būseną '6400' arba '6581'.

TCS_360 Jei komanda EXTERNAL_AUTHENTICATE yra sėkmingai įvykdoma ir galima pasinaudoti neseniai atliktos INTERNAL_AUTHENTICATE panaudos raktu, saugaus keitimosi pranešimais būdu nustatomas panaudos raktas būsimoms komandoms.

TCS_361 Jei iš ankstesnės komandos INTERNAL_AUTHENTICATE pirmojo panaudos rakto dalis nebeprieinama, antroji jo dalis, kurią atsiunčia IFD, kortelės atmintyje neišsaugoma. Šis mechanizmas užtikrina, kad abipusio autentiškumo patvirtinimo procesas vyktų 11 priedėlyje nustatyta tvarka.

3.6.10. **MANAGE_SECURITY_ENVIRONMENT (MSE)** [valdyti apsaugos aplinką]

Ši komanda skirta nustatyti atvirąjį raktą, skirtą autentiškumui patvirtinti.

Ši komanda atitinka ISO/IEC 7816-8. Šios komandos naudojimas apribotas pagal atitinkamą standartą.

TCS_362 MSE duomenų laukelyje nurodytas raktas galioja visoms tachografo DF rinkmenoms.

TCS_363 MSE duomenų laukelyje nurodytas raktas lieka esamuoju atviruoju raktu iki kitos teisingos MSE komandos.

TCS_364 Jei nurodyto rakto kortelėje (jau) nėra, apsaugos aplinka lieka nepakitusi.

TCS_365 Komandos pranešimas

Baitas	Ilgis	Vertė	Aprašymas
CLA	1	'00h'	CLA
INS	1	'22h'	INS
P1	1	'C1h'	P1: nurodytas raktas galioja visoms kriptografinėms operacijoms.
P2	1	'B6h'	P2 (nurodyti duomenys apie skaitmeninį raktą).
Lc	1	'0Ah'	Lc (į kortelę nusiųstų duomenų ilgis).
#6	1	'83h'	Atvirojo rakto nurodymo žymena asimetriškais atvejais.
#7	1	'08h'	Rakto nuorodos (rakto vardo) ilgis.
#8-#15	08h	'XX..XXh'	Kriptograma (žr. 11 priedėlį).

TCS_366 Atsakymo pranešimas

Baitas	Ilgis	Vertė	Aprašymas
SW	2	'XXXXh'	Būsenos žodžiai (SW1, SW2).

- Jei komanda sėkmingai įvykdoma, kortelė atsako '9000'.
- Jei kortelėje nėra nurodyto rakto, atsakyme nurodoma apdorojimo būseną '6A88'.
- Jei saugaus keitimosi pranešimais formatu nėra kai kurių lauktų duomenų objektų, atsakyme nurodoma apdorojimo būseną '6987'. Taip gali įvykti, jei nėra žymenos '83h'.
- Jei kai kurie iš duomenų objektų yra neteisingi, atsakyme nurodoma apdorojimo būseną '6988'. Taip gali įvykti, jei kriptogramos ilgis yra ne '08h'.
- Jei pasirinktas atvirasis raktas laikomas sugadintu, atsakyme nurodoma apdorojimo būseną '6400' arba '6581'.

3.6.11. **PSO: HASH [PSO: maiša]**

Ši komanda naudojama persiųsti į kortelę kai kurių duomenų maišiojo skaičiavimo rezultatus. Ji naudojama skaitmeniniams parašams tikrinti. Maišioji vertė laikoma atmintyje EEPROM kitai komandai „patikrinti skaitmeninį parašą“.

Ši komanda atitinka ISO/IEC 7816-87. Šios komandos naudojimas apribotas pagal atitinkamą standartą.

TCS_367 Komandos pranešimas

Baitas	Ilgis	Vertė	Aprašymas
CLA	1	'00h'	CLA
INS	1	'2Ah'	Atlikti apsaugos operaciją.
P1	1	'90h'	Grąžinti maišos kodą.
P2	1	'A0h'	Žymena: duomenų laukelyje yra maišai reikalingi DO.
Lc	1	'16h'	Kito duomenų laukelio ilgis Lc.
#6	1	'90h'	Maišos kodo žymena.
#7	1	'14h'	Maišos kodo ilgis.
#8-#27	20	'XX..XXh'	Maišos kodas.

TCS_368 Atsakymo pranešimas

Baitas	Ilgis	Vertė	Aprašymas
SW	2	'XXXXh'	Būsenos žodžiai (SW1, SW2).

- Jei komanda sėkmingai įvykdoma, kortelė atsako '9000'.
- Jei nėra kai kurių lauktų duomenų objektų (kaip nurodyta pirmiau), atsakyme nurodoma apdorojimo būseną '6987'. Taip gali įvykti, jei nėra žymenos '90h'.
- Jei kai kurie iš duomenų objektų yra neteisingi, atsakyme nurodoma apdorojimo būseną '6988'. Ši klaida įvyksta, jei reikiama žymena yra, tačiau jos ilgis yra ne '14h'.

3.6.12. **PERFORM_HASH_OF_FILE [atlikti rinkmenos maišą]**

Ši komanda neatitinka ISO/IEC 7816-8. Taigi šios komandos baitas CLA rodo, kad PERFORM_SECURITY_OPERATION/HASH naudojimas yra slapstasis.

TCS_369 Komanda PERFORM_HASH_OF_FILE naudojama esamu metu pasirinkto EF duomenų srities maišai atlikti.

TCS_370 Maišos operacijos rezultatas įrašomas į kortelės atmintį. Tuomet jį galima panaudoti rinkmenos skaitmeniniam parašui gauti naudojant komandą `PSO-COMPUTE_DIGITAL_SIGNATURE`. Šis rezultatas lieka galioti komandai `COMPUTE_DIGITAL_SIGNATURE` iki kitos sėkmingai įvykdomos komandos `PERFORM_HASH_OF_FILE`.

TCS_371 Komandos pranešimas

Baitas	Ilgis	Vertė	Aprašymas
CLA	1	'80h'	CLA
INS	1	'2Ah'	Atlikti apsaugos operaciją.
P1	1	'90h'	Žymena: maiša.
P2	1	'00h'	P2: atlikti esamu metu pasirinktos atvirosios rinkmenos maišą.

TCS_372 Atsakymo pranešimas

Baitas	Ilgis	Vertė	Aprašymas
SW	2	'XXXXh'	Būsenos žodžiai (SW1, SW2).

- Jei komanda sėkmingai įvykdoma, kortelė atsako '9000'.
- Jei nepasirenkama jokia programa, atsakyme nurodoma apdorojimo būsena '6985'.
- Jei pasirinkta EF laikoma sugadinta (yra rinkmenos atributų arba laikomų duomenų klaidų), atsakyme nurodoma apdorojimo būsena '6400' arba '6581'.
- Jei pasirinkta rinkmena nėra atvirosi, atsakyme nurodoma apdorojimo būsena '6986'.

3.6.13. **PSO: COMPUTE_DIGITAL_SIGNATURE** [PSO: *apskaičiuoti skaitmeninį parašą*]

Ši komanda naudojama anksčiau apskaičiuoto maišos kodo (žr. 3.6.12 punktą `PERFORM_HASH_OF_FILE`) skaitmeniniam parašui apskaičiuoti.

Ši komanda atitinka ISO/IEC 7816-8. Šios komandos naudojimas apribotas pagal atitinkamą standartą.

TCS_373 Kortelės slapstasis raktas naudojamas skaitmeniniam parašui apskaičiuoti ir yra netiesiogiai žinomas kortelei.

TCS_374 Kortelė sudaro skaitmeninį paršą naudodama išplėtimo metodą, kuris atitinka PKCS1 (išsamiau skaitykite 11 priedėlyje).

TCS_375 Komandos pranešimas

Baitas	Ilgis	Vertė	Aprašymas
CLA	1	'00h'	CLA
INS	1	'2Ah'	Atlikti apsaugos operaciją.
P1	1	'9Eh'	Grąžintinas skaitmeninis parašas.
P2	1	'9Ah'	Žymena: duomenų laukelyje yra pasirašytini duomenys. Jei duomenų laukelio nėra, duomenys jau turėtų būti kortelėje (rinkmenos maiša).
Le	1	'80h'	Laukiamo parašo ilgis.

TCS_376 Atsakymo pranešimas

Baitas	Ilgis	Vertė	Aprašymas
#1-#128	128	'XX..XXh'	Anksčiau apskaičiuotos maišos parašas.
SW	2	'XXXXh'	Būsenos žodžiai (SW1, SW2).

- Jei komanda sėkmingai įvykdoma, kortelė atsako '9000'.
- Jei netiesiogiai pasirinktas slapstasis raktas laikomas sugadintu, atsakyme nurodoma apdorojimo būsena '6400' arba '6581'.

3.6.14. PSO: VERIFY_DIGITAL_SIGNATURE [PSO: patikrinti skaitmeninį parašą]

Ši komanda naudojama patikrinti skaitmeninį parašą, kuris pateikiamas kaip įvestis pagal pranešimo, kurio maiša kortelei yra žinoma, PKCS1.

Ši komanda atitinka ISO/IEC 7816-8. Šios komandos naudojimas apribotas pagal atitinkamą standartą.

TCS_377 Komanda VERIFY_DIGITAL_SIGNATURE visuomet naudoja atvirąjį raktą, kurį pasirinko ankstesnė komanda MANAGE_SECURITY_ENVIRONMENT, ir ankstesnį maišos kodą, kurį įvedė PSO – maišos komandą.

TCS_378 Komandos pranešimas

Baitas	Ilgis	Vertė	Aprašymas
CLA	1	'00h'	CLA
INS	1	'2Ah'	Atlikti apsaugos operaciją.
P1	1	'00h'	Žymena: duomenų laukelyje yra tikrinimui reikalingi DO.
P2	1	'A8h'	
Lc	1	'83h'	Kito duomenų laukelio ilgis Lc.
#28	1	'9Eh'	Skaitmeninio parašo žymena.
#29-#30	2	'8180h'	Skaitmeninio parašo ilgis (128 baitai, užkoduotas pagal ISO/IEC 7816-6).
#31-#158	128	'XX..XXh'	Skaitmeninio parašo turinys.

TCS_379 Atsakymo pranešimas

Baitas	Ilgis	Vertė	Aprašymas
SW	2	'XXXXh'	Būsenos žodžiai (SW1, SW2).

- Jei komanda sėkmingai įvykdoma, kortelė atsako '9000'.
- Jei parašo patikrinti nepavyksta, atsakyme nurodoma apdorojimo būseną '6688'. Tikrinimo procesas aprašytas 11 priedėlyje.
- Jei nepasirinktas joks atvirasis raktas, atsakyme nurodoma apdorojimo būseną '6A88'.
- Jei nėra kai kurių lauktų duomenų objektų (kaip nurodyta pirmiau), atsakyme nurodoma apdorojimo būseną '6987'. Taip gali įvykti, jei nėra vienos iš reikalingų žymenų.
- Jei komandai apdoroti nėra maišos kodo (dėl ankstesnio PSO: maišos komandos), atsakyme nurodoma apdorojimo būseną '6985'.
- Jei kai kurie iš duomenų objektų yra neteisingi, atsakyme nurodoma apdorojimo būseną '6988'. Ši klaida įvyksta, jei vieno iš reikiamų duomenų objektų ilgis yra neteisingas.
- Jei pasirinktas atvirasis raktas laikomas sugadintu, atsakyme nurodoma apdorojimo būseną '6400' arba '6581'.

4. TACHOGRAFO KORTELIŲ STRUKTŪRA

Šiame skyriuje nurodyta tachografo kortelių struktūra, skirta prieinamiems duomenims laikyti.

Čia nenustatyta nuo kortelės gamintojo priklausanti vidinė struktūra, pvz., rinkmenų antraštės, taip pat tik vidaus naudojimui reikalingų duomenų elementų, pvz., `EuropeanPublicKey`, `CardPrivateKey`, `TDesSessionKey` arba `WorkshopCardPin`, laikymas ir tvarkymas.

Tachografų kortelių naudinga duomenų laikymo talpa turi būti ne mažesnė kaip 11 kB. Talpa gali būti ir didesnė. Tokiu atveju kortelės struktūra lieka tokia pati, tačiau padidėja įrašų skaičius kai kuriuose struktūros elementuose. Šiame skyriuje nurodytos mažiausios ir didžiausios šių įrašų skaičių vertės.

4.1. Vairuotojo kortelės struktūra

TCS_400 Atlikus suasmeninimą vairuotojo kortelės nuolatinė rinkmenų struktūra ir prieigos sąlygos turi būti tokios:

Rinkmena	Rinkmenos ID	Prieigos sąlygos		
		Skaityti	Atnaujinti	Užkoduoti
MF	3F00			
EF ICC	0002	ALW	NEV	No
EF IC	0005	ALW	NEV	No
DF Tachograph	0500			
EF Application_Identification	0501	ALW	NEV	No
EF Card_Certificate	C100	ALW	NEV	No
EF CA_Certificate	C108	ALW	NEV	No
EF Identification	0520	ALW	NEV	No
EF Card_Download	050E	ALW	ALW	No
EF Driving_Licence_Info	0521	ALW	NEV	No
EF Events_Data	0502	ALW	PRO SM / AUT	No
EF Faults_Data	0503	ALW	PRO SM / AUT	No
EF Driver_Activity_Data	0504	ALW	PRO SM / AUT	No
EF Vehicles_Used	0505	ALW	PRO SM / AUT	No
EF Places	0506	ALW	PRO SM / AUT	No
EF Current_Usage	0507	ALW	PRO SM / AUT	No
EF Control_Activity_Data	0508	ALW	PRO SM / AUT	No
EF Specific_Conditions	0522	ALW	PRO SM / AUT	No

TCS_401 Visa EF struktūra turi būti atvira.

TCS_402 Visas DF tachografo rinkmenas turi būti įmanoma nuskaityti saugaus keitimosi pranešimais būdu.

TCS_403 Vairuotojo kortelės duomenų struktūra turi būti tokia:

Rinkmena/duomenų elementas	Įrašų skaičius	Dydis (baitais)		Numatytosios vertės
		Min.	Max.	
MF	11411	24959		
EF ICC	25	25		
CardIccIdentification	25	25		
clockStop	1	1		{00}
cardExtendedSerialNumber	8	8		{00..00}
cardApprovalNumber	8	8		{20..20}
cardPersonaliserID	1	1		{00}
embedderIcAssemblerId	5	5		{00..00}
icIdentifier	2	2		{00 00}
EF IC	8	8		
CardChipIdentification	8	8		
icSerialNumber	4	4		{00..00}
icManufacturingReferences	4	4		{00..00}
DF Tachograph	11378	24926		
EF Application_Identification	10	10		
DriverCardApplicationIdentification	10	10		
typeOfTachographCardId	1	1		{00}
cardStructureVersion	2	2		{00 00}
noOfEventsPerType	1	1		{00}
noOfFaultsPerType	1	1		{00}
activityStructureLength	2	2		{00 00}
noOfCardVehicleRecords	2	2		{00 00}
noOfCardPlaceRecords	1	1		{00}
EF Card_Certificate	194	194		
CardCertificate	194	194		{00..00}
EF CA_Certificate	194	194		
MemberStateCertificate	194	194		{00..00}
EF Identification	143	143		
CardIdentification	65	65		
cardIssuingMemberState	1	1		{00}
cardNumber	16	16		{20..20}
cardIssuingAuthorityName	36	36		{20..20}
cardIssueDate	4	4		{00..00}
cardValidityBegin	4	4		{00..00}
cardExpiryDate	4	4		{00..00}
DriverCardHolderIdentification	78	78		
cardHolderName	72	72		
holderSurname	36	36		{00, 20..20}
holderFirstNames	36	36		{00, 20..20}
cardHolderBirthDate	4	4		{00..00}
cardHolderPreferredLanguage	2	2		{20 20}

EF Card_Download		4	4	
LastCardDownload		4	4	
EF Driving_Licence_Info		53	53	
CardDrivingLicenceInformation		53	53	
drivingLicenceIssuingAuthority		36	36	{00, 20..20}
drivingLicenceIssuingNation		1	1	{00}
drivingLicenceNumber		16	16	{20..20}
EF Events_Data		864	1728	
CardEventData		864	1728	
cardEventRecords	6	144	288	
CardEventRecord	n ₁	24	24	
eventType		1	1	{00}
eventBeginTime		4	4	{00..00}
eventEndTime		4	4	{00..00}
eventVehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
EF Faults_Data		576	1152	
CardFaultData		576	1152	
cardFaultRecords	2	288	576	
CardFaultRecord	n ₂	24	24	
faultType		1	1	{00}
faultBeginTime		4	4	{00..00}
faultEndTime		4	4	{00..00}
faultVehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
EF Driver_Activity_Data		5548	13780	
CardDriverActivity		5548	13780	
activityPointerOldestDayRecord		2	2	{00 00}
activityPointerNewestRecord		2	2	{00 00}
activityDailyRecords	n ₆	5544	13776	{00..00}
EF Vehicles_Used		2606	6202	
CardVehiclesUsed		2606	6202	
vehiclePointerNewestRecord		2	2	{00 00}
cardVehicleRecords		2604	6200	
CardVehicleRecord	n ₃	31	31	
vehicleOdometerBegin		3	3	{00..00}
vehicleOdometerEnd		3	3	{00..00}
vehicleFirstUse		4	4	{00..00}
vehicleLastUse		4	4	{00..00}
vehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
vuDataBlockCounter		2	2	{00 00}
EF Places		841	1121	
CardPlaceDailyWorkPeriod		841	1121	
placePointerNewestRecord		1	1	{00}
placeRecords		840	1120	
PlaceRecord	n ₄	10	10	
entryTime		4	4	{00..00}
entryTypeDailyWorkPeriod		1	1	{00}
dailyWorkPeriodCountry		1	1	{00}
dailyWorkPeriodRegion		1	1	{00}
vehicleOdometerValue		3	3	{00..00}
EF Current_Usage		19	19	
CardCurrentUse		19	19	
sessionOpenTime		4	4	{00..00}
sessionOpenVehicle				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
EF Control_Activity_Data		46	46	
CardControlActivityDataRecord		46	46	
controlType		1	1	{00}
controlTime		4	4	{00..00}
controlCardNumber				
cardType		1	1	{00}
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
controlVehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
controlDownloadPeriodBegin		4	4	{00..00}
controlDownloadPeriodEnd		4	4	{00..00}
EF Specific_Conditions		280	280	
SpecificConditionRecord	56	5	5	
entryTime		4	4	{00..00}
SpecificConditionType		1	1	{00}

TCS_404 Vairuotojo kortelės duomenų struktūroje turi būti naudojamos tokios didžiausios ir mažiausios įrašų skaičiaus vertės pirmiau esančioje lentelėje pateiktiems dydžiams nurodyti.

		Mažiausia	Didžiausia
n ₁	NoOfEventsPerType	6	12
n ₂	NoOfFaultsPerType	12	24
n ₃	NoOfCardVehicleRecords	84	200
n ₄	NoOfCardPlaceRecords	84	112
n ₆	CardActivityLengthRange	5 544baitai (28 dienos po 93 veiklos rūšių pokyčius)	13 776 baitai (28 dienos po 240 veiklos rūšių pokyčių)

4.2. Dirbtuvių kortelės struktūra

TCS_405 Atlikus suasmeninimą dirbtuvių kortelės nuolatinė rinkmenų struktūra ir prieigos sąlygos turi būti tokios:

Rinkmena	Rinkmenos ID	Prieigos sąlygos		
		Skaityti	Atnaujinti	Užkodota
MF	3F00			
EF ICC	0002	ALW	NEV	No
EF IC	0005	ALW	NEV	No
DF Tachograph	0500			
EF Application_Identification	0501	ALW	NEV	No
EF Card_Certificate	C100	ALW	NEV	No
EF CA_Certificate	C108	ALW	NEV	No
EF Identification	0520	ALW	NEV	No
EF Card_Download	0509	ALW	ALW	No
EF Calibration	050A	ALW	PRO SM / AUT	No
EF Sensor_Installation_Data	050B	ALW	NEV	Yes
EF Events_Data	0502	ALW	PRO SM / AUT	No
EF Faults_Data	0503	ALW	PRO SM / AUT	No
EF Driver_Activity_Data	0504	ALW	PRO SM / AUT	No
EF Vehicles_Used	0505	ALW	PRO SM / AUT	No
EF Places	0506	ALW	PRO SM / AUT	No
EF Current_Usage	0507	ALW	PRO SM / AUT	No
EF Control_Activity_Data	0508	ALW	PRO SM / AUT	No
EF Specific_Conditions	0522	ALW	PRO SM / AUT	No

TCS_406 Visa EF struktūra turi būti atvira.

TCS_407 Visas DF tachografo rinkmenas turi būti įmanoma nuskaityti saugaus keitimosi pranešimais būdu.

TCS_408 Dirbtuvių kortelės duomenų struktūra turi būti tokia:

Rinkmena/duomenų elementas	Įrašų skaičius	Dydis (baitais)		Numatytosios vertės
		Min.	Max.	
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 Dirbtuvių kortelės duomenų struktūroje turi būti naudojamos tokios didžiausios ir mažiausios įrašų skaičiaus vertės pirmiau esančioje lentelėje pateiktiems dydžiams nurodyti.

		Mažiausia	Didžiausia
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 baitai (1 diena, 93 veiklos rūšių pokyčiai)	492 baitai (1 diena, 240 veiklos rūšių pokyčių)

4.3. Kontrolės kortelės struktūra

TCS_410 Atlikus suasmeninimą kontrolės kortelės nuolatinė rinkmenų struktūra ir prieigos sąlygos turi būti tokios:

Rinkmena	Rinkmenos ID	Prieigos sąlygos		
		Skaityti	Atnaujinti	Užkoduota
MF	3F00			
EF ICC	0002	ALW	NEV	No
EF IC	0005	ALW	NEV	No
DF Tachograph	0500			
EF Application_Identification	0501	ALW	NEV	No
EF Card_Certificate	C100	ALW	NEV	No
EF CA_Certificate	C108	ALW	NEV	No
EF Identification	0520	AUT	NEV	No
EF Controller_Activity_Data	050C	ALW	PRO SM / AUT	No

TCS_411 Visa EF struktūra turi būti atvira.

TCS_412 Visas DF tachografo rinkmenas turi būti įmanoma nuskaityti saugaus keitimosi pranešimais būdu.

TCS_413 Kontrolės kortelės duomenų struktūra turi būti tokia:

Rinkmena/duomenų elementas	Įrašų skaičius	Dydis (baitais)		Numatytosios vertės
		Min.	Max.	
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 Kontrolės kortelės duomenų struktūroje turi būti naudojamos tokios didžiausios ir mažiausios įrašų skaičiaus vertės pirmiau esančioje lentelėje pateiktiems dydžiams nurodyti.

		Mažiausia	Didžiausia
n ₇	NoOfControlActivityRecords	230	520

4.4. Įmonės kortelės struktūra

TCS_415 Atlikus suasmeninimą įmonės kortelės nuolatinė rinkmenų struktūra ir prieigos sąlygos turi būti tokios:

Rinkmena	Rinkmenos ID	Prieigos sąlygos		
		Skaityti	Atnaujinti	Užkoduoti
MF	3F00			
EF ICC	0002	ALW	NEV	No
EF IC	0005	ALW	NEV	No
DF Tachograph	0500			
EF Application_Identification	0501	ALW	NEV	No
EF Card_Certificate	C100	ALW	NEV	No
EF CA_Certificate	C108	ALW	NEV	No
EF Identification	0520	AUT	NEV	No
EF Company_Activity_Data	050D	ALW	PRO SM / AUT	No

TCS_416 Visa EF struktūra turi būti atvira.

TCS_417 Visas DF tachografo rinkmenas turi būti įmanoma nuskaityti saugaus keitimosi pranešimais būdu.

TCS_418 Įmonės kortelės duomenų struktūra turi būti tokia:

Rinkmena/duomenų elementas	Įrašų skaičius	Dydis (baitais)		Numatytosios vertės
		Min.	Max.	
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 Įmonės kortelės duomenų struktūroje turi būti naudojamos tokios didžiausios ir mažiausios įrašų skaičiaus vertės pirmiau esančioje lentelėje pateiktiems dydžiams nurodyti.

		Mažiausia	Didžiausia
n ₈	NoOfCompanyActivityRecords	230	520

3 priedėlis

PIKTOGRAMOS

PIC_001 Tachografas gali naudoti tokias piktogramas ir jų derinius:

1. PAGRINDINĖS PIKTOGRAMOS

	Žmonės	Veiksmai	Darbo režimai
	Įmonė		Įmonės režimas
	Kontrolierius	Kontrolė	Kontrolės režimas
	Vairuotojas	Vairuotojas	Naudojimo režimas
	Dirbtuvė (tikrinimų stotis)	Patikra/kalibravimas	Kalibravimo režimas
	Gamintojas		
	Veikla	Trukmė	
	Pasirengęs dirbti	Esamas buvimo pasirengus dirbti laikotarpis	
	Vairuoja	Nepertraukiamo vairavimo trukmė	
	Ilsisi	Esamas poilsio laikotarpis	
	Dirba	Esamas darbo laikotarpis	
	Pertrauka	Bendroji poilsio trukmė	
	Nežinoma		
	Įranga	Funkcijos	
	Vairuotojo plyšys		
	Vairuotojo porininko plyšys		
	Kortelė		
	Laikrodis		
	Ekranas	Rodymas ekrane	
	Išorinė laikmena	Duomenų perkėlimas	
	Maitinimas		
	Spausdintuvas/spaudinys	Spausdinimas	
	Jutiklis		
	Padangų dydis		
	Transporto priemonė/transporto priemonės blokas		
	Ypatingos būsenos		
	Nekontroliuojama		
	Kelto perkėla/geležinkelio pervažis		
	Įvairūs		
	Įvykiai		Gedimai
	Dienos darbo laikotarpio pradžia		Dienos darbo laikotarpio pabaiga
	Vieta		Rankomis įvesta informacija apie vairuotojo veiklą
	Apsauga		Greitis
	Laikas		Iš viso/suma
	Apibrėžiamieji simboliai		
	Kasdien		
	Kas savaitę		
	Dvi savaitės		
	Nuo iki		

2. PIKTOGRAMŲ DERINIAI

	Įvairūs		
	Kontrolės vieta		Dienos darbo laikotarpio pabaigos vieta
	Dienos darbo laikotarpio pradžios vieta		Iki kada
	Nuo kada		
	Iš transporto priemonės		
	Nekontroliuojamo laikotarpio pradžia		Nekontroliuojamo laikotarpio pabaiga

Kortelės

	Vairuotojo kortelė
	Įmonės kortelė
	Kontrolės kortelė
	Dirbtuvių kortelė
	Kortelės nėra

Važiavimas

	Įgula
	Vienos savaitės vairavimo trukmė
	Dviejų savaitių vairavimo trukmė

Spaudiniai

24h	Vairuotojo veiklos kasdienis spaudinys iš kortelės
24h	Vairuotojo veiklos kasdienis spaudinys iš transporto priemonės bloko
	Įvykių ir gedimų spaudinys iš kortelės
	Įvykių ir gedimų spaudinys iš transporto priemonės bloko
	Techninių duomenų spaudinys
	Greičio viršijimo spaudinys

Įvykiai

	Įkišta negaliojanti kortelė
	Kortelių nesuderinamumas
	Dalinis laiko sutapimas
	Važiavimas be reikiamos kortelės
	Kortelė įkišta važiuojant
	Paskutinė kortelės panauda netinkamai užbaigta
	Greičio viršijimas
	Maitinimo nutrūkimas
	Judesio jutiklio klaida
	Apsaugos pažeidimas
	Laiko koregavimas (dirbtuvėse)
	Greičio viršijimo kontrolė

Gedimai

	Kortelės gedimas (vairuotojo plyšys)
	Kortelės gedimas (vairuotojo porininko plyšys)
	Ekranų gedimas
	Duomenų perkėlimo gedimas
	Spausdintuvo gedimas
	Jutiklio gedimas
	TPB vidinis gedimas

Rankinio įvedimo procedūra

	Tas pats dienos darbo laikotarpis?
	Ankstesnio darbo laikotarpio pabaiga?
	Patvirtinkite arba įveskite darbo laikotarpio pabaigos vietą
	Įveskite pradžios laiką
	Įveskite darbo laikotarpio pradžios vietą

Pastaba: papildomi piktogramų deriniai, sudarantys spaudinio bloką arba įrašų žymeklius, nurodyti 4 priedėlyje.

4 priedėlis

SPAUDINIAI

TURINYS

1.	Bendri dalykai	409
2.	Duomenų blokų specifikacija	409
3.	Spaudinio specifikacijos	415
3.1.	Vairuotojo veiklos kasdienis spaudinys iš kortelės	416
3.2.	Vairuotojo veiklos kasdienis spaudinys iš transporto priemonės bloko	416
3.3.	Įvykių ir gedimų spaudinys iš kortelės	417
3.4.	Įvykių ir gedimų spaudinys iš transporto priemonės bloko	417
3.5.	Techninių duomenų spaudinys	418
3.6.	Greičio viršijimo spaudinys	418

dd/mm/yyyy hh:mm (UTC)

2. **Spaudinio rūšis**
 Bloko vardas
 Spaudinio piktogramų derinys (žr. 3 priedėlį), greičio viršijimo įtaiso nustatymas (tik greičio viršijimo spaudinyje).

-----T-----
 Picto xxx km/h

3. **Kortelės turėtojo identifikacija**
 Bloko vardas. P = žmonių piktograma
 Kortelės turėtojo pavardė
 Kortelės turėtojo vardas (-ai) (jei yra)
 Kortelės identifikacija
 Kortelės galiojimo pabaigos data (jei yra)
 Jei kortelė yra neasmeninė ir joje neįrašyta kortelės turėtojo pavardė, vietoj jos spausdinamas įmonės, dirbtuvių arba kontrolės institucijos pavadinimas.

-----P-----
 P Last_Name _____
 First_Name _____
 Card_Identification _____
 dd/mm/yyyy

4. **Transporto priemonės identifikacija**
 Bloko vardas
 (TPIN)
 Registruojančioji valstybė narė ir TPRN.

-----A-----
 A VIN _____
 Nat/VRN _____

5. **TPB identifikacija**
 Bloko vardas
 TPB gamintojo pavadinimas
 TPB komponento šifras.

-----B-----
 B VU_Manufacturer _____
 VU_Part_Number _____

6. **Tachografo paskutinio kalibravimo data**
 Bloko vardas
 Dirbtuvių pavadinimas
 Dirbtuvių kortelės identifikacija
 Kalibravimo data.

-----T-----
 T Last_Name _____
 Card_Identification _____
 T dd/mm/yyyy

7. **Paskutinė kontrolė (atlikta kontrolės pareigūno)**
 Bloko vardas
 Kontrolieriaus kortelės identifikacija
 Kontrolės data, laikas ir rūšis
 Kontrolės rūšis: iki keturių piktogramų. Kontrolės rūšį gali nurodyti tokios piktogramos (jų deriniai):
 B: duomenų perkėlimas iš kortelės, T: duomenų perkėlimas iš TPB, Tspausdinimas, B: rodymas ekrane.

-----B-----
 Card_Identification _____
 B dd/mm/yyyy hh:mm pppp

8. **Kortelės atmintyje laikoma informacija apie vairuotojo veiklą chronologine tvarka**
 Bloko vardas
 Pareikalavimo data (kalendorinė diena, kurios duomenys spausdinami) + kortelės buvimo per dieną skaitiklis

-----B-----
 dd/mm/yyyy xxx

- 8.1. *Laikotarpis, kuriuo kortelė nebuvo įkišta*
 8.1a. Įrašo vardas (laikotarpio pradžia)
 8.1b. Nežinomas laikotarpis. Pradžios ir pabaigos laikas, trukmė.
 8.1c. Rankomis įvesta informacija apie veiklą
 Veiklos rūšies piktograma, pradžios ir pabaigos laikas (imtinai), trukmė, ne trumpesni kaip vienos valandos trukmės poilsio laikotarpiai paženklinami žvaigždute.

 ? hh:mm hh:mm hh:mm
 A hh:mm hh:mm hh:mm *

- 8.2. Kortelės įkišimas į plyšį S
Įrašo vardas; S = plyšio piktograma
Transporto priemonę registruojanti valstybė narė ir TPRN
Transporto priemonės hodometro rodmens vertė įkišant kortelę.
- 8.3. Veikla (kai kortelė buvo įkišta)
Veiklos rūšies piktograma, pradžios ir pabaigos laikas (imtinai), trukmė, igulos būseną (jei ĮGULA — igulos piktograma, jei VIENAS VAIRUOTOJAS — tuščia), ne trumpesni kaip vienos valandos trukmės poilsio laikotarpiai paženklinami žvaigždute.
- 8.3a. Ypatinga būseną. Įrašo laikas, ypatingos būsenos piktograma (arba jų derinys).
- 8.4. Kortelės ištraukimas
Transporto priemonės hodometro rodmens vertė ir nuo paskutinio įkišimo, kurio metu žinoma hodometro rodmens vertė, nuvažiuotas atstumas.
9. TPB atmintyje laikoma informacija apie vairuotojo veiklą chronologine tvarka (pagal kiekvieną plyšį)
Bloko vardas
Pareikalavimo data (kalendorinė diena, kurios duomenys spausdinami)
Transporto priemonės hodometro rodmens vertė 00.00 val. ir 24.00 val.
10. Plyšyje S užregistruota veikla
Bloko vardas
- 10.1. TPB laikotarpių suvestinė nesant kortelės vairuotojo plyšyje
Įrašo vardas
Kortelė neįkišta
Transporto priemonės hodometro rodmens vertė laikotarpio pradžioje.
- 10.2. Kortelės įkišimas
Įrašo apie kortelės įkišimą vardas
Vairuotojo pavardė
Vairuotojo vardas
Vairuotojo kortelės identifikacija
Vairuotojo kortelės galiojimo pabaigos data
Anksčiau naudotos transporto priemonės registruojančioji valstybė narė ir TPRN
Kortelės ištraukimo iš ankstesnės transporto priemonės data ir laikas
Tuščia eilutė
Transporto priemonės hodometro rodmens vertė įkišant kortelę, rankomis įvestos informacijos apie vairuotojo veiklą žymuo (jei buvo įvesta — M, jei ne — tuščia).
- 10.3. Veikla
Veiklos rūšies piktograma, pradžios ir pabaigos laikas (imtinai), trukmė, igulos būseną (jei ĮGULA — igulos piktograma, jei VIENAS VAIRUOTOJAS — tuščia), ne trumpesni kaip vienos valandos trukmės poilsio laikotarpiai paženklinami žvaigždute.

-----S-----
A Nat/VRN _____
x xxx xxx km

A hh:mm hh:mm hh:mm ☐☐ *

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 hh:mm ☐☐ *

- 10.3a. *Ypatinga būseną. Įrašo laikas, ypatingos būsenos piktograma (arba jų derinys).*
- hh:mm ----- pppp -----
- 10.4. *Kortelės ištraukimas arba laikotarpio „kortelė neįkišta“ pabaiga*
Transporto priemonės hodometro rodmens vertė ištraukiant kortelę arba pasibaigus laikotarpiui „kortelė neįkišta“ ir nuo kortelės įkišimo momento arba nuo laikotarpio „kortelė neįkišta“ pradžios nuvažiuotas atstumas.
- x xxx xxx km; x xxx km
11. **Dienos suvestinė**
Bloko vardas
- Σ -----
- 11.1. *TPB laikotarpių suvestinė nesant kortelės vairuotojo plyšyje*
Bloko vardas.
- 1 000 - - -
- 11.2. *TPB laikotarpių suvestinė nesant kortelės vairuotojo porininko plyšyje*
Bloko vardas.
- 2 000 - - -
- 11.3. *TPB dienos suvestinė apie kiekvieną vairuotoją*
Įrašo vardas
Vairuotojo pavardė
Vairuotojo vardas (-ai)
Vairuotojo kortelės identifikacija.
- Last_Name _____
 First_Name _____
 Card_Identification _____
- 11.4. *Įrašas apie vietą, kurioje prasideda ir (arba) baigiasi dienos darbo laikotarpis*
pi = pradžios (pabaigos) vietos piktograma, laikas, šalis, regionas
Hodometro rodmens vertė.
- pihh:mm Cou Reg
x xxx xxx km
- 11.5. *Veiklos suvestiniai duomenys (iš kortelės)*
Bendra vairavimo trukmė, nuvažiuotas atstumas
Bendra darbo ir buvimo pasirengus dirbti trukmė
Bendra poilsio ir nežinomų laikotarpių trukmė
Bendra įgulos veiklos trukmė.
- hh:mm x xxx km
 hh:mm hh:mm
 hh:mm ? hh:mm
 hh:mm
- 11.6. *Veiklos suvestiniai duomenys (laikotarpiai, kai vairuotojo plyšyje nebuvo kortelės)*
Bendra vairavimo trukmė, nuvažiuotas atstumas
Bendra darbo ir buvimo pasirengus dirbti trukmė
Bendra poilsio trukmė.
- hh:mm x xxx km
 hh:mm hh:mm
 hh:mm
- 11.7. *Veiklos suvestiniai duomenys (laikotarpiai, kai vairuotojo porininko plyšyje nebuvo kortelės)*
Bendra darbo ir buvimo pasirengus dirbti trukmė
Bendra poilsio trukmė.
- hh:mm hh:mm
 hh:mm

- 11.8. Veiklos suvestiniai duomenys (vieno vairuotojo; abu plyšiai)
Bendra vairavimo trukmė, nuvažiuotas atstumas
Bendra vairavimo trukmė, nuvažiuotas atstumas
Bendra poilsio trukmė
Bendra įgulos veiklos trukmė
Kai reikia išspausdinti spaudinį apie esamą dieną, suvestiniai duomenys apskaičiuojami pagal tuo metu turimą informaciją.

Ⓢ hh:mm x xxx km
Ⓢ hh:mm Ⓢ hh:mm
Ⓢ hh:mm
Ⓢ hh:mm

12. Kortelės atmintyje laikoma informacija apie įvykius ir (arba) gedimus

- 12.1. 5 paskutinių „įvykių ir gedimų“ iš kortelės bloko vardas

----- ! x Ⓢ -----

- 12.2. Visų užregistruotų kortelėje „įvykių“ bloko vardas

----- ! Ⓢ -----

- 12.3. Visų užregistruotų kortelėje „gedimų“ bloko vardas

----- x Ⓢ -----

- 12.4. Įrašas apie vykį ir (arba) gedimą
Įrašo vardas
Įvykio (gedimo) piktograma, įrašo tikslas, pradžios data ir laikas
Papildomas įvykio (gedimo) kodas (jei yra), trukmė
Transporto priemonės, kurioje įvyko įvykis arba gedimas, registruojančioji valstybė narė ir TPRN.

Pic dd/mm/yyyy hh:mm
! xxx hh:mm
Ⓢ Nat/VRN _____

13. TPB atmintyje laikoma informacija apie įvykius ir gedimus arba jame vykstantys įvykiai ir gedimai

- 13.1. 5 paskutinių „įvykių ir gedimų“ iš TPB bloko vardas

----- ! x Ⓢ -----

- 13.2. Visų užregistruotų TPB „įvykių“ bloko vardas

----- ! Ⓢ -----

- 13.3. Visų užregistruotų TPB „gedimų“ bloko vardas

----- x Ⓢ -----

- 13.4. Įrašas apie vykį ir (arba) gedimą
Įrašo vardas
Įvykio (gedimo) piktograma, įrašo tikslas, pradžios data ir laikas
Papildomas įvykio (gedimo) kodas (jei yra), panašių įvykių tą dieną skaičius, trukmė
Įvykio arba gedimo pradžios arba pabaigos momentu įkištų kortelių identifikacija (iki 4 eilučių, dukart nekartoiant vienos kortelės numerio)
Atvejais, kai kortelė nebuvo įkišta
Įrašo tikslas (p) — tai skaitmeninis kodas, paaiškinantis, kodėl įvykis arba gedimas buvo užregistruotas. Koduojama pagal duomenų elementą EventFaultRecordPurpose.

Pic (p) dd/mm/yyyy hh:mm
! xxx (xxx) hh:mm
Card_Identification _____
Card_Identification _____
Card_Identification _____
Card_Identification _____
Ⓢ ---

14. **TPB identifikacija**

Bloko vardas
 TPB gamintojo pavadinimas
 TPB gamintojo adresas
 TPB komponento šifras
 TPB patvirtinimo numeris
 TPB serijos numeris
 TPB pagaminimo metai
 TPB programinės įrangos versija ir įdiegimo data.

-----B-----
 B Name _____
 Address _____
 PartNumber _____
 Apprv _____
 S/N _____
 yyyy
 V xx.xx.xx dd/mm/yyyy

15. **Jutiklio identifikacija**

Bloko vardas
 Jutiklio serijos numeris
 Jutiklio patvirtinimo numeris
 Jutiklio pirmojo įrengimo data.

-----L-----
 L S/N _____
 Apprv _____
 dd/mm/yyyy

16. **Kalibravimo duomenys**

Bloko vardas

-----T-----

16.1. *Įrašas apie kalibravimą*

Įrašo vardas
 Kalibravimą atlikusios dirbtuvės
 Dirbtuvių adresas
 Dirbtuvių kortelės identifikacija
 Dirbtuvių kortelės galiojimo pabaigos data
 Tuščia eilutė
 Kalibravimo data ir tikslas
 TPIN
 Registruojančioji valstybė narė ir TPRN
 Transporto priemonės būdingasis koeficientas
 Tachografo konstanta
 Ratų padangų efektyvusis apskritimo ilgis
 Sumontuotų padangų dydis
 Greičio ribotuvo nustatymas
 Senoji ir naujoji hodometro rodmenų vertės
 Įrašo tikslas (p) – tai skaitmeninis kodas, paaiškinantis, kodėl
 šie kalibravimo parametrai buvo užregistruoti. Koduojama
 pagal duomenų elementą CalibrationPurpose.

 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
 e TyreSize _____
 > xxx km/h
 x xxx xxx – x xxx xxx km

17. **Laiko koregavimas**

Bloko vardas.

-----C-----

17.1. *Įrašas apie laiko koregavimą*

Įrašo vardas
 Senoji data ir laikas
 Naujoji data ir laikas
 Laiko koregavimą atlikusios dirbtuvės
 Dirbtuvių adresas
 Dirbtuvių kortelės identifikacija
 Dirbtuvių kortelės galiojimo pabaigos data.

 ! C dd/mm/yyyy hh:mm
 C dd/mm/yyyy hh:mm
 T Workshop_name _____
 Workshop_address _____
 Card-Identification _____
 dd/mm/yyyy

18. Vėliausias TPB atmintyje užregistruotas įvykis ir gedimas

Bloko vardas

Paskutinio įvykio data ir laikas

Paskutinio gedimo data ir laikas.

```
----- !x A -----
!  jj/mm/aaaa  hh:mm
x  jj/mm/aaaa  hh:mm
```

19. **Greičio viršijimo kontrolės informacija**

Bloko vardas

Paskutinės GREIČIO VIRŠIJIMO KONTROLĖS data ir laikas

Pirmojo greičio viršijimo data ir laikas ir greičio viršijimo įvykiu skaičius nuo tada.

```

----->>-----
> dd/mm/yyyy hh:mm
>> dd/mm/yyyy hh:mm (nnn)

```

20. Įrašas apie greičio viršijimą

20.1. Bloko vardas „Pirmasis greičio viršijimas po paskutinio kalibravimo“

----- >>↑ -----

20.2. Bloko vardas „5 rimčiausi per pastarąsias 365 dienas“

----- >> (365) -----

20.3. Bloko vardas „Rimčiausi per kiekvieną iš pastarųjų 10 dienų“

----- >>(10) -----

20.4. Įrašo vardas

Data, laikas ir trukmė

Didžiausias ir vidutinis greitis, panašių įvykių tą dieną skaičius

Vairuotojo pavardė

Vairuotojo vardas (-ai)

Vairuotojo kortelės identifikacija

```

-----
>> dd/mm/yyyy hh:mm hh:mm
    xxx km/h xxx km/h (xxx)

```

Last_Name _____
 First_Name _____
 Card_Identification _____

20.5. Jei bloke nėra įrašų apie greičio viršijimą.

>>> - - -

21. **Ranka rašoma informacija**

Bloko vardas

21.1. Kontrolēs vieta

21.2. Kontrolieriaus parašas

21.3. Nuo kada

21.4. Iki kada

21.5. Vairuotojo parašas

□ +
 □
 ⊗ +
 + ⊗
 ⊙

„Ranka rašoma informacija“ — ėterpiama pakankamai tuščių eilučių virš ranka įrašomo punkto, kad būtų įmanoma įrašyti reikiamą informaciją arba pasirašyti.

3. SPAUDINIO SPECIFIKACIJOS

Šiame skyriuje naudotos tokios sąlyginio žymėjimo priemonės:

N
N
X/Y

Išspausdinti bloką arba įrašą N.

Išspausdinti bloką arba įrašą N tiek kartų, kiek reikia.

Išspausdinti reikiamus blokus arba įrašus X ir (arba) Y tiek kartų, kiek reikia.

3.1. Vairuotojo veiklos kasdienis spaudinys iš kortelės

PRT_007 Vairuotojo veiklos kasdienis spaudinys iš kortelės turi būti tokio formato:

1	Dokumento spausdinimo data ir laikas
2	Spaudinio rūšis
3	Vairuotojo identifikacija (iš kortelės, iš kurios spausdinama)
4	Transporto priemonės identifikacija (transporto priemonė, iš kurios spausdinami duomenys)
5	TPB identifikacija (TPB, iš kurio spausdinami duomenys)
6	Šio TPB paskutinis kalibravimas
7	Paskutinė tikrinamo vairuotojo kontrolė
8	Vairuotojo veiklos ribotuvai
8.1a / 8.1b / 8.1c / 8.2 / 8.3 / 8.3a / 8.4	Vairuotojo veikla chronologine tvarka
11	Dienos suvestinės ribotuvai
11.4	Įvestos vietos chronologine tvarka
11.5	Veiklos suvestinės
12.1	Įvykių arba gedimų iš kortelės ribotuvai
12.4	Įrašai apie įvykius (gedimus) (kortelės atmintyje laikoma informacija apie paskutinius 5 įvykius ar gedimus)
13.1	Įvykių arba gedimų iš TPB ribotuvai
13.4	Įrašai apie įvykius (gedimus) (TPB atmintyje laikoma informacija apie paskutinius 5 įvykius ar gedimus arba jame vykstančius įvykius ar gedimus)
21.1	Kontrolės vieta
21.2	Kontrolieriaus parašas
21.5	Vairuotojo parašas

3.2. Vairuotojo veiklos kasdienis spaudinys iš transporto priemonės bloko

PRT_008 Vairuotojo veiklos kasdienis spaudinys iš transporto priemonės bloko turi būti tokio formato:

1	Dokumento spausdinimo data ir laikas
2	Spaudinio rūšis
3	Kortelės turėtojo identifikacija (visų į TPB įkištų kortelių)
4	Transporto priemonės identifikacija (transporto priemonė, iš kurios spausdinami duomenys)
5	TPB identifikacija (TPB, iš kurio spausdinami duomenys)
6	Šio TPB paskutinis kalibravimas
7	Šio tachografo paskutinė kontrolė
9	Vairuotojo veiklos ribotuvai
10	Vairuotojo plyšio ribotuvai (1 plyšys)
10.1 / 10.2 / 10.3 / 10.3a / 10.4	Veikla chronologine tvarka (vairuotojo plyšys)
10	Vairuotojo porininko plyšio ribotuvai (2 plyšys)
10.1 / 10.2 / 10.3 / 10.3a / 10.4	Veikla chronologine tvarka (vairuotojo porininko plyšys)
11	Dienos suvestinės ribotuvai
11.1	Laikotarpiai, kai vairuotojo plyšyje nebuvo kortelės, suvestinė
11.4	Įvestos vietos chronologine tvarka
11.6	Veiklos suvestinės

11.2	Laikotarpį, kai vairuotojo porininko plyšyje nebuvo kortelės, suvestinė
11.4	Įvestos vietos chronologine tvarka
11.7	Veiklos suvestinės
11.3	Vairuotojo veiklos pagal abu plyšius suvestinė
11.4	Vairuotojo įvestos vietos chronologine tvarka
11.7	Vairuotojo veiklos suvestinė
13.1	Įvykių arba gedimų iš kortelės ribotuvas
13.4	Įrašai apie įvykius (gedimus) (TPB atmintyje laikoma informacija apie paskutinius 5 įvykius ar gedimus arba jame vykstančius įvykius ar esamus gedimus)
21.1	Kontrolės vieta
21.2	Kontrolieriaus parašas
21.3	Nuo kada
21.4	Iki kada
21.5	Vairuotojo parašas

(vieta, kurioje kortelės neturintis vairuotojas gali nurodyti, kurie laikotarpiai yra taikytini jam pačiam)

3.3. Įvykių ir gedimų spaudinys iš kortelės

PRT_009 Įvykių ir gedimų spaudinys iš kortelės turi būti tokio formato:

1	Dokumento spausdinimo data ir laikas
2	Spaudinio rūšis
3	Kontrolieriaus identifikacija (jei į TPB įkišta kontrolės kortelė)
3	Vairuotojo identifikacija (iš kortelės, iš kurios spausdinama)
4	Transporto priemonės identifikacija (transporto priemonė, iš kurios spausdinami duomenys)
12.2	Įvykių ribotuvas
12.4	Įrašai apie įvykius (kortelės atmintyje laikoma informacija apie visus įvykius)
12.3	Gedimų ribotuvas
12.4	Įrašai apie gedimus (kortelės atmintyje laikoma informacija apie visus gedimus)
21.1	Kontrolės vieta
21.2	Kontrolieriaus parašas
21.5	Vairuotojo parašas

3.4. Įvykių ir gedimų spaudinys iš transporto priemonės bloko

PRT_010 Įvykių ir gedimų spaudinys iš transporto priemonės bloko turi būti tokio formato:

1	Dokumento spausdinimo data ir laikas
2	Spaudinio rūšis
3	Kontrolieriaus identifikacija (jei į TPB įkišta kontrolės kortelė)
4	Transporto priemonės identifikacija (transporto priemonė, iš kurios spausdinami duomenys)
13.2	Įvykių ribotuvas
13.4	Įrašai apie įvykius (TPB atmintyje laikoma informacija apie visus įvykius arba jame vykstantys įvykiai)
13.3	Gedimų ribotuvas
13.4	Įrašai apie gedimus (TPB atmintyje laikoma informacija apie visus gedimus arba jame esami gedimai)
21.1	Kontrolės vieta
21.2	Kontrolieriaus parašas
21.5	Vairuotojo parašas

3.5. Techninių duomenų spaudinys

PRT_011 Techninių duomenų spaudinys turi būti tokio formato:

1	Dokumento spausdinimo data ir laikas
2	Spaudinio rūšis
3	Kortelės turėtojo identifikacija (visų į TPB įkištų kortelių)
4	Transporto priemonės identifikacija (transporto priemonė, iš kurios spausdinami duomenys)
14	TPB identifikacija
15	Jutiklio identifikacija
16	Kalibravimo datos ribotuvai
16.1	Įrašai apie kalibravimą (visi turimi įrašai chronologine tvarka)
17	Laiko koregavimo ribotuvai
17.1	Įrašai apie laiko koregavimą (visi turimi įrašai iš duomenų apie laiko koregavimą ir kalibravimą)
18	Paskutinis TPB atmintyje įrašytas įvykis ir gedimas

3.6. Greičio viršijimo spaudinys

PRT_012 Greičio viršijimo spaudinys turi būti tokio formato:

1	Dokumento spausdinimo data ir laikas
2	Spaudinio rūšis
3	Kortelės turėtojo identifikacija (visų į TPB įkištų kortelių)
4	Transporto priemonės identifikacija (transporto priemonė, iš kurios spausdinami duomenys)
19	Greičio viršijimo kontrolės informacija
20.1	Greičio viršijimo datos vardas
20.4 / 20.5	Pirmasis greičio viršijimas po paskutinio kalibravimo
20.2	Greičio viršijimo datos vardas
20.4 / 20.5	5 rimčiausi greičio viršijimai per pastarąsias 365 dienas
20.3	Greičio viršijimo datos vardas
20.4 / 20.5	Rimčiausias greičio viršijimas kiekvieną iš paskutinių 10 dienų
21.1	Kontrolės vieta
21.2	Kontrolieriaus parašas
21.5	Vairuotojo parašas

5 priedėlis

EKRANAS

Šiame priedėlyje naudotos tokios formato sąlyginio žymėjimo priemonės:

- juodu šriftu išspausdinti rašmenys reiškia spausdinamą tekstą (tekstas spausdinamas įprastu šriftu),
- įprastu šriftu išspausdinti rašmenys žymi kintamuosius (piktogramas arba duomenis), vietoj kurių spausdinamos jų vertės:

dd mm yyyy: diena, mėnuo, metai,
 hh: valandos,
 mm: minutės,
 D: trukmės piktograma,
 EF: įvykių arba gedimų piktogramų derinys,
 O: darbo režimo piktograma.

DIS_001 Tachografas turi rodyti duomenis tokiais formatais:

Data	Format
Numatytasis rodinys	
Vietos laikas	hh:mm
Darbo režimas	O
Su vairuotoju susijusi informacija	1 Dhhmm hhmm
Su vairuotoju porininku susijusi informacija	2 Dhhmm
Prasidėjo nekontroliuojama būsena	OUT
Perspėjamasis rodinys	
Viršyta nepertraukiamo vairavimo trukmė	1 0hhmm hhmm
Įvykis arba gedimas	EF
Kiti rodiniai	
UTC laikas	UTC 0dd/mm/yyyy laikas
arba	UTC 0dd.mm.yyyy hh:mm
Vairuotojo nepertraukiamo vairavimo trukmė ir bendroji poilsio trukmė	1 0hhmm hhmm
Vairuotojo porininko nepertraukiamo vairavimo trukmė ir bendroji poilsio trukmė	2 0hhmm hhmm
Ankstesnės ir esamos savaitės vairuotojo bendroji vairavimo trukmė	1 0 hhhhmm
Ankstesnės ir esamos savaitės vairuotojo porininko bendroji vairavimo trukmė	2 0 hhhhmm

6 priedėlis

IŠORINĖS SĄSAJOS

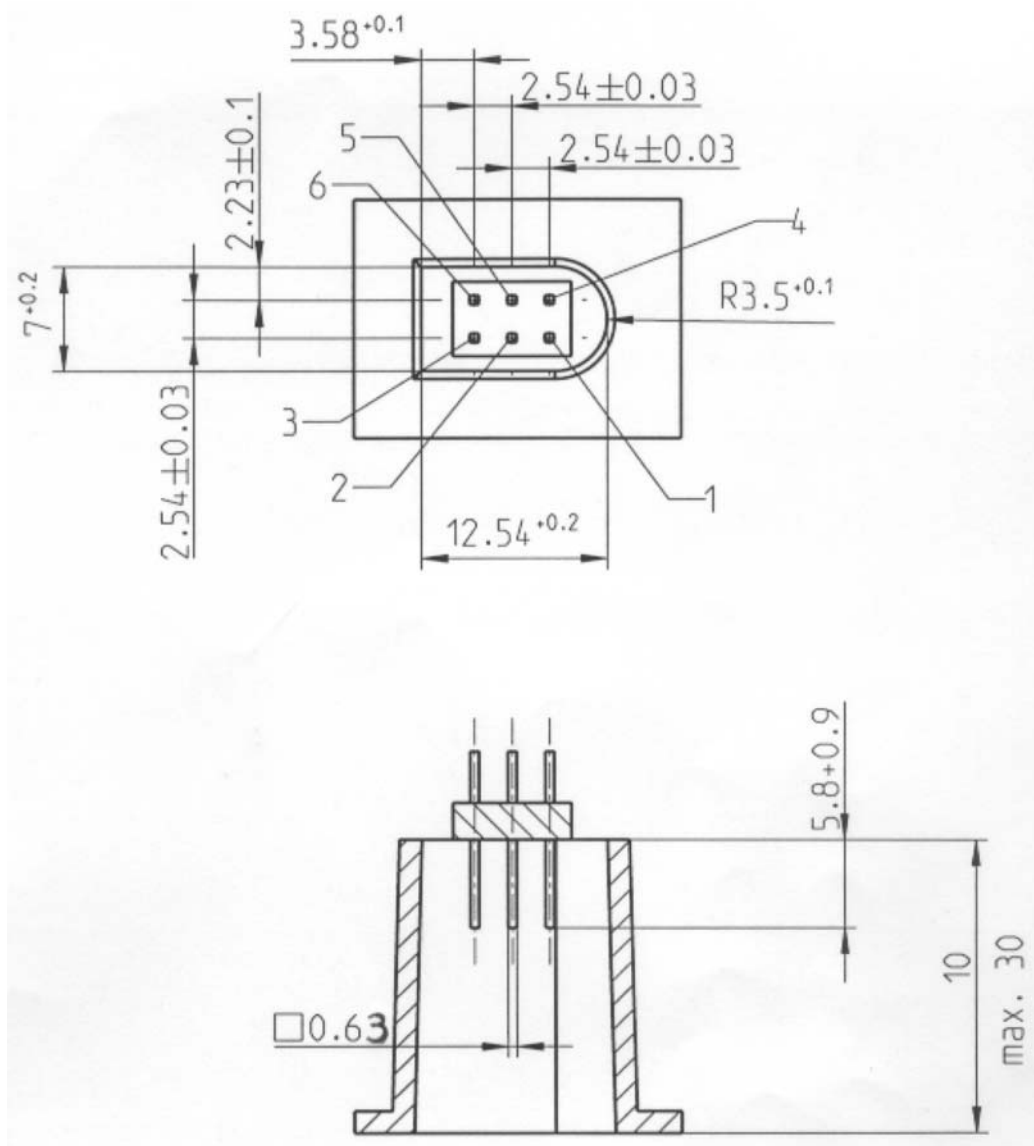
TURINYS

1.	Techninė įranga	422
1.1.	Jungtis	422
1.2.	Kontaktų paskirstymas	424
1.3.	Schema	424
2.	Duomenų perkėlimo sąsaja	424
3.	Kalibravimo sąsaja	425

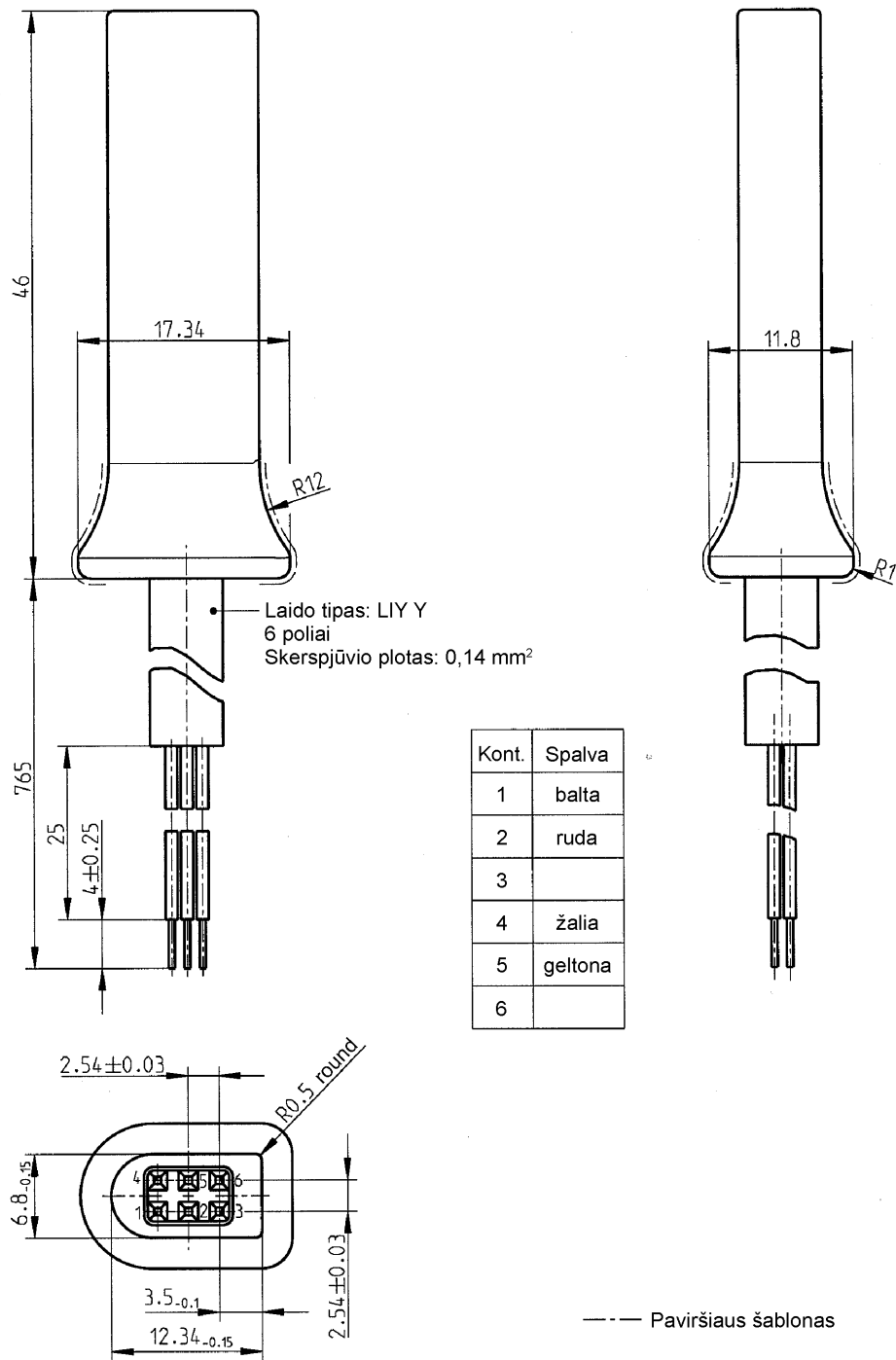
1. TECHNINĖ ĮRANGA

1.1. Jungtis

INT_001 Duomenų perkėlimo-kalibravimo jungtis turi būti šešių kontaktų, prieinama priekinėje plokštelėje neatjungiant nė vienos tachografo dalies ir atitinkanti toliau pateiktą brėžinį (visi matmenys nurodyti milimetrais):



Šiame brėžinyje pavaizduotas standartinis šešių kontaktų kištukas:



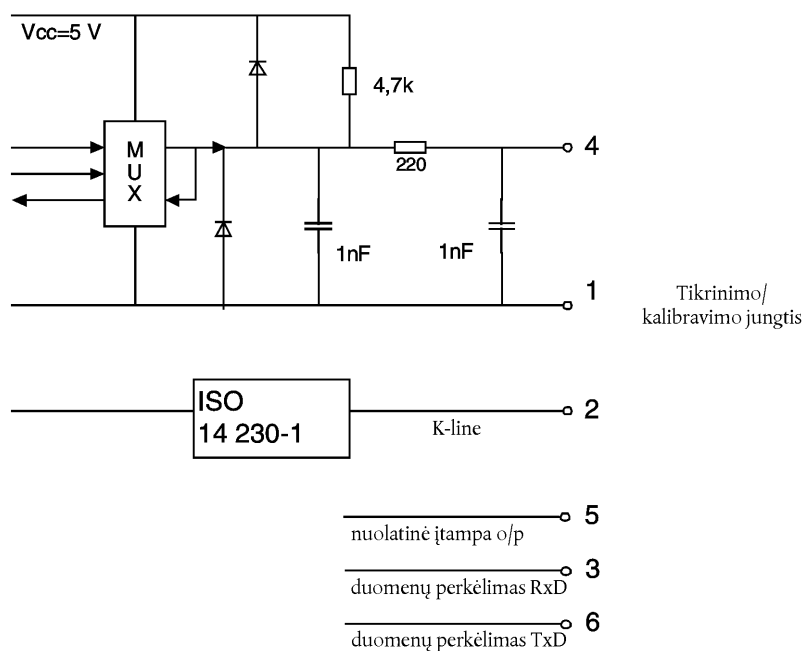
1.2. Kontaktų paskirstymas

INT_002 Kontaktai turi būti paskirstyti kaip nurodyta lentelėje:

Kontaktas	Aprašymas	Pastaba
1	Akumulatoriaus neigiamas polius	Sujungtas su transporto priemonės akumulatoriaus neigiamu poliumi
2	Duomenų perdavimas	K linija (ISO 14 230-1)
3	RxD – duomenų perkėlimas	Duomenų įvedimas į tachografą
4	Įvesties ir išvesties signalas	Kalibravimas
5	Nuolatinis stiprus išvesties signalas	Įtampa turi būti lygi transporto priemonės įtampai, sumažintai 3 V, įvertinant įtampos kritimą apsauginiame grandyne. Išvesties signalo srovės stipris: 40 mA
6	TxD – duomenų perkėlimas	Duomenų išvedimas iš tachografo

1.3. Schema

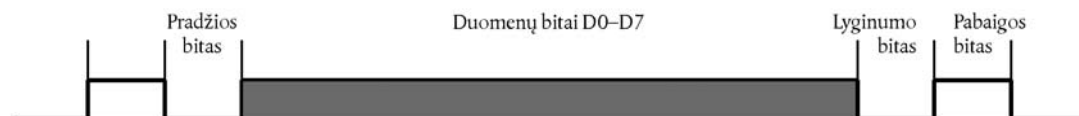
INT_003 Schema turi būti tokia:



2. DUOMENŲ PERKĖLIMO SĄSAJA

INT_004 Duomenų perkėlimo sąsaja turi atitikti specifikaciją RS232.

INT_005 Duomenų perkėlimo sąsaja turi naudoti vieną pradžios bitą, 8 duomenų bitus su LSB bitu pradžioje, vieną lyginumo patikros bitą ir vieną pabaigos bitą.



Duomenų baito struktūra

Pradžios bitas: vienas loginio lygio 0 bitas

Duomenų bitai: siunčiami su vienu LSB bitu pradžioje

Lyginumo bitas: lyginumo patikra

Pabaigos bitas: pabaigos loginio lygio 1 bitas

Kai siunčiami skaitmeniniai duomenys, kuriuos sudaro daugiau kaip vienas baitas, pats svarbiausias baitas siunčiamas pirmasis, o mažiausiai svarbus – paskutinis.

INT_006 Siuntimo spartą turi būti galima reguliuoti nuo 9 600 bps iki 115 200 bps. Turi būti siunčiama pačia didžiausia įmanoma sparta, o pradinė sparta pradedant perduoti duomenis turi būti nustatyta ties 9 600 bps.

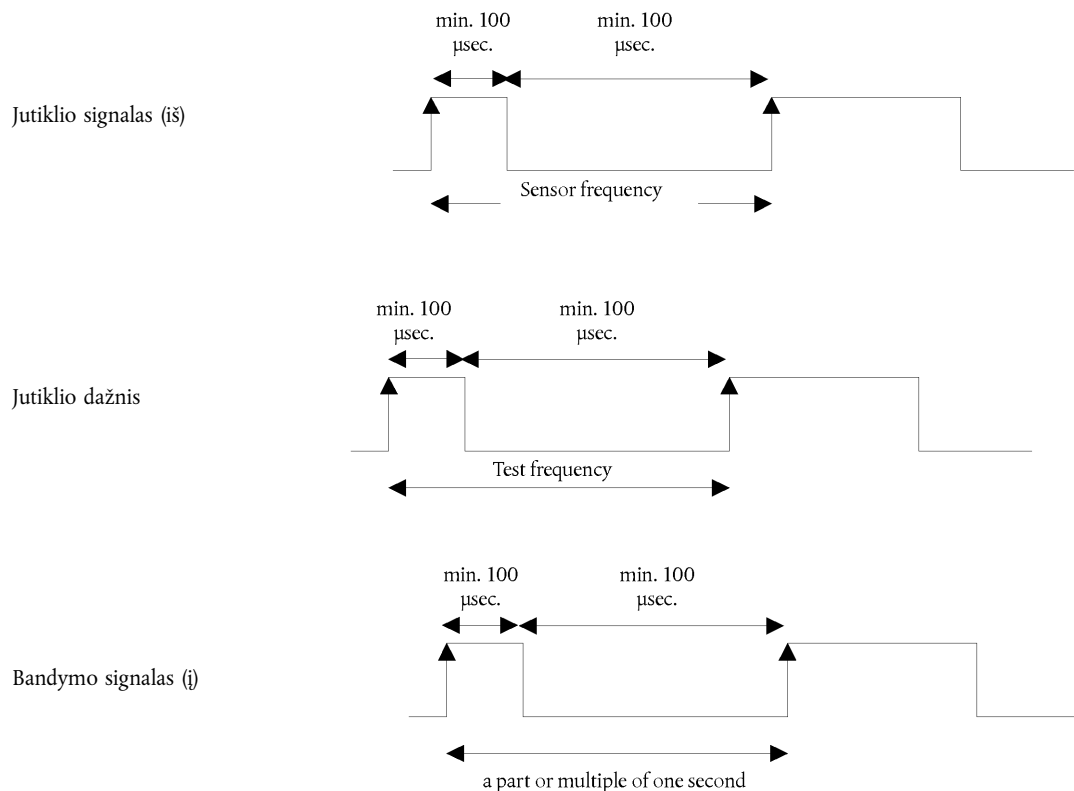
3. KALIBRAVIMO SĄSAJA

INT_007 Duomenys turi būti perduodami pagal ISO 14 230-1 „Kelių transporto priemonės. Diagnostikos sistemos. Raktažodžių protokolas 2000. 1 dalis. Fizinis sluoksnis“. Pirmasis leidimas, 1999 m.

INT_008 Įvesties ir išvesties signalas turi atitikti tokią elektros specifikaciją:

Parametras	Mažiausia vertė	Įprasta vertė	Didžiausia vertė	Pastaba
$U_{\text{žema}} (i)$			1,0 V	$I = 750 \mu\text{A}$
$U_{\text{aukšta}} (i)$	4 V			$I = 200 \mu\text{A}$
Dažnis			4 kHz	
$U_{\text{žema}} (i)$			1,0 V	$I = 1 \text{ mA}$
$U_{\text{aukšta}} (iš)$	4 V			$I = 1 \text{ mA}$

INT_009 Įvesties ir išvesties signalas turi atitikti tokią laiko schemą:



7 priedėlis

DUOMENŲ PERKĖLIMO PROTOKOLAI

TURINYS

1.	Įvadas	428
1.1.	Taikymo sritis	428
1.2.	Santrumpos ir žymenys	428
2.	Duomenų perkėlimas iš TPB	429
2.1.	Duomenų perkėlimo procedūra	429
2.2.	Duomenų perkėlimo protokolai	429
2.2.1.	Pranešimų struktūra	429
2.2.2.	Pranešimų rūšys	430
2.2.2.1.	Start communication request [pareikalavimas pradėti ryšį] (SID 81)	432
2.2.2.2.	Positive response start communication [teigiamas atsakymas į pareikalavimą pradėti ryšį] (SID C1)	432
2.2.2.3.	Start diagnostic session request [pareikalavimas pradėti diagnostikos seansą] (SID 10)	432
2.2.2.4.	Positive response start diagnostic [teigiamas atsakymas į pareikalavimą pradėti diagnostikos seansą] (SID 50)	432
2.2.2.5.	Link control service [ryšio kanalo valdymo paslaugos pareikalavimas] (SID 87)	432
2.2.2.6.	Link control positive response [teigiamas atsakymas į pareikalavimą suteikti ryšio kanalo valdymo paslaugą] (SID C7)	432
2.2.2.7.	Request upload [duomenų nusiuntimo pareikalavimas] (SID 35)	432
2.2.2.8.	Positive response request upload [teigiamas atsakymas į nusiuntimo pareikalavimą] (SID 75)	432
2.2.2.9.	Transfer data request [duomenų perdavimo pareikalavimas] (SID 36)	432
2.2.2.10.	Positive response transfer data [teigiamas atsakymas į duomenų perdavimo pareikalavimą] (SID 76)	433
2.2.2.11.	Transfer exit request [pareikalavimas nutraukti siuntimą] (SID 37)	433
2.2.2.12.	Positive response request transfer exit [teigiamas atsakymas į pareikalavimą nutraukti siuntimą] (SID 77)	433
2.2.2.13.	Stop communication [pareikalavimas nutraukti ryšį] (SID 82)	433
2.2.2.14.	Positive response stop communication [teigiamas atsakymas į pareikalavimą nutraukti ryšį] (SID C2)	433
2.2.2.15.	Acknowledge submessage [popranešimo patvirtinimas] (SID C2)	433
2.2.2.16.	Negative response [neigiamas atsakymas] (SID 7F)	433
2.2.3.	Pranešimų srautas	434
2.2.4.	Sinchronizavimas	435
2.2.5.	Klaidų valdymas	435
2.2.5.1.	Ryšio pradžios etapas	435
2.2.5.2.	Ryšio etapas	435
2.2.6.	Atsakymo pranešimo turinys	438
2.2.6.1.	Positive response transfer data overview [teigiamas atsakymas į duomenų perdavimo pareikalavimą: apžvalga]	438
2.2.6.2.	Positive response transfer data activities [teigiamas atsakymas į duomenų perdavimo pareikalavimą: veiklos rūšys]	439
2.2.6.3.	Positive response transfer data events and faults [teigiamas atsakymas į duomenų perdavimo pareikalavimą: įvykiai ir gedimai]	440

2.2.6.4.	Positive response transfer data detailed speed [teigiamas atsakymas į duomenų perdavimo pareikala- vimą: išsami informacija apie greitį]	441
2.2.6.5.	Positive response transfer data technical data [teigiamas atsakymas į duomenų perdavimo pareikala- vimą: techniniai duomenys]	441
2.3.	ESM rinkmenų laikymas	442
3.	Duomenų perkėlimo iš tachografo kortelių protokolas	442
3.1.	Taikymo sritis	442
3.2.	Apibrėžimai	442
3.3.	Duomenų perkėlimas iš kortelės	442
3.3.1.	Inicijavimo seka	443
3.3.2.	Duomenų rinkmenų be parašo seka	443
3.3.3.	Duomenų rinkmenų be parašo seka	443
3.3.4.	Kalibravimo skaitiklio grąžinimo į nulį seka	444
3.4.	Duomenų įrašymo formatas	444
3.4.1.	Įvadas	444
3.4.2.	Rinkmenų formatas	444
4.	Duomenų perkėlimas iš tachografo kortelės per transporto priemonės bloką	445

1. ĮVADAS

Šiame priedėlyje nurodytos procedūros, pagal kurias duomenys įvairiais būdais perkeliami į išorines laikmenas, ir protokolai, kuriuos reikia naudoti, kad duomenys būtų perduodami teisingai ir perkeltų duomenų formatas būtų visiškai suderintas, kad kontrolierius galėtų juos patikrinti ir prieš analizuodamas nustatyti jų autentiškumą ir nepažeistumą.

1.1. Taikymo sritis

Duomenys gali būti perkelti į ESM:

- iš transporto priemonės bloko: specializuota įranga su mikroprocesoriumi (IDE), sujungta su TPB,
- iš tachografo kortelės: IDE, sujungta su kortelės sąsajos įtaisu (IFD),
- iš tachografo kortelės: per transporto priemonės bloką, IDE, sujungta su TPB.

Tam, kad būtų galimybė patikrinti į ESM rašomų perkeltų duomenų autentiškumą ir nepažeistumą, duomenys perkeliama su pridėtu parašu laikantis 11 priedėlio „Bendrieji apsaugos mechanizmai“ nuostatų. Taip pat perkeliama šaltinio įrangos (TPB arba kortelės) identifikacijos ir apsaugos pažymėjimai (valstybės narės ir įrangos). Duomenų tikrintojas turi pats turėti patikimą europinį atvirąjį raktą.

DDP_001 Vienos duomenų perkėlimo panaudos metu perkelti duomenys turi būti laikomi vienoje ESM rinkmenoje.

1.2. Santrumpos ir žymenys

Šiame priedėlyje naudojamos tokios santrumpos:

AID	taikomosios programos vardas;
ATR	atsakymas į perkrovimą;
CS	kontrolinės sumos baitas;
DF	paskirtoji rinkmena;
DS_	diagnostikos seansas;
EF	elementarioji rinkmena;
ESM	išorinė laikmena;
FID	rinkmenos vardas (rinkmenos ID);
FMT	formato baitas (pirmasis pranešimo antraštės baitas);
ICC	kortelė su integriniu grandynu;
IDE	specializuota įranga su mikroprocesoriumi: įranga, naudojama duomenų perkėlimui į ESM (pvz., asmeninis kompiuteris);
IFD	sąsajos įtaisas;
KWP	raktažodžių protokolas 2000;
LEN	ilgio baitas (paskutinis pranešimo antraštės baitas);
PPS	protokolo parametro pasirinkimas;
PSO	atlikti apsaugos operaciją;
SID	paslaugos vardas;
SRC	šaltinio baitas;
TGT	tikslinis baitas;
TLV	žymenos ilgio vertė;
TREP	transporto priemonės blokas;
TRTP	perdavimo atsakymo parametras;
VU	perdavimo pareikalavimo parametras.

2. DUOMENŲ PERKĖLIMAS IŠ TPB

2.1. Duomenų perkėlimo procedūra

Norėdamas perkelti duomenis iš TPB, operatorius turi atlikti tokius veiksmus:

- įkišti savo tachografo kortelę į TPB plyšį kortelei ⁽¹⁾,
- prijungti IDE prie TPB duomenų perkėlimo jungties,
- užmegzti ryšį tarp IDE ir TPB,
- IDE pasirinkti reikiamus perkelti duomenis ir nusiųsti pareikalavimą į TPB,
- užbaigti duomenų perkėlimo seansą.

2.2. Duomenų perkėlimo protokolas

Protokolas sudarytas pagal schemą „vadovas – pavaldinys“, kai IDE vaidina vadovo, o TPB – pavaldinio vaidmenį.

Pranešimų struktūra, rūšys ir srutai iš daugiausia remiasi Raktažodžių protokolu 2000 (KWP) (ISO 14230-2 „Kelių transporto priemonės. Diagnostikos sistemos. Raktažodžių protokolas 2000. 2 dalis. Duomenų perdavimo kanalo sluoksnis“).

Programos sluoksnis daugiausia remiasi naujausiu ISO 14229-1 projektu („Kelių transporto priemonės. Diagnostikos sistemos. 1 dalis. Diagnostikos paslaugos“. 2001 m. vasario 22 d., 6 versija).

2.2.1. Pranešimų struktūra

DDP_002 Visi pranešimai, kuriais keičiasi IDE ir TPB yra struktūros, kurią sudaro trys dalys:

- antraštė, kurią sudaro formato baitas (FMT), tikslinis baitas (TGT), šaltinio baitas (SRC) ir neprivalomas ilgio baitas (LEN),
- duomenų laukelis, kurį sudaro paslaugos vardo baitas (SID) ir įvairus duomenų baitų skaičius, tarp kurių gali būti diagnostikos seanso baitas (DS_) arba neprivalomas perdavimo parametrų baitas (TRTP arba TREP),
- kontrolinė suma, kurią sudaro kontrolinės sumos baitas (CS).

Antraštė				Duomenų laukelis					Kontrolinė suma
FMT	TGT	SRC	LEN	SID	ADAT	...	...	...	CS
4 baitai				daugiausia 255 baitai					1 baitas

TGT ir SRC baitai žymi pranešimo gavėjo ir siuntėjo fizinį adresą. IDE vertės yra F0 Hex, o TPB — EE Hex.

LEN baitas nurodo duomenų laukelio ilgį.

Kontrolinės sumos baitas yra 8 bitų modulio 256 visų pranešimo baitų, išskyrus pačią CS, sumos serija.

Baitai FMT, SID, DS_, TRTP ir TREP yra apibrėžti toliau.

⁽¹⁾ Įkišta kortelė suteiks atitinkamas prieigos prie duomenų perkėlimo funkcijos ir duomenų teises.

DDP_003 Jei pranešimu reikia persiųsti duomenis, kurių ilgis didesnis už duomenų laukeliui skirtą vietą, pranešimas siunčiamas keletu popranešimų. Kiekviename popranešime yra antraštė, tas pats SID, TREP ir 2 baitų popranešimų skaitiklis, nurodantis jo eilės numerį visame pranešime. Tam, kad galima būtų tikrinti, ar nėra klaidų ir nutraukti siuntimą, IDE patvirtina kiekvieną popranešimą. IDE gali priimti popranešimą, paprašyti jį pakartoti, pareikalauti TPB pradėti siųsti iš naujo arba nutraukti siuntimą.

DDP_004 Jei paskutinio popranešimo duomenų laukelyje yra tiksliai 255 baitai, pranešimo pabaigai nurodyti turi būti išsiųstas galutinis popranešimas su tuščiu duomenų laukeliu (išskyrus SID, TREP ir popranešimų skaitiklį).

Pavyzdys:

Antraštė	SID	TREP	Pranešimas	CS
4 baitai	daugiau kaip 255 baitai			

Siunčiama taip:

Antraštė	SID	TREP	00	01	Popranešimis Nr. 1	CS
4 baitai	255 baitai					

Antraštė	SID	TREP	00	02	Popranešimis Nr. 2	CS
4 baitai	255 baitai					

...

Antraštė	SID	TREP	xx	yy	Popranešimis Nr. n	CS
4 baitai	mažiau kaip 255 baitai					

arba:

Antraštė	SID	TREP	00	01	Popranešimis Nr. 1	CS
4 baitai	255 baitai					

Antraštė	SID	TREP	00	02	Popranešimis Nr. 2	CS
4 baitai	255 baitai					

...

Antraštė	SID	TREP	xx	yy	Popranešimis Nr. n	CS
4 baitai	255 baitai					

Antraštė	SID	TREP	xx	yy+1	CS
4 baitai	4 baitai				

2.2.2. Pranešimų rūšys

Pagal duomenų perkėlimo iš (i) TPB ir IDE protokolą reikia naudoti aštuonių skirtingų rūšių pranešimus.

Šie pranešimai nurodyti toliau esančioje lentelėje.

Pranešimo struktūra		Antraštė daugiausia 4 baitai				Duomenys daugiausia 255 baitai			Kontrolinė suma 1 baitas								
IDE ->	<- TPB	FMT	TGT	SRC	LEN	SID	DS_/TRTP	DATA	CS								
Ryšio pareikalavimo pradžia		81	EE	F0		81			E0								
Teigiamas atsakymas, ryšio pradžia		80	F0	EE	03	C1		8F,EA	9B								
Diagnostikos seanso pareikalavimo pradžia		80	EE	F0	02	10	81		F1								
Teigiamas atsakymas, diagnostikos pradžia		80	F0	EE	02	50	81		31								
Ryšio kanalo valdymo paslauga																	
Patikrinti spartą bodais (1 etapas)																	
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								
Teigiamas atsakymas, patikrinti spartą		80	F0	EE	02	C7		01	28								
Perdavimo sparta bodais (2 etapas)		80	EE	F0	03	87		02,03	ED								
Nusiuntimo pareikalavimas		80	EE	F0	0A	35		00,00,00, 00,00,FF,FF, FF,FF	99								
Teigiamas atsakymas, nusiųsti duomenis		80	F0	EE	03	75		00,FF	D5								
Pareikalavimas persiųsti duomenis																	
Apžvalga										80	EE	F0	02	36	01		97
Veikla										80	EE	F0	06	36	02	Data	CS
Įvykiai ir gedimai										80	EE	F0	02	36	03		99
Išsami informacija apie greitį										80	EE	F0	02	36	04		9A
Techniniai duomenys										80	EE	F0	02	36	05		9B
Duomenų perkėlimas iš kortelės		80	EE	F0	02	36	06		9C								
Teigiamas atsakymas, persiųsti duomenis		80	F0	EE	Len	76	TREP	Duomenys	CS								
Nutraukti perdavimą		80	EE	F0	01	37			96								
Teigiamas atsakymas, nutraukti perdavimą		80	F0	EE	01	77			D6								
Pareikalavimas nutraukti ryšį		80	EE	F0	01	82			E1								
Teigiamas atsakymas, nutraukti ryšį		80	F0	EE	01	C2			21								
Patvirtinti popranešimų		80	EE	F0	Len	83		Duomenys	CS								
Neigiami atsakymai																	
Bendrasis atmetimas		80	F0	EE	03	7F	Sid req	10	CS								
Paslauga netinkama		80	F0	EE	03	7F	Sid req	11	CS								
Funkcija netinkama		80	F0	EE	03	7F	Sid req	12	CS								
Netinkamas pranešimo ilgis		80	F0	EE	03	7F	Sid req	13	CS								
Netinkamos sąlygos arba pareikalavimo sekos klaida		80	F0	EE	03	7F	Sid req	22	CS								
Pareikalavimas nepriimtinas		80	F0	EE	03	7F	Sid req	31	CS								
Nusiuntimas nepriimtinas		80	F0	EE	03	7F	Sid req	50	CS								
Laukiama atsakymo		80	F0	EE	03	7F	Sid req	78	CS								
Duomenų negalima gauti		80	F0	EE	03	7F	Sid req	FA	CS								

Pastabos:

— Sid Req = atitinkamo pareikalavimo SID.

— TREP = atitinkamo pareikalavimo TRTP.

— Juodi langeliai reiškia, kad niekas nesiunčiama.

— Terminas „nusiųsti“ [upload] (vertinant iš IDE) vartojamas pagal ISO 14229. Jis reiškia tą patį, ką ir perkelti duomenis (vertinant iš TPB).

— Šioje lentelėje nepavaizduoti galimi 2 baitų ilgio popranešimų skaitikliai.

2.2.2.1. *Start communication request [pareikalavimas pradėti ryšį] (SID 81)*

DDP_005 Ši pranešimą IDE siunčia norėdama užmegzti ryšį su TPB. Iš pradžių visuomet bendraujama 9 600 bodų sparta (iki sparta pakeičiama naudojantis atitinkamomis ryšio kanalo valdymo paslaugomis).

2.2.2.2. *Positive response start communication [teigiamas atsakymas į pareikalavimą pradėti ryšį] (SID C1)*

DDP_006 Ši pranešimą TPB siunčia norėdamas teigiamai atsakyti į pareikalavimą pradėti ryšį. Pranešime yra du raktiniai baitai „8F“ ir „EA“, kurie nurodo, kad įrenginys geba taikyti protokolą su antrašte, kurioje yra informacija apie tikslą, šaltinį ir ilgį.

2.2.2.3. *Start diagnostic session request [pareikalavimas pradėti diagnostikos seansą] (SID 10)*

DDP_007 Pranešimą **Start diagnostic session request** IDE siunčia naujam diagnostikos seansui su TPB pradėti. Subfunkcija „numatytasis seansas“ (81 Hex) nurodo, kad reikia pradėti standartinį diagnostikos seansą.

2.2.2.4. *Positive response start diagnostic [teigiamas atsakymas į pareikalavimą pradėti diagnostikos seansą] (SID 50)*

DDP_008 Pranešimą **Positive response start diagnostic** TPB siunčia norėdamas teigiamai atsakyti į pareikalavimą pradėti diagnostikos seansą.

2.2.2.5. *Link control service [ryšio kanalo valdymo paslaugos pareikalavimas] (SID 87)*

DDP_052 Pranešimą **Link control service** IDE naudoja duomenų perdavimo spartai pakeisti. Tai vyksta dviem etapais. Pirmu etapu IDE pasiūlo pakeisti spartą ir nurodo naują spartą. Gavusi teigiamą atsakymą iš TPB, IDE siunčia į TPB spartos pakeitimo patvirtinimą (antrasis etapas). Tuomet IDE pradeda naudoti naują spartą. Gavęs patvirtinimą, TPB taip pat pradeda naudoti naują spartą.

2.2.2.6. *Link control positive response [teigiamas atsakymas į pareikalavimą suteikti ryšio kanalo valdymo paslaugą] (SID C7)*

DDP_053 Pranešimą **Link control positive response** TPB siunčia norėdamas teigiamai atsakyti į pareikalavimą suteikti ryšio kanalo valdymo paslaugą (pirmasis etapas). Atkreipkite dėmesį, kad į patvirtinimo pareikalavimą neatsakoma (antrasis etapas).

2.2.2.7. *Request upload [duomenų nusiuntimo pareikalavimas] (SID 35)*

DDP_009 Pranešimą **Request upload** IDE siunčia norėdama nurodyti TPB, kad reikalauja duomenų perkėlimo operacijos. Laikantis ISO 14229 reikalavimų, pranešime nurodomas reikalaujamų duomenų adresas, dydis ir formatas. Jei iki duomenų perkėlimo tai nėra žinoma IDE, atminties adresas nustatomas į 0, formatas nekoduojamas ir nearchyvuojamas, o atminties dydis nustatomas didžiausias.

2.2.2.8. *Positive response request upload [teigiamas atsakymas į nusiuntimo pareikalavimą] (SID 75)*

DDP_010 Pranešimą **Positive response request upload** TPB siunčia norėdamas pranešti IDE, kad TPB pasirengęs priimti duomenis. Laikantis ISO 14229 reikalavimų, šiame pranešime yra informacija, nurodanti IDE, kad kituose teigiamo atsakymo į duomenų perdavimo pareikalavimą pranešimuose bus ne daugiau kaip 00FF hex baitų.

2.2.2.9. *Transfer data request [duomenų perdavimo pareikalavimas] (SID 36)*

DDP_011 Pranešimą **Transfer data request** IDE siunčia norėdama nurodyti TPB duomenų, kuriuos reikia perkelti, rūšį. Vieno baito perdavimo pareikalavimo parametras (TRTP) nurodo perdavimo rūšį.

Yra šešios duomenų perdavimo rūšys:

- apžvalga (TRTP 01),
- veikla nurodytą datą (TRTP 02),
- įvykiai ir gedimai (TRTP 03),
- išsami informacija apie greitį (TRTP 04),
- techniniai duomenys (TRTP 05),
- duomenų perkėlimas iš kortelės (TRTP 06).

DDP_054 Duomenų perkėlimo seanso metu IDE privalo pareikalauti perduoti duomenis (TRTP 01), kadangi tik taip užtikrinama, kad į atsiųstą rinkmeną bus įrašyti TPB pažymėjimai (ir galima bus patikrinti skaitmeninį parašą).

Antruoju atveju (TRTP 02) duomenų perdavimo pareikalavimo pranešime nurodoma kalendorinė diena (formatu *Time-Real*), kurios duomenys turi būti perkelti.

2.2.2.10. *Positive response transfer data* [teigiamas atsakymas į duomenų perdavimo pareikalavimą] (SID 76)

DDP_012 Pranešimą **Positive response transfer data** TPB siunčia atsakydamas į pareikalavimą. Pranešime yra pareikalauti duomenys ir pareikalavimo TRTP atitinkantis perdavimo atsakymo parametras (TREP).

DDP_055 Pirmuoju atveju (TREP 01) TPB siunčia duomenis, padėdamas IDE operatoriui pasirinkti, kokius dar duomenis jis nori perkelti. Šiame pranešime yra tokia informacija:

- apsaugos pažymėjimai,
- transporto priemonės identifikacija,
- TPB esama data ir laikas,
- ankščiaušieji ir vėliausioji data, kurių duomenis galima perkelti (TPB duomenys),
- kortelių buvimo TPB nuoroda,
- ankstesnis duomenų perkėlimas į įmonę,
- įmonės užrašai,
- pirmiau atliktos kontrolės.

2.2.2.11. *Request transfer exit* [pareikalavimas nutraukti siuntimą] (SID 37)

DDP_013 Pranešimą **Request transfer exit** IDE siunčia norėdama informuoti TPB, kad duomenų perkėlimo seansas nutraukiamas.

2.2.2.12. *Positive response request transfer exit* [teigiamas atsakymas į pareikalavimą nutraukti siuntimą] (SID 77)

DDP_014 Pranešimą **Positive response request transfer exit** TPB siunčia pareikalavimui patvirtinti.

2.2.2.13. *Stop communication* [pareikalavimas nutraukti ryšį] (SID 82)

DDP_015 Pranešimą **Stop communication** IDE siunčia norėdama nutraukti ryšio su TPB jungtį.

2.2.2.14. *Positive response stop communication* [teigiamas atsakymas į pareikalavimą nutraukti ryšį] (SID C2)

DDP_016 Pranešimą **Positive response stop communication** TPB siunčia pareikalavimui patvirtinti.

2.2.2.15. *Acknowledge submessage* [popranešimo patvirtinimas] (SID C2)

DDP_017 Pranešimą **Acknowledge submessage** IDE siunčia kiekvienos pranešimo dalies gavimui patvirtinti, kai pranešimas siunčiamas keletu popranešimų. Duomenų laukelyje yra iš TPB gautas SID ir 2 baitų kodas:

- MsgC+1: patvirtina, kad popranešimis Nr. MsgC gautas tinkamai.

IDE siunčia reikalavimą TPB atsiųsti kitą popranešimą,

- MsgC: žymi nesklandumą priimant popranešimą Nr. MsgC.

IDE siunčia reikalavimą TPB pakartoti popranešimą,

- FFFF: reikalauja nutraukti pranešimą.

Šį kodą IDE gali naudoti TPB pranešimo siuntimui nutraukti dėl bet kokios priežasties.

Paskutinis pranešimo popranešimis (LEN baitas < 255) gali būti patvirtintas naudojant bet kurį iš pirmiau nurodytų kodų arba išvis nepatvirtintas.

TPB atsakymai, sudaryti iš keleto popranešimų, yra:

- Teigiamas atsakymas į duomenų perdavimo pareikalavimą (SID 76).

2.2.2.16. *Negative response* [neigiamas atsakymas] (SID 7F)

DDP_018 Pranešimą **Negative response** TPB siunčia atsakydamas į pirmiau išvardytus pranešimus, kai TPB negali patenkinti pareikalavimo. Pranešimo duomenų laukelyje yra atsakymo SID (7F), pareikalavimo SID ir kodas, nurodantis neigiamo atsakymo priežastį. Galimi tokie kodai:

- 10: bendrasis atmetimas:
Veiksmo atlikti negalima ne dėl vienos iš toliau nurodytų priežasčių.
- 11: paslauga netinkama:
Nesuprantamas pareikalavimo SID.
- 12 funkcija netinkama:
Nesuprantamas pareikalavimo DS_ arba TRTP arba nėra kitų popranešimų, kuriuos reikia persiųsti.
- 13: netinkamas pranešimo ilgis:
Gauto pranešimo ilgis yra netinkamas.
- 22: netinkamos sąlygos arba pareikalavimo sekos klaida:
Pareikalauta paslauga neaktyvi arba pareikalavimo pranešimų seka yra neteisinga.
- 31: pareikalavimas nepriimtinas:
Pareikalavimo parametro įrašas (duomenų laukelis) negalioja.
- 50: nusiuntimas nepriimtinas:
Pareikalavimo negalima patenkinti (TPB veikia ne tuo darbo režimu arba įvyko vidinis gedimas).
- 78: laukiama atsakymo:
Pareikalauto veiksmo negalima užbaigti laiku ir TPB nepasirengęs priimti kito pareikalavimo.
- FA: duomenų negalima gauti
TPB nėra pareikalavimo persiųsti duomenis objekto (pvz., neįkišta kortelė ir pan.).

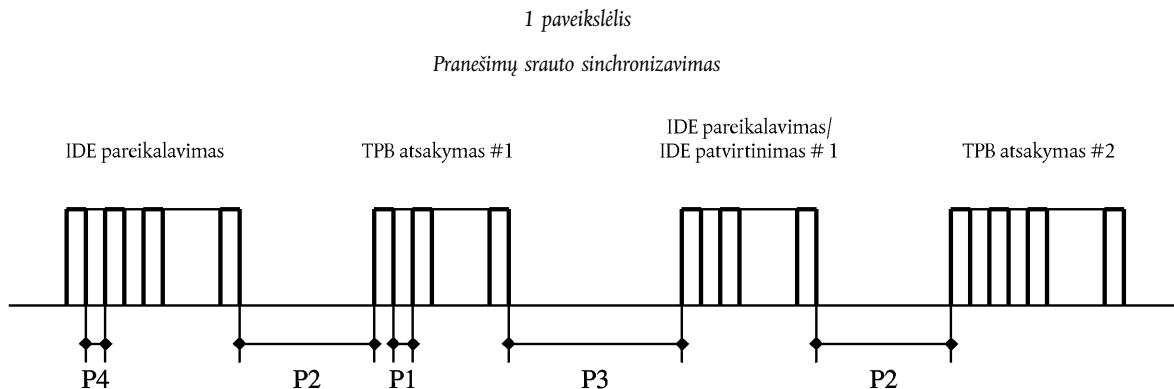
2.2.3. Pranešimų srautas

Įprastinės duomenų perkėlimo procedūros pranešimų srautas paprastai būna toks:

IDE		FE
Pareikalavimas pradėti ryšį	⇒ ⇐	Teigiamas atsakymas
Pareikalavimas pradėti diagnostikos seansą	⇒ ⇐	Teigiamas atsakymas
Nusiuntimo pareikalavimas	⇒ ⇐	Teigiamas atsakymas
Duomenų perdavimo pareikalavimas: apžvalga	⇒ ⇐	Teigiamas atsakymas, persiųsti
Duomenų pareikalavimas #2	⇒ ⇐	Teigiamas atsakymas #1
Patvirtinti popranešimą #1	⇒ ⇐	Teigiamas atsakymas #2
Patvirtinti popranešimą #2	⇒ ⇐	Teigiamas atsakymas #m
Patvirtinti popranešimą #m	⇒ ⇐	Teigiamas atsakymas (duomenų laukelis < 255 baitai)
Patvirtinti popranešimą (neprivaloma)	⇒	
...		
Duomenų perdavimo pareikalavimas #3	⇒ ⇐	Teigiamas atsakymas
Pareikalavimas nutraukti siuntimą	⇒ ⇐	Teigiamas atsakymas
Pareikalavimas nutraukti ryšį	⇒ ⇐	Teigiamas atsakymas

2.2.4. Sinchronizavimas

DDP_019 Įprasto darbo metu naudojami paveikslėlyje pavaizduoti sinchronizavimo parametrai:



Čia:

P1 = tarpbaitinis laikas TPB atsakymui.

P2 = laikas tarp IDE pareikalavimo pabaigos ir TPB atsakymo pradžios arba tarp IDE patvirtinimo pabaigos ir kitos TPB atsakymo pradžios.

P3 = laikas tarp TPB atsakymo pabaigos ir naujo IDE pareikalavimo pradžios arba tarp TPB atsakymo pabaigos ir IDE patvirtinimo pradžios arba tarp IDE pareikalavimo pabaigos ir naujo IDE pareikalavimo pradžios (jei TPB neat-sako).

P4 = tarpbaitinis laikas IDE pareikalavimui.

P5 = pailginta P3 trukmė perkeliant duomenis iš kortelės.

Sinchronizavimo parametrų leistinos vertės pateiktos toliau esančioje lentelėje (KWP išplėstasis sinchronizavimo para-metrų rinkinys, naudojamas fizinio adresavimo atveju spartesniam ryšiui).

Sinchronizavimo parametras	Apatinė ribinė vertė (ms)	Viršutinė ribinė vertė (ms)
P1	0	20
P2	20	1 000 (*)
P3	10	5 000
P4	5	20
P5	10	20 minučių

(*) Jei TPB atsako neigiamai ir atsakyme yra kodas, reiškiantis „pareikalavimas gautas tinkamai, laukiama atsakymo“, ši vertė didinama iki P3 viršutinės ribinės vertės.

2.2.5. Klaidų valdymas

Jei keičiantis pranešimais įvyksta klaida, pranešimų srauto schema pakeičiama atsižvelgiant į tai, kurioje įrangoje aptikta klaida, ir į klaidą sąlygojantį pranešimą.

2 ir 3 paveikslėliuose pavaizduotos atitinkamai TPB ir IDE klaidų valdymo procedūros.

2.2.5.1. Ryšio pradžios etapas

DDP_020 Jei IDE aptinka klaidą pagal sinchronizavimą arba bitų srautą ryšio pradžios etapu, tuomet ji palaukia P3 minučių laiko-tarpį ir pakartoja pareikalavimą.

DDP_021 Jei TPB aptinka klaidą iš IDE atėjusioje sekoje, jis nesiunčia atsakymo ir ne ilgiau kaip P3 laikotarpį laukia kito pareikala-vimo pradėti ryšį.

2.2.5.2. Ryšio etapas

Galima išskirti dvi atskiras klaidų valdymo sritis:

1. TPB aptinka IDE siuntimo klaidą.

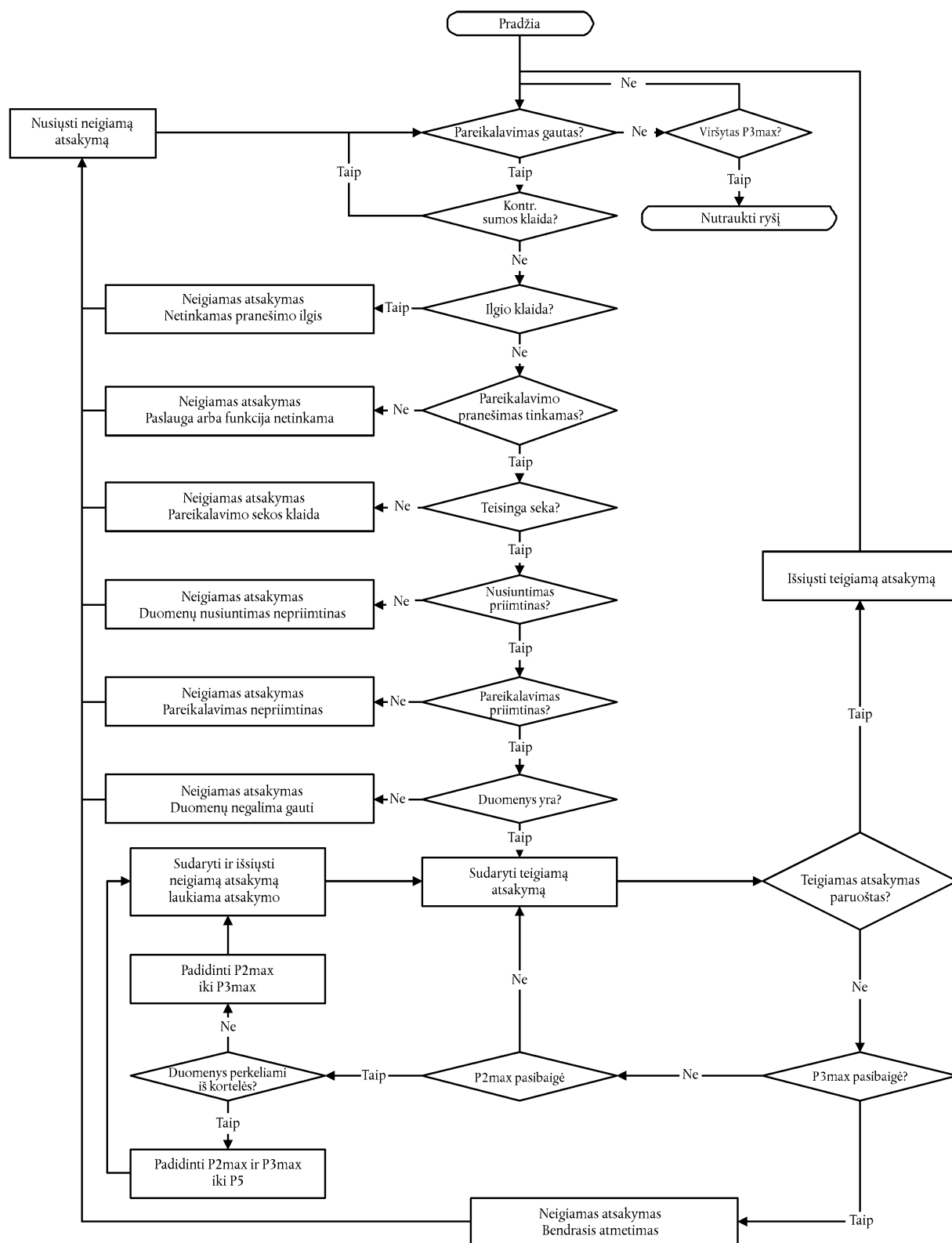
DDP_022 TPB turi aptikti visas sinchronizavimo klaidas, baitų formato klaidas (pvz., pradžios arba pabaigos bito pažeidimus) ir struktūros klaidas (neteisingą gautų baitų skaičių, neteisingą kontrolinės sumos baitą).

DDP_023 Jei TPB aptinka vieną iš pirmiau išvardytų klaidų, jis nesiunčia atsakymo ir ignoruoja priimtą pranešimą.

DDP_024 TPB gali aptikti ir kitas gauto pranešimo formato arba turinio klaidas (pvz., pranešimas netinkamas) net jei pranešimas atitinka ilgio ir kontrolinės sumos reikalavimus; tokiu atveju TPB atsako neigiamu atsakymo pranešimu ir nurodo klaidos pobūdį.

2 paveikslėlis

TPB klaidų valdymas

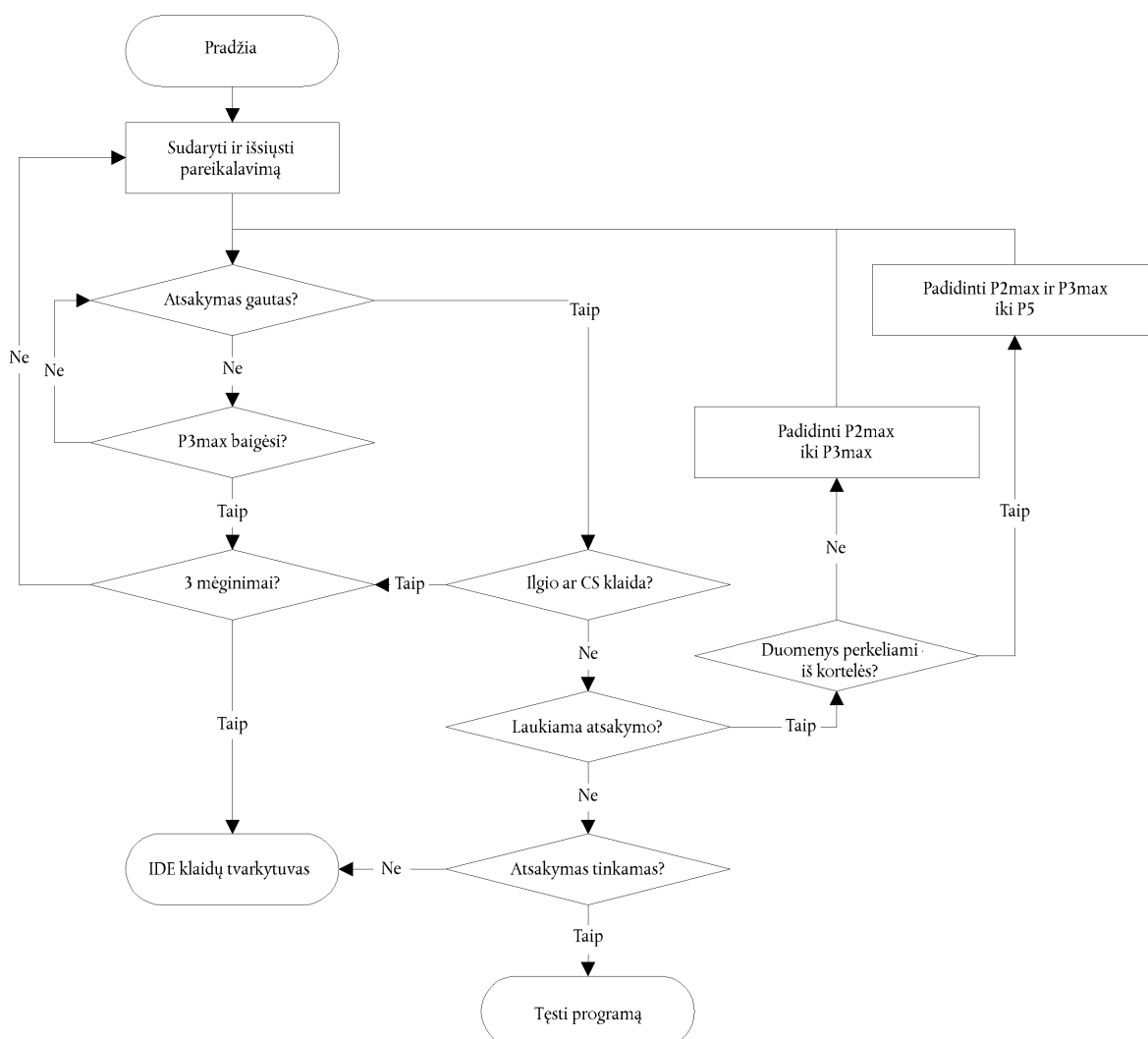


2. IDE aptinka TPB siuntimo klaidą.

- DDP_025 IDE turi aptikti visas sinchronizavimo klaidas, baitų formato klaidas (pvz., pradžios arba pabaigos bito pažeidimus) ir struktūros klaidas (neteisingą gautų baitų skaičių, neteisingą kontrolinės sumos baitą).
- DDP_026 IDE turi aptikti sekos klaidas, pvz., netinkamą popranešimų skaitiklio kitimą vienas po kito gautuose pranešimuose.
- DDP_027 Jei IDE aptinka klaidą arba TPB neatsako per laikotarpį P2max, pareikalavimo pranešimas siunčiamas pakartotinai (iš viso ne daugiau kaip tris kartus). Kad būtų galima aptikti šią klaidą, popranešimo patvirtinimas laikomas pareikalavimu TPB.
- DDP_028 Prieš pradėdama naują siuntimą IDE turi palaukti ne trumpiau kaip laikotarpį P3min; pauzės laikotarpis skaičiuojamas nuo paskutinio apskaičiuoto pabaigos bito pasirodymo aptikus klaidą.

3 paveikslėlis

IDE klaidų valdymas



2.2.6. Atsakymo pranešimo turinys

Šiame punkte aprašytas įvairių teigiamo atsakymo pranešimų duomenų laukelių turinys.

Duomenų elementų apibrėžimas pateiktas 1 priedėlyje „Duomenų žodynelis“.

2.2.6.1. Positive response transfer data overview [teigiamas atsakymas į duomenų perdavimo pareikalavimą: apžvalga]

DDP_029 Pranešimo Positive response transfer data overview duomenų laukelyje turi būti tokia informacija, išdėstyta tokia tvarka pagal SID 76 Hex, TREP 01 Hex ir tokiu būdu atskiriant bei skaičiuojant popranešimus:

Duomenų elementas	Ilgis (baitais)	Komentaras
MemberStateCertificate	194	TPB apsaugos pažymėjimai
VUCertificate	194	
VehicleIdentificationNumber	17	Transporto priemonės identifikacija
VehicleRegistrationIdentification	1	
vehicleRegistrationNation vehicleRegistrationNumber	14	
CurrentDateTime	4	TPB esama data ir laikas
VuDownloadablePeriod		Laikotarpis, kurio duomenis galima perkelti
minDownloadableTime maxDownloadableTime	4 4	
CardSlotsStatus	1	Į TPB įkištų kortelių rūšys
VuDownloadActivityData		Ankstesnis duomenų perkėlimas iš TPB
downloadingTime	4	
fullCardNumber companyOrWorkshopName	18 36	
VuCompanyLocksData		Visi į atmintį įrašyti įmonės užraktai. Jei segmentas tuščias, siunčiama tik noOfLocks=0.
noOfLocks	1	
...	(98)	
Vu Company Locks Record	4	
lockInTime	4	
lockOutTime	36	
companyName companyAddress companyCardNumber	36 18	
...		Visi TPB atmintyje laikomi įrašai apie kontrolę. Jei segmentas tuščias, siunčiama tik noOfControls=0.
VuControlActivityData	1	
noOfControls	(31)	
...		
Vu Control Activity Record	1	
controlType controlTime controlCardNumber downloadPeriodBeginTime downloadPeriodEndTime	4 18 4 4	
...		Visų duomenų (išskyrus pažymėjimus), pradedant nuo įrašo Vehicle-IdentificationNumber iki paskutinio įrašo VuControlActivityRecord paskutinio brito, RSA parašas.
Signature	128	

2.2.6.2. Positive response transfer data activities [teigiamas atsakymas į duomenų perdavimo pareikalavimą: veiklos rūšys]

DDP_030 Pranešimo Positive response transfer data activities duomenų laukelyje turi būti tokia informacija, išdėstyta tokia tvarka pagal SID 76 Hex, TREP 02 Hex ir tokiu būdu atskiriant bei skaičiuojant popranešimus:

Duomenų elementas	Ilgis (baitais)	Komentaras
TimeReal	4	Dienos, kurios duomenys perkeliami, data
OdometerValueMidnight	3	Hodometro rodmenys vertė dienos, kurios duomenys perkeliami, pabaigoje
VuCardIWData noOfVuCardIWRecords	2	Duomenys apie kortelių įkišimo ir ištraukimo ciklus.
...	(129)	– Jei šiame segmente nėra duomenų, siunčiama tik noOfVuCardIWRecords=0.
VuCardIWRecord	36	– Jei įrašas VuCardIWRecord pereina 00.00 val. ribą
cardHolderName	36	(kortelė įkišta ankstesnę dieną)
holderSurname	18	arba 24.00 val. ribą
holderFirstNames	4	(kortelė ištraukta kitą dieną), jis turi būti pateiktas visas, aprėpiant abi dienas.
fullCardNumber	4	
cardExpiryDate	4	
cardInsertionTime	3	
vehicleOdometerValueAtInsertion	1	
cardSlotNumber	4	
cardWithdrawalTime	3	
vehicleOdometerValueAtWithdrawal		
previousVehicleInfo		
vehicleRegistrationIdentification	1	
vehicleRegistrationNation	14	
vehicleRegistrationNumber	4	
cardWithdrawalTime	4	
manualInputFlag	1	
...		
VuActivityDailyData noOfActivityChanges	2	Plyšių būseną 00.00 val. ir veiklos pasikeitimai, užregistruoti dieną, kurios duomenys perkeliami.
...		
ActivityChangeInfo	2	
...		
VuPlaceDailyWorkPeriodData noOfPlaceRecords	1	Duomenys apie vietas, užregistruoti dieną, kurios duomenys perkeliami.
...	(28)	Jei segmentas tuščias, siunčiama tik noOfPlaceRecords=0.
VuPlaceDailyWorkPeriodRecord	18	
fullCardNumber	4	
placeRecord	1	
entryTime	1	
entryTypeDailyWorkPeriod	1	
dailyWorkPeriodCountry	1	
dailyWorkPeriodRegion	1	
vehicleOdometerValue	3	
...		
VuSpecificConditionData noOfSpecificConditionRecords	2	Duomenys apie ypatingas būsenas, užregistruoti dieną, kurios duomenys perkeliami.
...	(5)	Jei segmentas tuščias, siunčiama tik noOfSpecificCondition-Records=0.
SpecificConditionRecord	4	
EntryTime	1	
specificConditionType		
...		
Signature	128	Visų duomenų (išskyrus pažymėjimus), pradedant nuo įrašo TimeReal iki paskutinio įrašo apie ypatingą sąlygą paskutinio baido, RSA parašas.

2.2.6.3. Positive response transfer data events and faults [teigiamas atsakymas į duomenų perdavimo pareikalavimą: įvykiai ir gedimai]

DDP_031 Pranešimo Positive response transfer data events and faults duomenų laukelyje turi būti tokia informacija, išdėstyta tokia tvarka pagal SID 76 Hex, TREP 03 Hex ir tokiu būdu atskiriant bei skaičiuojant popranešimus:

Duomenų elementas		Ilgis (baitais)	Komentaras
VuFaultData			
NoOfVuFaults		1	Visa TPB atmintyje įrašyta informacija apie gedimus. Jei segmentas tuščias, siunčiama tik noOfVuFaults=0.
...		(82)	
VuFaultRecord	FaultType	1	
	FaultRecordPurpose	1	
	FaultBeginTime	4	
	FaultEndTime	4	
	CardNumberDriverSlotBegin	18	
	cardNumberCodriverSlotBegin	18	
	CardNumberDriverSlotEnd	18	
	CardNumberCodriverSlotEnd	18	
...			
VuEventData			
NoOfVuEvents		1	Visa TPB atmintyje įrašyta informacija apie įvykius (išskyrus greičio viršijimą). Jei segmentas tuščias, siunčiama tik 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	Duomenys apie paskutinę greičio viršijimo kontrolę (jei duomenų nėra – numatytoji vertė).
FirstOverspeedSince		4	
NumberOfOverspeedSince		1	
VuOverSpeedingEventData			
NoOfVuOverSpeedingEvents		1	Visa TPB atmintyje įrašyta informacija apie greičio viršijimo įvykius. Jei segmentas tuščias, siunčiama tik noOfOverSpeedingEvents=0.
...		(31)	
VuOverSpeedingEventRecord	EventType	1	
	EventRecordPurpose	1	
	EventBeginTime	4	
	EventEndTime	4	
	MaxSpeedValue	1	
	AverageSpeedValue	1	
	CardNumberDriverSlotBegin	18	
	SimilarEventsNumber	1	
...			
VuTimeAdjustmentData			
NoOfVuTimeAdjRecords		1	Visa TPB atmintyje įrašyta informacija apie laiko koregavimo įvykius (išskyrus visiško kalibravimo atvejus). Jei segmentas tuščias, siunčiama tik noOfVuTimeAdjRecords=0.
...		(98)	
VuTimeAdjustmentRecord	OldTimeValue	4	
	NewTimeValue	4	
	WorkshopName	36	
	WorkshopAddress	36	
	WorkshopCardNumber	18	
...			
Signature		128	Visų duomenų (išskyrus pažymėjimus), pradedant nuo įrašo NoOfVuFaults iki paskutinio įrašo apie laiko koregavimą paskutinio baido, RSA parašas.

2.2.6.4. *Positive response transfer data detailed speed* [teigiamas atsakymas į duomenų perdavimo pareikalavimą: išsami informacija apie greitį]

DDP_032 Pranešimo Positive response transfer data detailed speed duomenų laukelyje turi būti tokia informacija, išdėstyta tokia tvarka pagal SID 76 Hex, TREP 04 Hex ir tokiu būdu atskiriant bei skaičiuojant popranešimus:

Duomenų elementas		Ilgis (baitais)	Komentaras
VuDetailedSpeedData			
NoOfSpeedBlocks		2	Visa TPB atmintyje įrašyta informacija apie laiko koregavimo įvykius (išskyrus visiško kalibravimo atvejus). Jei segmentas tuščias, siunčiama tik noOfVuTimeAdjRecords=0.
...			
VuDetailedSpeedBlock	SpeedBlockBeginDate	4	
	speedsPerSecond	60	
...			
Signature		128	Visų duomenų (išskyrus pažymėjimus), pradedant nuo įrašo NoOfVuFaults iki paskutinio įrašo apie laiko koregavimą paskutinio brito, RSA parašas.

2.2.6.5. *Positive response transfer data technical data* [teigiamas atsakymas į duomenų perdavimo pareikalavimą: techniniai duomenys]

DDP_033 Pranešimo Positive response transfer data technical data duomenų laukelyje turi būti tokia informacija, išdėstyta tokia tvarka pagal SID 76 Hex, TREP 05 Hex ir tokiu būdu atskiriant bei skaičiuojant popranešimus:

Duomenų elementas		Ilgis (baitais)	Komentaras
VuIdentification			
vuManufacturerName		36	
vuManufacturerAddress		36	
vuPartNumber		16	
vuSerialNumber		8	
vuSoftwareIdentification			
vuSoftwareVersion		4	
vuSoftInstallationDate		4	
vuManufacturingDate		4	
vuApprovalNumber		8	
SensorPaired			
sensorSerialNumber		8	
sensorApprovalNumber		8	
sensorPairingDateFirst		4	
VuCalibrationData			
noOfVuCalibrationRecords		1	Visa TPB atmintyje laikomi įrašai apie kalibravimą.
...		(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	Visų duomenų (išskyrus pažymėjimus), pradedant nuo įrašo vuManufacturer-Name iki paskutinio įrašo VuCalibrationRecord paskutinio brito, RSA parašas.

2.3. ESM rinkmenų laikymas

- DDP_034 Kai duomenų perkėlimo seanse perduodami duomenys iš TPB, IDE turi įrašyti vienoje fizinėje rinkmenoje visus per duomenų perkėlimo seansą pranešimuose **Positive response transfer data** iš TPB gautus duomenis. Neįrašomos tik pranešimų antraštės, popranešimų skaitikliai, tušti popranešimai ir kontrolinės sumos, tačiau įrašomi SID ir TREP (jei yra keletas popranešimų — tik pirmojo popranešimo).

3. DUOMENŲ PERKĖLIMO IŠ TACHOGRAFO KORTELIŲ PROTOKOLAS

3.1. Taikymo sritis

Šiame skyriuje aprašyta, kaip duomenys tiesiogiai perkeliama iš tachografo kortelės į IDE. IDE nėra apsaugos aplinkos dalis, todėl tarp kortelės ir IDE autentiškumas netikrinamas.

3.2. Apibrėžimai

Duomenų perkėlimo seansas: Laikas, kai iš ICC perkeliama duomenys. Seansas aprėpia visą procedūrą nuo ICC perkrovimo, kurį atlieka IFD, iki ICC dezaktyvavimo (kortelės ištraukimo arba kito perkrovimo).

Duomenų rinkmena su parašu: Rinkmena iš ICC. Rinkmena siunčiama į IFD paprastu tekstu. ICC atliekama rinkmenos maiša, ji pasirašoma, o parašas perduodamas į IFD.

3.3. Duomenų perkėlimas iš kortelės

- DDP_035 Duomenys iš tachografo kortelės perkeliama tokiais etapais:

- bendra kortelės informacija perkeliama į EF ICC ir IC. Ši informacija yra neprivaloma, ji neapsaugota skaitmeniniu parašu,
- perkeliama EFs Card_Certificate ir CA_Certificate. Ši informacija neapsaugota skaitmeniniu parašu.

Kiekvieną duomenų perkėlimo seansą privaloma perkelti šias rinkmenas:

- perkeliama EF su kitais programos duomenimis (iš DF Tachograph) išskyrus EF Card_Download. Ši informacija apsaugota skaitmeniniu parašu,
- kiekvieną duomenų perkėlimo seansą privaloma perkelti EF Application_Identification ir ID,
- perkelti duomenis iš vairuotojo kortelės taip pat privaloma perkelti šiuos EF:
 - Events_Data,
 - Faults_Data,
 - Driver_Activity_Data,
 - Vehicles_Used,
 - Places,
 - Control_Activity_Data,
 - Specific_Conditions.
- perkelti duomenis iš vairuotojo kortelės, atnaujinama EF LastCardDownload esanti data Card_Download,
- perkelti duomenis iš dirbtuvių kortelės, EF Card_Download esantis kalibravimo skaitiklis grąžinamas į nulį.

3.3.1. Inicijavimo seka

DDP_036 IDE turi būti inicijuota seka taip:

Kortelė	Kryptis	IDE/IFD	Reikšmė, pastabos
	↵	Techninės įrangos perkrovimas	
ATR	⇒		

Galima naudoti PPS didesnei spartai pasirinkti, jei ji yra tinkama ICC.

3.3.2. Duomenų rinkmenų be parašo seka

DDP_037 ICC, IC, Card_Certificate ir CA_Certificate duomenų perkėlimo seka yra tokia:

Kortelė	Kryptis	IDE/IFD	Reikšmė, pastabos
	↵	Pasirinkti rinkmeną	Pasirinkti rinkmeną pagal vardą.
OK	⇒		
	↵	Nuskaityti dvinarį	Jei rinkmenoje yra daugiau duomenų, nei telpa skaitytuvo arba kortelės buferioje, komanda kartojama tol, kol nuskaityti visi duomenys.
Rinkmenos duomenys OK	⇒	Įrašyti duomenis į ESM	Pagal 3.4 „Duomenų laikymo formatus“.

:Pastaba: prieš pasirenkant EF Card_Certificate reikia pasirinkti Tachografo programą (pasirenkama pagal AID).

3.3.3. Duomenų rinkmenų be parašo seka

DDP_038 Kiekviena iš toliau nurodytų rinkmenų, kurias reikia perkelti su jų parašais, turi būti perkeliama tokia seka:

Kortelė	Kryptis	IDE/IFD	Reikšmė, pastabos
	↵	Pasirinkti rinkmeną	
OK	⇒		
	↵	Atlikti rinkmenos maišą	Pagal nustatytą maišos algoritmą (11 priedėlis) apskaičiuojama pasirinktos rinkmenos duomenų maišos vertė. Ši komanda nėra komanda pagal ISO.
Apskaičiuoti rinkmenos maišą ir laikinai įrašyti į atmintį maišos vertę			
OK	⇒		
	↵	Nuskaityti dvinarį	Jei rinkmenoje yra daugiau duomenų, nei telpa skaitytuvo arba kortelės buferioje, komanda kartojama tol, kol nuskaityti visi duomenys.
Rinkmenos duomenys OK	⇒	Įrašyti duomenis į ESM	Pagal 3.4 „Duomenų laikymo formatus“.
	↵	PSO: apskaičiuoti skaitmeninį parašą	
Atlikti apsaugos operaciją „apskaičiuoti skaitmeninį parašą“ panaudojant laikinai saugomą maišos vertę			
Parašas OK	⇒	Prirašyti duomenis prie ank- čiau į ESM įrašytų duomenų	Pagal 3.4 „Duomenų laikymo formatus“.

3.3.4. Kalibravimo skaitiklio grąžinimo į nulį seka

DDP_039 Dirbtuvių kortelės EF Card_Download skaitiklio NoOfCalibrationsSince-Download grąžinimo į nulį seka yra tokia:

Kortelė	Kryptis	IDE/IFD	Reikšmė, pastabos
OK	↩	Pasirinkti EF Card_Download	Pasirinkti rinkmeną pagal vardą
	↪		
	↩	Atnaujinti dvinarį NoOfCalibrations SinceDownload = '00 00'	
Grąžina duomenų perkėlimų iš kortelės skaitiklį į nulį			
OK	↪		

3.4. Duomenų įrašymo formatas

3.4.1. Įvadas

DDP_040 Perkelti duomenys turi būti įrašomi pagal tokius reikalavimus:

- duomenys turi būti įrašomi atvirai. Tai reiškia, kad įrašant turi išlikti tokia pati baitų eilės tvarka ir bitų eilės tvarka baite, kokia buvo kortelėje,
- visi per vieną duomenų perkėlimo seansą perkelti duomenys įrašomi vienoje ESM rinkmenoje.

3.4.2. Rinkmenų formatas

DDP_041 Rinkmenų formatas yra keleto TLV objektų sąryšis.

DDP_042 EF žymena yra FID ir priedas „00“.

DDP_043 EF parašo žymena yra FID ir priedas „01“.

DDP_044 Ilgis yra dviejų baitų vertė. Ši vertė apibrėžia baitų skaičių verčių laukelyje. Vertė !!!FF FF!!! ilgio laukelyje yra skirta panaudoti ateityje.

DDP_045 Kai duomenys iš rinkmenos neperkeliami, į atmintį neturi būti įrašoma jokia su ja susijusi informacija (jokios žymenos ir nulio ilgio).

DDP_046 Parašas turi būti įrašomas kaip TLV objektas, esantis iškart po TLV objekto, kuriame yra rinkmenos duomenys.

Apibrėžimas	Reikšmė	Ilgis
FID (2 baitai) „00“	EF (FID) žymena	3 baitai
FID (2 baitai) „01“	EF (FID) parašo žymena	3 baitai
xx xx	Verčių laukelio ilgis	2 baitai

Į ESM perkeltaje rinkmenoje esančių duomenų pavyzdys:

Žymena	Ilgis	Vertė
00 02 00	00 11	EF ICC duomenys
C1 00 00	00 C2	EF Card_Certificate duomenys
		...
05 05 00	0A 2E	EF Vehicles_Used duomenys
05 05 01	00 80	EF Vehicles_Used parašas

4. DUOMENŲ PERKĖLIMAS IŠ TACHOGRAFO KORTELĖS PER TRANSPORTO PRIEMONĖS BLOKĄ

- DDP_047 TPB turi leisti perkelti duomenis iš vairuotojo kortelės, įkištos į prijungtą IDE.
- DDP_048 IDE turi išsiųsti į TPB pranešimą **Transfer data request card download**, kad būtų pradėtas duomenų perkėlimo iš kortelės režimas (žr. 2.2.2.9).
- DDP_049 Tuomet rinkmena po rinkmenos pagal 3 skyriuje nustatytą protokolą TPB turi perkelti visus duomenis iš kortelės ir perduoti juos į IDE atitinkamu TLV rinkmenos formatu (žr. 3.4.2), įterpęs į pranešimą **Positive response transfer data**.
- DDP_050 IDE turi išrinkti kortelės duomenis iš pranešimo **Positive response transfer data** (pašalindama visas antraštes, SID, TREP, popranešimų skaitiklius ir kontrolines sumas) ir įrašyti juos į vieną fizinę rinkmeną, kaip aprašyta 2.3 poskyryje.
- DDP_051 Tuomet TPB turi atnaujinti vairuotojo kortelės rinkmenas `Control_Activity_Data` arba `Card_Download`.
-

8 priedėlis

KALIBRAVIMO PROTOKOLAS

TURINYS

1.	Įvadas	448
2.	Terminai, apibrėžimai ir nuorodos	448
3.	Paslaugų apžvalga	448
3.1.	Galimos paslaugos	448
3.2.	Atsakymo kodai	449
4.	Ryšio paslaugos	449
4.1.	Paslauga „StartCommunication“ [pradėti ryšį]	449
4.2.	Paslauga „StopCommunication“ [nutraukti ryšį]	451
4.2.1.	Pranešimo aprašymas	451
4.2.2.	Pranešimo formatas	452
4.2.3.	Parametrų apibrėžimas	453
4.3.	Paslauga „TesterPresent“ [testeris yra]	453
4.3.1.	Pranešimo aprašymas	453
4.3.2.	Pranešimo formatas	453
5.	Valdymo paslaugos	454
5.1.	Paslauga „StartDiagnosticSession“ [pradėti diagnostikos seansą]	454
5.1.1.	Pranešimo aprašymas	454
5.1.2.	Pranešimo formatas	455
5.1.3.	Parametrų apibrėžimas	456
5.2.	Paslauga „SecurityAccess“ [apsauginė prieiga]	456
5.2.1.	Pranešimo aprašymas	456
5.2.2.	Pranešimo formatas. „SecurityAccess“. „requestSeed“	457
5.2.3.	Pranešimo formatas. „SecurityAccess“. „sendKey“	458
6.	Duomenų perdavimo paslaugos	459
6.1.	Paslauga „ReadDataByIdentifier“ [nuskaityti duomenis pagal vardą]	459
6.1.1.	Pranešimo aprašymas	459
6.1.2.	Pranešimo formatas	459
6.1.3.	Parametrų apibrėžimas	460
6.2.	Paslauga „WriteDataByIdentifier“ [įrašyti duomenis pagal vardą]	461
6.2.1.	Pranešimo aprašymas	461
6.2.2.	Pranešimo formatas	461
6.2.3.	Parametrų apibrėžimas	462
7.	Bandomųjų impulsų valdymas. įvesties ir išvesties valdymo funkcinis blokas	462
7.1.	Paslauga „InputOutputControlByIdentifier“ [įvesties ir išvesties valdymas pagal vardus]	462

7.1.1.	Pranešimo aprašymas	462
7.1.2.	Pranešimo formatas	463
7.1.3.	Parametrų apibrėžimas	464
8.	Duomenų įrašų formatai	465
8.1.	Siunčiamų parametrų grupės	465
8.2.	dataRecords formatai	466

1. ĮVADAS

Šiame priedėlyje aprašyta, kaip vyksta keitimasis duomenimis tarp transporto priemonės bloko ir testerio per K liniją, kuri yra 6 priedėlyje aprašytos kalibravimo sąsajos dalis. Čia taip pat aprašytas įvesties ir išvesties signalo linijos kalibravimo jungtyje valdymas.

Kaip užmezgamas ryšys per K liniją aprašyta 4 skyriuje „Ryšio paslaugos“.

Šiame priedėlyje K linijos valdymo taikymo sritį įvairiomis sąlygomis apibrėžia diagnostinių „seansų“ sąvoka. Numatytasis seansas yra **StandardDiagnosticSession**, kurio metu iš transporto priemonės bloko galima nuskaityti visus duomenis, tačiau nieko negalima į jį įrašyti.

Kaip diagnostikos seansai pasirenkami, aprašyta 5 skyriuje „Valdymo paslaugos“.

CPR_001 Seanso **ECUProgrammingSession** metu galima rašyti duomenis į transporto priemonės bloką. Norint įvesti duomenis apie kalibravimą (097 ir 098 reikalavimai), transporto priemonės blokas turi veikti KALIBRAVIMO režimu.

Kaip duomenys perduodami per K liniją, aprašyta 6 skyriuje „Duomenų perdavimo paslaugos“. Perduodamų duomenų formatai išsamiai aprašyti 8 skyriuje „Duomenų įrašų formatai“.

CPR_002 Seanso **ECUAdjustmentSession** metu per K linijos sąsają galima pasirinkti kalibravimo I/O signalo linijos I/O režimą. Kalibravimo I/O signalo valdymas aprašytas 7 skyriuje „Bandomųjų impulsų valdymas. Įvesties ir išvesties valdymo funkcinis blokas“.

CPR_003 Šiame dokumente testerio adresas žymimas „tt“. Nors testerių adresai gali būti privilegijuoti, TPB turi teisingai atsakyti į bet kokį testerio adresą. TPB fizinis adresas yra 0xEE.

2. TERMINAI, APIBRĖŽIMAI IR NUORODOS

Protokoliai, pranešimai ir klaidų kodai daugiausia remiasi naujausiu ISO 14229-1 projektu („Kelių transporto priemonės. Diagnostikos sistemos. 1 dalis. Diagnostikos paslaugos“. 2001 m. vasario 22 d. 6 versija).

Paslaugų vardams, paslaugų pareikalavimams bei atsakymams ir standartiniams parametrų naudojami baitų kodavimas ir šešiolyktainės vertės.

Terminas „testeris“ reiškia įrangą, naudojamą programavimo (kalibravimo) duomenims įvesti į TPB.

Terminai „klientas“ ir „tarnybinė stotis“ atitinkamai reiškia testerį ir TPB.

Terminas EVB reiškia „elektroninį valdymo bloką“ ir žymi TPB.

Nuorodos:

ISO 14230-2: Kelių transporto priemonės. Diagnostikos sistemos. Raktažodžių protokolas 2000. 2 dalis. Duomenų perdavimo kanalo sluoksnis. Pirmasis leidimas, 1999 m. Transporto priemonės. Diagnostikos sistemos.

3. PASLAUGŲ APŽVALGA

3.1. Galimos paslaugos

Toliau esančioje lentelėje nurodytos paslaugos, kurias teikia tachografas ir kurios apibrėžtos šiame dokumente.

CPR_004 Lentelėje nurodytos paslaugos, kuriomis galima naudotis pradėjus diagnostikos seansą:

- pirmoje skiltyje išvardytos galimos paslaugos,
- antroje skiltyje nurodytas šio priedėlio skyriaus, kuriame paslauga aprašyta išsamiau, numeris,

- trečioje skiltyje nurodytos pareikalavimo pranešimų paslaugos vardo vertės,
- ketvirtoje skiltyje nurodytos **StandardDiagnosticSession** (SD) paslaugos, kurios turi būti įdiegtos kiekviename TPB,
- penktoje skiltyje nurodytos **ECUAdjustmentSession** (ECUAS) paslaugos, kurios turi būti įdiegtos, kad I/O signalo liniją būtų galima kontroliuoti TPB priekinėje plokštelėje esančia kalibravimo jungtimi,
- šeštoje skiltyje nurodytos **ECUProgrammingSession** (ECUPS) paslaugos, kurios turi būti įdiegtos, kad būtų galima programuoti TPB parametrus.

1 lentelė

Paslaugų vardų verčių lentelė

Diagnosticos paslaugos pavadinimas	Segmento Nr.	SID Req. Vertė	Diagnosticos seansai		
			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		■	

■ Šis simbolis reiškia, kad paslauga yra privaloma diagnostikos seansui.
Kai simbolio nėra pateikta, reiškia, kad ši paslauga diagnostikos seansui neleistina.

3.2. Atsakymo kodai

Kiekvienai paslaugai nustatyti atsakymo kodai.

4. RYŠIO PASLAUGOS

Kai kurios paslaugos reikalingos pagrindiniam ryšiui užmegzti. Jų nematyti programos sluoksnyje. Galimos paslaugos nurodytos toliau esančioje lentelėje:

2 lentelė

Ryšio paslaugos

Paslaugos pavadinimas	Aprašymas
StartCommunication	Klientas reikalauja pradėti ryšio su tarnybine stotimi (stotimis) seansą
StopCommunication	Klientas reikalauja nutraukti esamą ryšio seansą
TesterPresent	Klientas nurodo tarnybinei stotčiai, kad vis dar tebėra

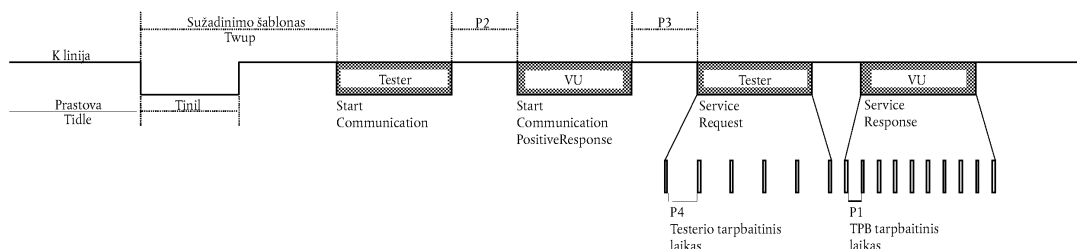
CPR_005 Paslauga **StartCommunication** naudojama ryšiui užmegzti. Norint, kad paslauga būtų atliekama, reikia užmegzti ryšį, o ryšio parametrai turi atitikti pageidaujamą režimą.

4.1. Paslauga „StartCommunication“ [pradėti ryšį]

CPR_006 Gavęs nurodomąjį bazinį elementą **StartCommunication**, TPB turi patikrinti, ar reikalaujamas ryšys gali būti užmegztas esamomis sąlygomis. Ryšiui užmegzti tinkamos sąlygos aprašytos dokumente ISO 14230-2.

CPR_007 Tuomet TPB turi atlikti visus veiksmus, kurių reikia ryšiui užmegzti ir išsiųsti atsakomąjį bazinį elementą **StartCommunication** su parinktais teigiamo atsakymo parametrais.

- CPR_008 Jei jau inicijuotas (ir pradėjęs diagnostikos seansą) TPB gauna naują pareikalavimą **StartCommunication** (pvz., dėl klaidos ištaisymo testeryje), tas pareikalavimas turi būti priimtas, o TPB inicijuotas iš naujo.
- CPR_009 Jei dėl kokios nors priežasties ryšio pradėti negalima, TPB turi toliau vykdyti funkcijas, kurias jis atliko prieš pat bandymą užmegzti ryšį.
- CPR_010 Pranešimas **StartCommunication** turi būti fiziškai adresuotas.
- CPR_011 TPB paslaugos inicijuojamos taikant „greitojo inicijavimo“ metodą:
- prieš bet kurią veiklą yra prastovos laikas,
 - tuomet testeris išsiunčia inicijavimo šabloną,
 - TPB atsakyme pateikiama visa informacija, reikalinga ryšiui užmegzti.
- CPR_012 Pasibaigus inicijavimui:
- pagal raktinius baitus nustatomos 4 lentelėje nurodytos visų ryšio parametrų vertės,
 - TPB laukia testerio pirmojo pareikalavimo,
 - TPB veikia numatytuoju diagnostikos režimu, t. y. **StandardDiagnosticSession**,
 - kalibravimo I/O signalo linija yra numatytosios būsenos, t. y. dezaktyvuota.
- CPR_014 Duomenų perdavimo sparta K linijoje turi būti 10 400 bodų.
- CPR_016 Greitasis inicijavimas prasideda, kai testeris nusiunčia į K liniją sužadinimo šabloną (Wup). Šablonas prasideda po prastovos laiko K linijoje žemuoju laiku **Tinil**. Testeris siunčia pirmąjį paslaugos **StartCommunication** bitą po pirmojo nuolydžio praėjus laikui **Twup**.



- CPR_017 Greitojo inicijavimo ir ryšio bendrai sinchronizavimo vertės nurodytos toliau pateikiamose lentelėse. Prastovos trukmė gali būti įvairi:
- pirmasis siuntimas po maitinimo įjungimo, $T_{\text{prastovos}} = 300 \text{ ms}$,
 - užbaigus paslaugą **StopCommunication**, $T_{\text{prastovos}} = P3 \text{ min.}$,
 - nutraukus ryšį dėl to, kad baigėsi skirtas laikas $P3_{\text{max}}$, $T_{\text{prastovos}} = 0$.

3 lentelė

Greitojo inicijavimo sinchronizavimo vertės

Parametras	Mažiausia vertė	Didžiausia vertė
Tinil	$25 \pm 1 \text{ ms}$	24 ms
Twup	$50 \pm 1 \text{ ms}$	49 ms

4 lentelė

Ryšio sinchronizavimo vertės

Sinchronizavimo parametras	Parametro aprašymas	Apatinės ribos vertės (ms)	Viršutinės ribos vertės (ms)
		mažiausia	didžiausia
P1	Tarpbaitinis laikas TPB atsakymui	0	20
P2	Laikas tarp testerio pareikalavimo ir TPB atsakymo arba dviejų TPB atsakymų	25	250
P3	Laikas tarp TPB atsakymų pabaigos ir testerio naujo pareikalavimo pradžios	55	5 000
P4	Tarpbaitinis laikas testerio pareikalavimui	5	20

CPR_018 Greitojo inicijavimo pranešimų formatas nurodytas toliau pateikiamose lentelėse:

5 lentelė

Pranešimas „StartCommunication request“

Baito Nr.	Parametro aprašymas	Šešiolyktainė vertė	Mnemoninis žymuo
1	Formato baitas – fizinis adresas	81	FMT
2	Paskirties adreso baitas	EE	TGT
3	Šaltinio adreso baitas	tt	SRC
4	Paslaugos StartCommunication request identifikacija	81	SCR
5	Kontrolinė suma	00-FF	CS

6 lentelė

Pranešimas „StartCommunication positive response“

Baito Nr.	Parametro aprašymas	Šešiolyktainė vertė	Mnemoninis žymuo
1	Formato baitas – fizinis adresas	80	FMT
2	Paskirties adreso baitas	tt	TGT
3	Šaltinio adreso baitas	EE	SRC
4	Papildomas ilgio baitas	03	LEN
5	Paslaugos StartCommunication positive response identifikacija	C1	SCRPR
6	Rakto baitas Nr. 1	EA	KB1
7	Rakto baitas Nr. 2	8F	KB2
8	Kontrolinė suma	00-FF	CS

CPR_019 Neigiamo atsakymo į pranešimą **StartCommunication request** nėra – jei teigiamo atsakymo pranešimo išsiųsti negalima, kai TPB nėra inicijuotas, niekas nesiunčiama ir TPB veikia įprastu režimu.

4.2. Paslauga „StopCommunication“ [nutraukti ryšį]

4.2.1. Pranešimo aprašymas

Šios ryšio sluoksnio paslaugos paskirtis – nutraukti ryšio seansą.

CPR_020 Gavęs nurodomąjį bazinį elementą **StopCommunication**, TPB turi patikrinti, ar esamomis sąlygomis galima nutraukti ryšį. Jei taip, TPB turi atlikti visus veiksmus, kurių reikia ryšiui nutraukti.

CPR_021 Jei ryšį nutraukti įmanoma, TPB turi išsiųsti atsakomąjį bazinį elementą **StopCommunication** su parinktais teigiamo atsakymo parametrais ir tuomet nutraukti ryšį.

CPR_022 Jei ryšio dėl kokios nors priežasties nutraukti negalima, TPB turi siųsti atsakomąjį bazinį elementą **StopCommunication** su pasirinktu neigiamo atsakymo parametru.

CPR_023 Jei TPB aptinka, kad baigėsi P3max laikas, ryšys nutraukiamas nesiunčiant atsakomojo bazinio elemento.

4.2.2. Pranešimo formatai

CPR_024 Bazinių elementų **StopCommunication** pranešimo formatai nurodyti toliau pateikiamose lentelėse:

7 lentelė

Pranešimas „StopCommunication request“

Baito Nr.	Parametro aprašymas	Šešiolyktainė vertė	Mnemoninis žymuo
1	Formato baitas – fizinis adresas	80	FMT
2	Paskirties adreso baitas	EE	TGT
3	Šaltinio adreso baitas	tt	SRC
4	Papildomas ilgio baitas	01	LEN
5	Paslaugos StopCommunication request identifikacija	82	SPR
6	Kontrolinė suma	00-FF	CS

8 lentelė

Pranešimas „StopCommunication positive response“

Baito Nr.	Parametro aprašymas	Šešiolyktainė vertė	Mnemoninis žymuo
1	Formato baitas – fizinis adresas	80	FMT
2	Paskirties adreso baitas	tt	TGT
3	Šaltinio adreso baitas	EE	SRC
4	Papildomas ilgio baitas	01	LEN
5	Paslaugos StopCommunication positive response identifikacija	C2	SPRPR
6	Kontrolinė suma	00-FF	CS

9 lentelė

Pranešimas „StopCommunication negative response“

Baito Nr.	Parametro aprašymas	Šešiolyktainė vertė	Mnemoninis žymuo
1	Formato baitas – fizinis adresas	80	FMT
2	Paskirties adreso baitas	tt	TGT
3	Šaltinio adreso baitas	EE	SRC
4	Papildomas ilgio baitas	03	LEN
5	Neigiamo atsakymo paslaugos identifikacija	7F	NR
6	Paslaugos StopCommunication request identifikacija	82	SPR
7	responseCode = generalReject	10	RC_GR
8	Kontrolinė suma	00-FF	CS

4.2.3. Parametrų apibrėžimas

Šiai paslaugai parametrų apibrėžti nereikia.

4.3. Paslauga „TesterPresent“ [testeris yra]

4.3.1. Pranešimo aprašymas

Paslaugą **TesterPresent** testeris naudoja tarnybinei stočiai nurodyti, kad jis dar tebėra, ir kad stotis automatiškai vėl neimtų veikti įprastu režimu ir nenutrauktų ryšio. Ši periodiškai siunčiama paslauga išlaiko aktyvų diagnostikos seansą (ryšį) grąžindama P3 matuoklį į nulį kiekvienąsyk, kai gaunamas šios paslaugos pareikalavimas.

4.3.2. Pranešimo formatas

CPR_079 Bazinių elementų **TesterPresent** pranešimo formatai nurodyti toliau pateikiamose lentelėse.

10 lentelė

Pranešimas „TesterPresent request“

Baito Nr.	Parametro aprašymas	Šešiolyktainė vertė	Mnemoninis žymuo
1	Formato baitas – fizinis adresas	80	FMT
2	Paskirties adreso baitas	EE	TGT
3	Šaltinio adreso baitas	tt	SRC
4	Papildomas ilgio baitas	02	LEN
5	Paslaugos TesterPresent request identifikacija	3E	TP
6	SubFunction = responseRequired = [yes no]	01	RESPREQ_Y
		02	RESPREQ_NO
7	Kontrolinė suma	00-FF	CS

CPR_080 Jei parametras **responseRequired** nustatytas į „yes“, tuomet tarnybinė stotis turi atsakyti toliau nurodytu teigiamo atsakymo pranešimu. Jei nustatyta „no“, tarnybinė stotis atsakymo nesiunčia.

11 lentelė

Pranešimas „TesterPresent positive response“

Baito Nr.	Parametro aprašymas	Šešiolyktainė vertė	Mnemoninis žymuo
1	Formato baitas – fizinis adresas	80	FMT
2	Paskirties adreso baitas	tt	TGT
3	Šaltinio adreso baitas	EE	SRC
4	Papildomas ilgio baitas	01	LEN
5	Paslaugos TesterPresent positive response identifikacija	7E	TPPR
6	Kontrolinė suma	00-FF	CS

CPR_081 Tarnybinė stotis turi gebėti naudoti tokius neigiamų atsakymų kodus:

12 lentelė

Pranešimas „StopCommunication negative response“

Baito Nr.	Parametro aprašymas	Šešiolyktinė vertė	Mnemoninis žymuo
1	Formato baitas – fizinis adresas	80	FMT
2	Paskirties adreso baitas	tt	TGT
3	Šaltinio adreso baitas	EE	SRC
4	Papildomas ilgio baitas	03	LEN
5	Neigiamo atsakymo paslaugos identifikacija	7F	NR
6	Paslaugos TesterPresent request identifikacija	3E	TP
7	responseCode = [SubFunctionNotSupported-InvalidFormat incorrectMessageLength]	12	RC_SFNS_IF
		13	RC_IML
8	Kontrolinė suma	00-FF	CS

5. VALDYMO PASLAUGOS

Galimos paslaugos nurodytos toliau esančioje lentelėje:

13 lentelė

Valdymo paslaugos

Paslaugos pavadinimas	Aprašymas
StartDiagnosticSession	Klientas reikalauja pradėti diagnostikos seansą su TPB
SecurityAccess	Klientas reikalauja prieigos prie funkcijų, kuriomis leista naudotis tik įgaliojtiems naudotojams

5.1. Paslauga „StartDiagnosticSession“ [pradėti diagnostikos seansą]

5.1.1. Pranešimo aprašymas

CPR_025 Paslauga **StartDiagnosticSession** naudojama įvairiems diagnostikos seansams pradėti tarnybinėje stotyje. Diagnostikos seanso metu aktyvuojamas specialių paslaugų rinkinys, kaip nurodyta 17 lentelėje. Gali būti aktyvuojamos transporto priemonės gamintojo nustatytos paslaugos, kurios šiame dokumente neaprašytos. Taikymo taisyklės turi atitikti tokius reikalavimus:

- TPB visuomet turi būti aktyvus tiksliai vienas diagnostikos seansas,
- įjungus TPB maitinimą, jis visuomet turi pradėti seansą **StartDiagnosticSession**. Jei kiti diagnostikos seansai nepradedami, tuomet **StartDiagnosticSession** turi veikti tol, kol TPB būna įjungtas,
- jei testeris pareikalauja jau vykstančio diagnostikos seanso, tuomet TPB turi išsiųsti teigiamo atsakymo pranešimą,
- kai testeris pareikalauja naujo diagnostikos seanso, TPB iš pradžių turi išsiųsti pranešimą **StartDiagnosticSession positive response** ir tik po to pradėti naują seansą. Jei TPB negali pradėti pareikalauto naujo seanso, tuomet jis turi išsiųsti pranešimą **StartDiagnosticSession negative response** ir tęsti esamąjį.

CPR_026 Diagnostikos seansas turi būti pradedamas tik tuomet, jei tarp kliento ir TPB užmegztas ryšys.

CPR_027 Sėkmingai pradėjus paslaugą **StartDiagnosticSession**, turi galioti 4 lentelėje nustatyti sinchronizavimo parametrai, o jei anksčiau vyko kitas diagnostikos seansas, parametras **diagnosticSession** turi būti nustatytas į **StandardDiagnosticSession**.

5.1.2. *Pranešimo formatas*

CPR_028 Bazinių elementų **StartDiagnosticSession** pranešimo formatai nurodyti toliau pateikiamose lentelėse:

14 lentelė

Pranešimas „StartDiagnosticSession request“

Baito Nr.	Parametro aprašymas	Šešiolyktainė vertė	Mnemoninis žymuo
1	Formato baitas – fizinis adresas	80	FMT
2	Paskirties adreso baitas	EE	TGT
3	Šaltinio adreso baitas	tt	SRC
4	Papildomas ilgio baitas	02	LEN
5	Paslaugos StartDiagnosticSession request identifikacija	10	STDS
6	diagnosticSession = (viena iš 17 lentelėje nurodytų verčių)	xx	DS_...
7	Kontrolinė suma	00-FF	CS

15 lentelė

Pranešimas „StartDiagnosticSession positive response“

Baito Nr.	Parametro aprašymas	Šešiolyktainė vertė	Mnemoninis žymuo
1	Formato baitas – fizinis adresas	80	FMT
2	Paskirties adreso baitas	tt	TGT
3	Šaltinio adreso baitas	EE	SRC
4	Papildomas ilgio baitas	02	LEN
5	Paslaugos StartDiagnosticSession positive response identifikacija	50	STDSPR
6	diagnosticSession = (ta pati vertė, kaip ir 6 baito 14 lentelėje)	xx	DS_...
7	Kontrolinė suma	00-FF	CS

16 lentelė

Pranešimas „StartDiagnosticSession negative response“

Baito Nr.	Parametro aprašymas	Šešiolyktainė vertė	Mnemoninis žymuo
1	Formato baitas – fizinis adresas	80	FMT
2	Paskirties adreso baitas	tt	TGT
3	Šaltinio adreso baitas	EE	SRC
4	Papildomas ilgio baitas	03	LEN
5	Neigiamo atsakymo paslaugos identifikacija	7F	NR
6	Paslaugos StartDiagnosticSession request identifikacija	10	STDS
7	ResponseCode = (subFunctionNotSupported ^(a))	12	RC_SFNS
	incorrectMessageLength ^(b)	13	RC_IML
	conditionsNotCorrect ^(c)	22	RC_CNC
8	Kontrolinė suma	00-FF	CS

^(a) Pareikalavimo pranešimo 6 baite įrašyta vertė netinkama, t. y. ji nenurodyta 17 lentelėje.

^(b) Pranešimo ilgis netinkamas.

^(c) Nesilaikyta pareikalavimo **StartDiagnosticSession** kriterijų.

5.1.3. *Parametrų apibrėžimas*

CPR_029 Parametrą **diagnosticSession (DS_)** paslauga **StartDiagnosticSession** naudoja tam tikram tarnybinės (-ių) stoties (-čių) veikimo būdai pasirinkti. Šiame dokumente nustatyti tokie diagnostikos seansai:

17 lentelė

„diagnosticSession“ verčių apibrėžimas

Šešiolyk-tainė vertė	Aprašymas	Mnemoninis žymuo
81	StandardDiagnosticSession Per šį diagnostikos seansą galima naudoti visas 1 lentelės 4 skiltyje (SD) pažymėtas paslaugas. Šios paslaugos leidžia nuskaityti iš tarnybinės stoties (TPB) visus duomenis. Šis diagnostikos seansas veikia sėkmingai atlikus inicijavimą tarp kliento (testerio) ir tarnybinės stoties (TPB). Šį diagnostikos seansą gali pakeisti kiti šiame skyriuje nurodyti diagnostikos seansai.	SD
85	ECUProgrammingSession Per šį diagnostikos seansą galima naudoti visas 1 lentelės 6 skiltyje (ECUPS) pažymėtas paslaugas. Šios paslaugos leidžia programuoti tarnybinės stoties (TPB) atmintį. Šį diagnostikos seansą gali pakeisti kiti šiame skyriuje nurodyti diagnostikos seansai.	ECUPS
87	ECUAdjustmentSession Per šį diagnostikos seansą galima naudoti visas 1 lentelės 5 skiltyje (ECUAS) pažymėtas paslaugas. Šios paslaugos leidžia valdyti tarnybinės stoties (TPB) įvestį ir išvestį. Šį diagnostikos seansą gali pakeisti kiti šiame skyriuje nurodyti diagnostikos seansai.	ECUAS

5.2. Paslauga „SecurityAccess“ [apsauginė prieiga]

Jei TPB veikia ne KALIBRAVIMO režimu, neišmanoma įrašyti duomenų apie kalibravimą arba prieiti prie įvesties ir išvesties linijos. Įkišus į TPB galiojančią dirbtuvių kortelę dar reikia įvesti atitinkamą PIN ir tik tuomet suteikiama galimybė naudotis KALIBRAVIMO režimu.

Paslauga **SecurityAccess** suteikia galimybę įvesti PIN ir nurodyti testerui, ar TPB veikia KALIBRAVIMO režimu, ar ne.

PIN leidžiama įvesti ir kitais būdais.

5.2.1. *Pranešimo aprašymas*

Paslaugą **SecurityAccess** sudaro pranešimas **requestSeed** [pareikalauti „seed“], po kurio gali būti siunčiamas pranešimas **sendKey** [atsiųsti raktą]. Paslauga **SecurityAccess** turi būti suteikiama po paslaugos **StartDiagnosticSession**.

CPR_033 Testeris turi apsauginės prieigos pranešimu **requestSeed** patikrinti, ar transporto priemonės blokas yra pasirengęs priimti PIN.

CPR_034 Jei transporto priemonės blokas jau veikia KALIBRAVIMO režimu, jis turi atsakyti į pareikalavimą pasinaudodamas teigiamu atsakymu į paslaugą **SecurityAccess** ir išsiųsdamas „seed“, lygų 0x0000.

CPR_035 Jei transporto priemonės blokas pasirengęs priimti PIN, kad jį patikrintų dirbtuvių kortelė, jis turi atsakyti į pareikalavimą pasinaudodamas teigiamu atsakymu į paslaugą **SecurityAccess** ir išsiųsdamas „seed“, didesnę kaip 0x0000.

CPR_036 Jei transporto priemonės blokas nepasirengęs priimti PIN iš testerio dėl to, kad įkišta dirbtuvių kortelė negalioja, ji neįkišta arba transporto priemonės blokas tikisi, kad PIN bus įvestas kitu būdu, jis turi atsakyti į pareikalavimą neigiamu atsakymu pranešimu, kuriame nustatytas atsakymo kodas **conditionsNotCorrectOrRequestSequenceError** [sąlygų netinkamumo arba pareikalavimo sekos klaida].

CPR_037 Tuomet testeris naudodamasis apsauginės prieigos pranešimu **sendKey** turi nusiųsti transporto priemonės blokui PIN. Tam, kad galėtų būti atlikta kortelės autentiškumo tikrinimo procedūra, TPB turi naudoti neigiamo atsakymo kodą **requestCorrectlyReceived-ResponsePending** [pareikalavimas gautas tinkamai – laukiama atsakymo] atsakymo laikui pratęsti. Tačiau tas laikas negali trukti ilgiau kaip 5 minutes. Kai tik pareikalauta paslauga užbaigiama, TPB turi išsiųsti teigiamo arba neigiamo atsakymo pranešimą, kurio kodas skiriasi nuo nurodytojo. Neigiamo atsakymo kodą **requestCorrectlyReceived-ResponsePending** TPB gali kartoti tol, kol reikalaujamoji paslauga užbaigiama ir išsiunčiamas galutinio atsakymo pranešimas.

CPR_038 Transporto priemonės blokas turi atsakyti į šį pareikalavimą teigiamu atsakymu į paslaugą SecurityAccess tik veikdamas KALIBRAVIMO režimu.

CPR_039 Toliau nurodytais atvejais transporto priemonės blokas turi išsiųsti neigiamą atsakymą su tokiais atsakymo kodais:

- **subFunctionNot supported:** netinkamas subfunkcijos parametro formatas (accessType),
- **conditionsNotCorrectOrRequestSequenceError:** transporto priemonės blokas nepasirengęs priimti įvedamo PIN,
- **invalidKey:** PIN netinkamas, leidžiamų PIN patikrinimų skaičius neviršytas,
- **exceededNumberOfAttempts:** PIN netinkamas ir viršytas leidžiamų PIN patikrinimų skaičius,
- **generalReject:** PIN teisingas, tačiau nepavyko abipusio autentiškumo tikrinimo su dirbtuvių kortele procedūra.

5.2.2. Pranešimo formatas. „SecurityAccess“. „requestSeed“

CPR_040 Bazinių elementų SecurityAccess requestSeed pranešimo formatai nurodyti toliau pateikiamose lentelėse:

18 lentelė

Pranešimas „SecurityAccess request – requestSeed“

Baito Nr.	Parametro aprašymas	Šešiolyktainė vertė	Mnemoninis žymuo
1	Formitum-bijt – fizikai čkmzės	80	FMT
2	Paskirties adreso baitas	EE	TGT
3	Šaltinio adreso baitas	tt	SRC
4	Papildomas ilgio baitas	02	LEN
5	Paslaugos SecurityAccess request identifikacija	27	SA
6	accessType – requestSeed	7D	AT_RSD
7	Kontrolinė suma	00-FF	CS

19 lentelė

Pranešimas „SecurityAccess – requestSeed positive response“

Baito Nr.	Parametro aprašymas	Šešiolyktainė vertė	Mnemoninis žymuo
1	Formitum-bijt – fizikai čkmzės	80	FMT
2	Paskirties adreso baitas	tt	TGT
3	Šaltinio adreso baitas	EE	SRC
4	Papildomas ilgio baitas	04	LEN
5	Paslaugos SecurityAccess positive response identifikacija	67	SAPR
6	accessType – requestSeed	7D	AT_RSD
7	Seed High	00-FF	SEEDH
8	Seed Low	00-FF	SEEDL
9	Kontrolinė suma	00-FF	CS

20 lentelė

Pranešimas „SecurityAccess negative response“

Baito Nr.	Parametro aprašymas	Šešiolyktainė vertė	Mnemoninis žymuo
1	Formitum-bijt – fizikai čkmzés	80	FMT
2	Paskirties adreso baitas	tt	TGT
3	Šaltinio adreso baitas	EE	SRC
4	Papildomas ilgio baitas	03	LEN
5	Neigiamo atsakymo paslaugos identifikacija	7F	NR
6	Paslaugos SecurityAccess request identifikacija	27	SA
7	responseCode = (conditionsNotCorrectOrRequestSequenceError incorrectMessageLength)	22	RC_CNC
		13	RC_IML
8	Kontrolinė suma	00-FF	CS

5.2.3. Pranešimo formatai. „SecurityAccess“. „sendKey“

CPR_041 Bazinių elementų **SecurityAccess sendKey** pranešimo formatai nurodyti toliau pateikiamose lentelėse:

21 lentelė

Pranešimas „SecurityAccess request – sendKey“

Baito Nr.	Parametro aprašymas	Šešiolyktainė vertė	Mnemoninis žymuo
1	Formato baitas – fizinis adresas	80	FMT
2	Paskirties adreso baitas	EE	TGT
3	Šaltinio adreso baitas	tt	SRC
4	Papildomas ilgio baitas	m+2	LEN
5	Paslaugos SecurityAccess request identifikacija	27	SA
6	accessType – sendKey	7E	AT_SK
nuo 7 iki (m+6)	Raktas #1 (High)	xx	KEY
	...	...	
	Raktas #m (low , m turi būti nuo 4 iki 8)	xx	
m+7	Kontrolinė suma	00-FF	CS

22 lentelė

Pranešimas „SecurityAccess – sendKey positive response“

Baito Nr.	Parametro aprašymas	Šešiolyktainė vertė	Mnemoninis žymuo
1	Formato baitas – fizinis adresas	80	FMT
2	Paskirties adreso baitas	tt	TGT
3	Šaltinio adreso baitas	EE	SRC
4	Papildomas ilgio baitas	02	LEN
5	Paslaugos SecurityAccess positive response identifikacija	67	SAPR
6	accessType – sendKey	7E	AT_SK
7	Kontrolinė suma	00-FF	CS

23 lentelė

Pranešimas „SecurityAccess negative response“

Baito Nr.	Parametro aprašymas	Šešiolyktainė vertė	Mnemoninis žymuo
1	Formato baitas – fizinis adresas	80	FMT
2	Paskirties adreso baitas	tt	TGT
3	Šaltinio adreso baitas	EE	SRC
4	Papildomas ilgio baitas	03	LEN
5	Neigiamo atsakymo paslaugos identifikacija	7F	NR
6	Paslaugos SecurityAccess request identifikacija	27	SA
7	ResponseCode = (generalReject	10	RC_GR
	subFunctionNotSupported	12	RC_SFNS
	incorrectMessageLength	13	RC_IML
	conditionsNotCorrectOrRequestSequenceError	22	RC_CNC
	invalidKey	35	RC_IK
	exceededNumberOfAttempts	36	RC_ENA
	requestCorrectlyReceived-ResponsePending)	78	RC_RCR_RP
8	Kontrolinė suma	00-FF	CS

6. DUOMENŲ PERDAVIMO PASLAUGOS

Galimos paslaugos nurodytos toliau esančioje lentelėje:

24 lentelė

Valdymo paslaugos

Paslaugos pavadinimas	Aprašymas
ReadDataByIdentifier	Klientas reikalauja persiųsti esamą įrašo, pasiekiamo su recordDataIdentifier [įrašo duomenų vardas], vertę
WriteDataByIdentifier	Klientas reikalauja įrašyti įrašą, pasiekiamą su recordDataIdentifier

6.1. Paslauga „ReadDataByIdentifier“ [nuskaityti duomenis pagal vardą]

6.1.1. Pranešimo aprašymas

CPR_050 Paslaugą **ReadDataByIdentifier** klientas naudoja reikalauti duomenų įrašų vertėms iš tarnybinės stoties. Duomenys identifikuojami pagal **recordDataIdentifier**. TPB gamintojas atsako už tai, kad atliekant šią paslaugą būtų laikomasi tarnybinės stoties reikalavimų.

6.1.2. Pranešimo formatas

CPR_051 Bazinių elementų **ReadDataByIdentifier** pranešimo formatai nurodyti toliau pateikiamose lentelėse:

25 lentelė

Pranešimas „ReadDataByIdentifier request“

Baito Nr.	Parametro aprašymas	Šešiolyktainė vertė	Mnemoninis žymuo
1	Formato baitas – fizinis adresas	80	FMT
2	Paskirties adreso baitas	EE	TGT
3	Šaltinio adreso baitas	tt	SRC
4	Papildomas ilgio baitas	03	LEN
5	Paslaugos ReadDataByIdentifier request identifikacija	22	RDBI
6 ir 7	recordDataIdentifier = (viena iš 28 lentelėje nurodytų verčių)	xxxx	RDI_...
8	Kontrolinė suma	00-FF	CS

26 lentelė

Pranešimas „ReadDataByIdentifier positive response“

Baito Nr.	Parametro aprašymas	Šešiolyktainė vertė	Mnemoninis žymuo
1	Formato baitas – fizinis adresas	80	FMT
2	Paskirties adreso baitas	tt	TGT
3	Šaltinio adreso baitas	EE	SRC
4	Papildomas ilgio baitas	m+3	LEN
5	Paslaugos ReadDataByIdentifier positive response identifikacija	62	RDBIPR
6 ir 7	recordDataIdentifier = (ta pati vertė, kaip ir 6 bei 7 baitų 25 lentelėje)	xxxx	RDI_...
nuo 8 iki (m+7)	dataRecord() = (duomenys #1 : duomenys #m)	xx : xx	DREC_DATA1 : DREC_DATAm
m+8	Kontrolinė suma	00-FF	CS

27 lentelė

Pranešimas „ReadDataByIdentifier negative response“

Baito Nr.	Parametro aprašymas	Šešiolyktainė vertė	Mnemoninis žymuo
1	Formato baitas – fizinis adresas	80	FMT
2	Paskirties adreso baitas	tt	TGT
3	Šaltinio adreso baitas	EE	SRC
4	Papildomas ilgio baitas	03	LEN
5	Neigiamo atsakymo paslaugos identifikacija	7F	NR
6	Paslaugos ReadDataByIdentifier request identifikacija	22	RDBI
7	ResponseCode = (requestOutOfRange incorrectMessageLength conditionsNotCorrect)	31 13 22	RC_ROOR RC_IML RC_CNC
8	Kontrolinė suma	00-FF	CS

6.1.3. Parametrų apibrėžimas

CPR_052 Parametras **recordDataIdentifier** (RDI_) pranešime **ReadDataByIdentifier** request identifikuoja duomenų įrašą.

CPR_053 Šiame dokumente nustatytos **recordDataIdentifier** vertės pateiktos toliau esančioje lentelėje.

recordDataIdentifier lentelę sudaro keturios skiltys:

- pirmoje skiltyje (hex) pateiktos trečioje skiltyje nurodyto **recordDataIdentifier** šešiolyktainės vertės,
- antroje skiltyje (duomenų elementas) nurodytas duomenų elementas pagal 1 priedėlį, kuriuo paremtas **recordDataIdentifier** (kartais reikia perkoduoti),
- trečioje skiltyje (aprašymas) nurodytas atitinkamo **recordDataIdentifier** pavadinimas,
- ketvirtoje skiltyje (mnemoninis žymuo) nurodytas šio **recordDataIdentifier** mnemoninis žymuo.

28 lentelė

„recordDataIdentifier“ verčių apibrėžimas

Hex	Duomenų elementas	recordDataIdentifier pavadinimas (žr. formatą 8.2 poskyryje)	Mnemoninis žymuo
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 Parametrą **dataRecord** (DREC_) pranešimas **ReadDataByIdentifier positive response** naudoja suteikti klientui (testeriui) duomenų įrašo vertes, nurodytas vardu **recordDataIdentifier**. Duomenų formatai nurodyti 8 skyriuje. Galima naudoti papildomus parametrus **dataRecord**, skirtus papildomiems naudotojams, įskaitant TPB pritaikytus įvesties, vidinius ir išvesties duomenis, tačiau šiame dokumente jie neaprašyti.

6.2. Paslauga „WriteDataByIdentifier“ [įrašyti duomenis pagal vardą]

6.2.1. Pranešimo aprašymas

CPR_056 Paslaugą **WriteDataByIdentifier** klientas naudoja duomenų įrašų vertėms įrašyti į tarnybinę stotį. Duomenys identifikuojami pagal **recordDataIdentifier**. TPB gamintojas atsako už tai, kad atliekant šią paslaugą būtų laikomasi tarnybinės stoties reikalavimų. Norint atnaujinti 28 lentelėje išvardytus parametrus TPB turi veikti KALIBRAVIMO režimu.

6.2.1. Pranešimo formatai

CPR_057 Bazinių elementų **WriteDataByIdentifier** pranešimo formatai nurodyti toliau pateikiamose lentelėse:

29 lentelė

Pranešimas „WriteDataByIdentifier request“

Baito Nr.	Parametro aprašymas	Šešioktainė vertė	Mnemoninis žymuo
1	Formato baitas – fizinis adresas	80	FMT
2	Paskirties adreso baitas	EE	TGT
3	Šaltinio adreso baitas	tt	SRC
4	Papildomas ilgio baitas	m+3	LEN
5	Paslaugos WriteDataByIdentifier request identifikacija	2E	WDBI
6 ir 7	recordDataIdentifier = (viena iš 28 lentelėje nurodytų verčių)	xxxx	RDI_...
nuo 8 iki (m+7)	dataRecord() = (duomenys #1 : duomenys #m)	xx : xx	DREC_DATA1 : DREC_DATAm
m+8	Kontrolinė suma	00-FF	CS

30 lentelė

Pranešimas „WriteDataByIdentifier positive response“

Baito Nr.	Parametro aprašymas	Šešiolyktainė vertė	Mnemoninis žymuo
1	Formato baitas – fizinis adresas	80	FMT
2	Paskirties adreso baitas	tt	TGT
3	Šaltinio adreso baitas	EE	SRC
4	Papildomas ilgio baitas	03	LEN
5	Paslaugos WriteDataByIdentifier positive response identifikacija	6E	WDBIPR
6 ir 7	recordDataIdentifier = (ta pati vertė, kaip ir 6 bei 7 baitų 29 lentelėje)	xxxx	RDI_...
8	Kontrolinė suma	00-FF	CS

31 lentelė

Pranešimas „WriteDataByIdentifier negative response“

Baito Nr.	Parametro aprašymas	Šešiolyktainė vertė	Mnemoninis žymuo
1	Formato baitas – fizinis adresas	80	FMT
2	Paskirties adreso baitas	tt	TGT
3	Šaltinio adreso baitas	EE	SRC
4	Papildomas ilgio baitas	03	LEN
5	Neigiamo atsakymo paslaugos identifikacija	7F	NR
6	Paslaugos WriteDataByIdentifier request identifikacija	2E	WDBI
7	ResponseCode = (requestOutOfRange incorrectMessageLength conditionsNotCorrect)	31 13 22	RC_ROOR RC_IML RC_CNC
8	Kontrolinė suma	00-FF	CS

6.2.3. Parametrų apibrėžimas

Parametras **recordDataIdentifier** (RDI_) apibrėžtas 28 lentelėje.

Parametrą **dataRecord** (DREC_) pranešimas **WriteDataByIdentifier positive response** naudoja suteikti tarnybinei stočiai (TPB) duomenų įrašo vertes, nurodytas vardu **recordDataIdentifier**. Duomenų formatai nurodyti 8 skyriuje.

7. BANDOMŲJŲ IMPULSŲ VALDYMAS. ĮVESTIES ir IŠVESTIES VALDYMO FUNKCINIS BLOKAS

Galimos paslaugos nurodytos toliau esančioje lentelėje:

32 lentelė

Įvesties ir išvesties valdymo funkcinis blokas

Paslaugos pavadinimas	Aprašymas
InputOutputControlByIdentifier	Klientas reikalauja valdyti tarnybinei stočiai skirtą įvestį ir išvestį.

7.1. Paslauga „InputOutputControlByIdentifier“ [įvesties ir išvesties valdymas pagal vardus]

7.1.1. Pranešimo aprašymas

Priekinėje jungtyje yra sujungimas, per kurį galima kontroliuoti arba stebėti bandymų impulsus naudojant tinkamą testerį.

CPR_058 Ši kalibravimo I/O signalą galima konfigūruoti K linijos komanda, paslauga **InputOutputControlByIdentifier** parenkant linijai reikiamą įvesties arba išvesties funkciją. Galimos tokios linijos būsenos:

- dezaktyvuota,
- **speedSignalInput** [greičio signalo įvestis], kai kalibravimo I/O signalo linija naudojama greičio signalui (bandymų signalui) įvesti, pakeičiant iš judesio jutiklio ateinantį greičio signalą,
- **realTimeSpeedSignalOutputSensor** [greičio signalo išvestis iš jutiklio esamuoju laiku], kai kalibravimo I/O signalo linija naudojama judesio jutiklio greičio signalui išvesti,
- **RTCOutput**, kai kalibravimo I/O signalo linija naudojama UTC laikrodžio signalui išvesti.

CPR_059 Tam, kad būtų galima sukonfigūruoti linijos būseną, transporto priemonės bloke turi būti prasidėjęs reguliavimo seansas ir jis turi veikti KALIBRAVIMO režimu. Baigdamas reguliavimo seansą arba KALIBRAVIMO režimą transporto priemonės blokas turi užtikrinti, kad kalibravimo I/O signalo linija būtų grąžinta į (numatytąją) dezaktyvuotą būseną.

CPR_060 Jei greičio impulsai TPB greičio signalo įvesties esamuoju laiku linijoje priimami tuomet, kai kalibravimo I/O signalo linija nustatyta įvesties režimu, kalibravimo I/O signalo linija turi būti pervesta į išvesties režimą arba grąžinta į dezaktyvuotą būseną.

CPR_061 Seka turi būti tokia:

- naudojantis paslauga **StartCommunication** užmezgamas ryšys,
- naudojantis paslauga **StartDiagnosticSession** pradedamas reguliavimo seansas ir nustatomas KALIBRAVIMO režimas (šių dviejų operacijų eiliškumas nesvarbus),
- naudojantis paslauga **InputOutputControlByIdentifier** pakeičiama išvesties būsena.

7.1.2. Pranešimo formatas

CPR_062 Bazinių elementų **InputOutputControlByIdentifier** pranešimo formatai nurodyti toliau pateikiamose lentelėse:

33 lentelė

Pranešimas „InputOutputControlByIdentifier request“

Baito Nr.	Parametro aprašymas	Šešiolyktainė vertė	Mnemoninis žymuo
1	Formato baitas – fizinis adresas	80	FMT
2	Paskirties adreso baitas	EE	TGT
3	Šaltinio adreso baitas	tt	SRC
4	Papildomas ilgio baitas	xx	LEN
5	Paslaugos InputOutputControlByIdentifier identifikacija	2F	IOCBI
6 ir 7	InputOutputIdentifier = (CalibrationInputOutput)	F960	IOI_CIO
8 arba nuo 8 iki 9	ControlOptionRecord = (inputOutputControlParameter – viena iš 36 lentelės verčių controlState – viena iš 38 lentelės verčių (žr. pastabą žemiau))	xx	COR_...
		xx	IOCP_...
9 arba 10	Kontrolinė suma	00-FF	CS

:Pastaba: parametras **controlState** būna tik kai kuriais atvejais (žr. 7.1.3).

34 lentelė

Pranešimas „InputOutputControlByIdentifier positive response“

Baito Nr.	Parametro aprašymas	Šešiolyktainė vertė	Mnemoninis žymuo
1	Formato baitas – fizinis adresas	80	FMT
2	Paskirties adreso baitas	tt	TGT
3	Šaltinio adreso baitas	EE	SRC
4	Papildomas ilgio baitas	xx	LEN
5	Paslaugos InputOutputControlByIdentifier positive response identifikacija	6F	IOCBIPR
6 ir 7	InputOutputIdentifier = (CalibrationInputOutput)	F960	IOI_CIO
8 arba nuo 8 iki 9	controlStatusRecord() = (inputOutputControlParameter (ta pati vertė, kaip ir 8 baito 33 lentelėje)	xx	CSR_ IOCP_...
	controlState (ta pati vertė, kaip ir 9 baito 33 lentelėje)) (jei taikytina)	xx	CS_...
9 arba 10	Kontrolinė suma	00-FF	CS

35 lentelė

Pranešimas „InputOutputControlByIdentifier negative response“

Baito Nr.	Parametro aprašymas	Šešiolyktainė vertė	Mnemoninis žymuo
1	Formato baitas – fizinis adresas	80	FMT
2	Paskirties adreso baitas	tt	TGT
3	Šaltinio adreso baitas	EE	SRC
4	Papildomas ilgio baitas	03	LEN
5	Neigiamo atsakymo paslaugos identifikacija	7F	NR
6	Paslaugos InputOutputControlByIdentifier request identifikacija	2F	IOCBI
7	responseCode = (incorrectMessageLength	13	RC_IML
	conditionsNotCorrect	22	RC_CNC
	requestOutOfRange	31	RC_ROOR
	deviceControlLimitsExceeded)	7A	RC_DCLE
8	Kontrolinė suma	00-FF	CS

7.1.3. Parametrų apibrėžimas

CPR_064 Parametras **inputOutputControlParameter** (IOCP_) apibrėžtas toliau esančioje lentelėje:

36 lentelė

„inputOutputControlParameter“ verčių apibrėžimas

Šešiolyktainė vertė	Aprašymas	Mnemoninis žymuo
00	ReturnControlToECU Ši vertė turi nurodyti tarnybinei stočiai (TPB), kad testeris daugiau nebevaldo kalibravimo I/O signalo linijos.	RCTECU
01	ResetToDefault Ši vertė turi nurodyti tarnybinei stočiai (TPB), kad reikalaujama grąžinti kalibravimo I/O signalo liniją į jo numatytąją būseną.	RTD
03	ShortTermAdjustment Ši vertė turi nurodyti tarnybinei stočiai (TPB), kad reikalaujama suderinti kalibravimo I/O signalo liniją su verte, nurodyta parametru controlState.	STA

CPR_065 Parametras controlState yra tik tuomet kai parametras inputOutputControlParameter nustatytas į ShortTermAdjustment; jis apibrėžtas toliau esančioje lentelėje:

37 lentelė

„controlState“ verčių apibrėžimas

Režimas	Šešiolyktainė vertė	Aprašymas
Dezaktyvuota	00	I/O linija yra dezaktyvuota (numatytoji būsena)
Aktyvuota	01	Kalibravimo I/O linija aktyvuota režimu speedSignalInput
Aktyvuota	02	Kalibravimo I/O linija aktyvuota režimu realTimeSpeedSignalOutputSensor
Aktyvuota	03	Kalibravimo I/O linija aktyvuota režimu RTCOutput

8. DUOMENŲ ĮRAŠŲ FORMATAI

Skyriuje aprašyta:

- bendrosios taisyklės, kurias reikia taikyti transporto priemonės bloko testerui siunčiamų signalų parametų grupėms,
- formatai, kuriuos reikia naudoti 6 skyriuje aprašytais duomenų perdavimo paslaugomis siunčiamiems duomenims.

CPR_067 Visus nurodytus parametrus turi gebėti naudoti TPB.

CPR_068 TPB atsakant į pareikalavimo pranešimus testerui siunčiami duomenys turi būti išmatuojamojo tipo (t. y. esama reikalaujamo parametro vertė, kurią išmatavo arba nustatė TPB).

8.1. Siunčiamų parametų grupės

CPR_069 38 lentelėje apibrėžtos grupės, naudojamos siunčiamų parametų galiojimui nustatyti.

CPR_070 070 Grupės „klaidos indikatorius“ vertės skirtos tam, kad transporto priemonės blokas galėtų iškart nurodyti, kad galiojantys parametų duomenys šiuo metu neprieinami dėl tam tikros rūšies klaidos tachografe.

CPR_071 071 Grupės „neturima“ vertės skirtos tam, kad transporto priemonės blokas galėtų išsiųsti pranešimą, kuriame yra tame modulyje neturimas arba netinkamas parametras. Grupės „nereikalaujama“ vertės skirtos tam, kad įrenginys galėtų siųsti komandinį pranešimą ir identifikuoti tuos parametrus, kai iš priimančiojo įtaiso nelaukiama atsakymo.

CPR_072 Jei dėl komponento gedimo negalima persiųsti galiojančių parametro duomenų, vietoj tų parametro duomenų turi būti naudojamas klaidos indikatorius, kaip nurodyta 38 lentelėje. Tačiau, jei išmatuoti arba apskaičiuoti duomenys įgavo tokią vertę, kuri yra galiojanti, tačiau nėra pateikta tarp nurodytų parametrų, klaidos indikatorius neturi būti naudojamas. Duomenys turi būti perduodami naudojant atitinkamą mažiausią arba didžiausią parametro vertę.

38 lentelė

„dataRecords“ grupės

Grupės pavadinimas	1 baitas (šešiolyktinė vertė)	2 baitai (šešiolyktinė vertė)	4 baitai (šešiolyktinė vertė)	ASCII
Galiojantis signalas	nuo 00 iki FA	nuo 0000 iki FAFF	nuo 00000000 iki FAFFFFFF	nuo 1 iki 254
Parametrui skirtas indikatorius	FB	nuo FB00 iki FBFF	nuo FB000000 iki FBFFFFFF	nėra
Rezervuota grupė būsimiems indikatoriniams bitams	nuo FC iki FD	nuo FC00 iki FDFF	nuo FC000000 iki FDFFFFFF	nėra
Klaidos indikatorius	FE	nuo FE00 iki FEFF	nuo FE000000 iki FEFFFFFF	0
Neturima arba nereikalinga	FF	nuo FF00 iki FFFF	nuo FF000000 iki FFFFFFFF	FF

CPR_073 ASCII užkoduotiems parametrų ASCII rašmuo „*“ rezervuotas kaip skirtukas.

8.2. dataRecords formatai

Toliau esančiose nuo 40 iki 44 lentelėse nurodyti formatai, kuriuose reikia naudoti su paslaugomis **ReadDataByIdentifier** ir **WriteDataByIdentifier**.

CPR_074 40 lentelėje nurodytas kiekvieno pagal savo **recordDataIdentifier** identifikuojamo parametro ilgis, skiriamoji geba ir naudojimo ribos:

39 lentelė

„dataRecords“ formatai

Parametro pavadinimas	Duomenų ilgis (baitais)	Skiriamoji geba	Naudojimo ribos
TimeDate	8	Daugiau žr. 40 lentelėje	
HighResolutionTotalVehicleDistance	4	5 m/bit paskuba, 0 m paklaida	nuo 0 iki + 21 055 406 km
Kfactor	2	0,001 impulso/m/bit paskuba, paklaida – 0	nuo 0 iki 64,255 impulsų/m
LfactorTyreCircumference	2	$0,125 \times 10^{-3}$ /bit paskuba, paklaida – 0	nuo 0 iki 8 031 m
WvehicleCharacteristicFactor	2	0,001 impulso/m/bit paskuba, paklaida – 0	nuo 0 iki 64,255 impulsų/m
TyreSize	15	ASCII	ASCII
NextCalibrationDate	3	Daugiau žr. 41 lentelėje	
SpeedAuthorised	2	1/256 km/h/bit paskuba, paklaida – 0	nuo 0 iki 250 996 km/h
RegisteringMemberState	3	ASCII	ASCII
VehicleRegistrationNumber	14	Daugiau žr. 44 lentelėje	
TPIN	17	ASCII	ASCII

CPR_075 40 lentelėje nurodyti parametro **TimeDate** įvairių baitų formatai:

40 lentelė

„TimeDate“ išsamus formatas (recordDataIdentifier # F00B)

Baitas	Parametro apibrėžimas	Skiriamoji geba	Naudojimo ribos
1	Sekundės	0,25 s/bit paskuba, 0 s paklaida	nuo 0 iki 59,75 s
2	Minutės	1 min./bit paskuba, 0 min. paklaida	nuo 0 iki 59 min.
3	Valandos	1 h/bit paskuba, 0 h paklaida	nuo 0 iki 23 h
4	Mėnuo	1 mėn./bit paskuba, 0 mėn. paklaida	nuo 1 iki 12 mėnesių
5	Diena	0,25 dienos/bit paskuba, 0 dienų paklaida (žr. pastabą 41 lent.)	nuo 0,25 iki 31,75 dienos
6	Metai	1 metų/bit paskuba, 1985 metų paklaida (žr. pastabą 41 lent.)	nuo 1985 m. iki 2235 m.
7	Minučių vietos laiku paklaida	1 min./bit paskuba, –125 min. paklaida	nuo –59 iki 59 min.
8	Valandų vietos laiku paklaida	1 h/bit paskuba, –125 h paklaida	nuo –23 iki +23 val.

CPR_076 41 lentelėje nurodyti parametro **NextCalibrationDate** įvairių baitų formatai:

41 lentelė

„NextCalibrationDate“ išsamus formatas (recordDataIdentifier # F022)

Baitas	Parametro apibrėžimas	Skiriamoji geba	Naudojimo ribos
1	Mėnuo	1 mėn./bit paskuba, 0 mėn. paklaida	nuo 1 iki 12 mėnesių
2	Diena	0,25 dienos/bit paskuba, 0 dienų paklaida (žr. pastabą)	nuo 0,25 iki 31,75 dienos
3	Metai	1 metų/bit paskuba, +1985 metų paklaida (žr. pastabą)	nuo 1985 m. iki 2235 m.

Pastaba dėl parametro „diena“ naudojimo:

- Datos vertė 0 reiškia nulį. Vertės 1, 2, 3 ir 4 naudojamos pirmajai mėnesio dienai žymėti; 5, 6, 7 ir 8 žymi antrąją mėnesio dieną ir t. t.
- Šis parametras neturi įtakos ir nekeičia pirmiau nurodyto valandų parametro.

Pastaba dėl parametro „metai“ naudojimo:

Metų vertė 0 reiškia 1985 metus; vertė 1 reiškia 1986 metus ir t. t.

CPR_078 42 lentelėje nurodyti parametro **VehicleRegistrationNumber** įvairių baitų formatai:

42 lentelė

„VehicleRegistrationNumber“ išsamus formatas (recordDataIdentifier # F07E)

Baitas	Parametro apibrėžimas	Skiriamoji geba	Naudojimo ribos
1	Kodo puslapis (kaip apibrėžta 1 priedėlyje)	ASCII	nuo 01 iki 0A
nuo 2 iki 14	Transporto priemonės registracijos numeris (kaip apibrėžta 1 priedėlyje)	ASCII	ASCII

9 priedėlis

TIPO PATVIRTINIMAS. BŪTINIAUSIŲ BANDYMŲ SĄRAŠAS

TURINYS

1.	Įvadas	469
1.1.	Tipo patvirtinimas	469
1.2.	Nuorodos	469
2.	Transporto priemonės bloko funkciniai bandymai	470
3.	Judesio jutiklio funkciniai bandymai	473
4.	Tachografo kortelių funkciniai bandymai	475
5.	Funkcinio suderinamumo bandymai	476

1. ĮVADAS

1.1. Tipo patvirtinimas

Į tachografo (ar jo komponentų) arba tachografo kortelių EEB tipo patvirtinimą įeina:

- apsaugotumo atestacija, kurią atlieka ITSEC institucija atsižvelgdama į apsaugos tikslus, atitinkančius šio priedo 10 priedėlio nuostatas,
- funkcinė atestacija, kurią atlieka valstybės narės institucija ir kuri patvirtina, kad tachografas (arba tachografo kortelė) atitinka šio priedo reikalavimus dėl atliekamų funkcijų, matavimo tikslumo ir atsparumo aplinkos poveikiui,
- funkcinio suderinamumo atestacija, kurią atlieka kompetentinga institucija ir kuri patvirtina, kad tachografas (arba tachografo kortelė) yra visiškai funkciškai suderinamas su reikiama tachografo kortele (tachografu) (žr. šio priedo VIII skyrių).

Šiame priedėlyje nurodyta, kuriuos funkcinis bandymus privalo atlikti valstybė narė ir kuriuos funkcinio suderinamumo bandymus turi atlikti kompetentinga institucija. Bandymų atlikimo tvarka ir jų rūšys išsamiau neaprašytos.

Šiame priedėlyje neaprašyti apsaugotumo atestacijos klausimai. Jei kai kurie tipo patvirtinimui reikalingi bandymai atlikti vertinant ir atestuojant apsaugotumą, šių bandymų kartoti nebereikia. Tokiu atveju galima tik patikrinti tokių bandymų rezultatus. Tie reikalavimai, kurie turėtų būti tikrinami (arba labai artimi numatomiems atlikti bandymams), šiame priedėlyje pažymėti žvaigždute.

Šiame priedėlyje atskirai nagrinėjamas judesio jutiklio ir transporto priemonės bloko, kaip tachografo komponentų, tipo patvirtinimas. Funkcinis suderinamumas tarp kiekvieno modelio judesio jutiklio ir kiekvieno modelio transporto priemonės bloko nereikalaujamas, todėl judesio jutiklio tipo patvirtinimas suteikiamas tik derinant kartu su transporto priemonės bloko tipo patvirtinimu ir atvirkščiai.

1.2. Nuorodos

Šiame priedėlyje naudotasi tokiais šaltiniais:

IEC 68-2-1	Aplinkos poveikio bandymai. 2 dalis. Bandymai. A bandymai: šaltis. 1990 m. + 2 pataisa, 1994 m.
IEC 68-2-2	Aplinkos poveikio bandymai. 2 dalis. Bandymai. B bandymai: sausas karštis. 1974 m. + 2 pataisa, 1994 m.
IEC 68-2-6	Pagrindinės aplinkos poveikio bandymų procedūros. Bandymų metodika. Fc bandymas ir nurodymai: vibracija (sinusoidinė). 6 leidimas, 1985 m.
IEC 68-2-14	Pagrindinės aplinkos poveikio bandymų procedūros. Bandymų metodika. N bandymas: temperatūros pokytis. 1 modifikacija, 1986 m.
IEC 68-2-27	Pagrindinės aplinkos poveikio bandymų procedūros. Bandymų metodika. Ea bandymas ir nurodymai: smūgis. 3 leidimas, 1987 m.
IEC 68-2-30	Pagrindinės aplinkos poveikio bandymų procedūros. Bandymų metodika. Db bandymas ir nurodymai: karščio su drėgme cikliškas poveikis (12 + 12 valandų ciklas). 1 modifikacija, 1985 m.
IEC 68-2-35	Pagrindinės aplinkos poveikio bandymų procedūros. Bandymų metodika. Fda bandymas: plataus diapazono vibracija. Didelio laipsnio atkuriamumas. 1 modifikacija, 1983 m.
IEC 529	Įdėklų suteikiamos apsaugos laipsniai (IP kodas). 2 leidimas, 1989 m.
IEC 61000-4-2	Elektromagnetinis suderinamumas (EMS). Bandymų ir matavimo metodika. Atsparumo elektrosstatinėms iškrovoms bandymas, 1995 m.; 1 pataisa, 1998 m.
ISO 7637-1	Kelių transporto priemonės. Elektros trikdžiai dėl laidumo ir sankabos. 1 dalis. Lengvieji automobiliai ir lengvosios komercinės transporto priemonės su 12 V vardine maitinimo įtampa. Trumpalaikis elektros laidumas tik per maitinimo linijas. 2 leidimas, 1990 m.

- ISO 7637-2 Kelių transporto priemonės. Elektros trikdžiai dėl laidumo ir sankabos. 2 dalis. Komercinės transporto priemonės su 24 V vardine maitinimo įtampa. Trumpalaikis elektros laidumas tik per maitinimo linijas. Pirmasis leidimas, 1990 m.
- ISO 7637-3 Kelių transporto priemonės. Elektros trikdžiai dėl laidumo ir sankabos. 3 dalis. Transporto priemonės su 12 V arba 24 V maitinimo įtampa. Trumpalaikis elektros tekėjimas dėl talpinės arba indukcinės sankabos ne per maitinimo linijas. Pirmasis leidimas, 1995 m. + 1 pataisa, 1995 m.
- ISO/IEC 7816-1 Identifikacijos kortelės. Kortelės su integriniu grandynu (integriniais grandynais) ir kontaktais. 1 dalis. Fizinės savybės. Pirmasis leidimas, 1998 m.
- ISO/IEC 7816-2 Informacinė technologija. Identifikacijos kortelės. Kortelės su integriniu grandynu (integriniais grandynais) ir kontaktais. 2 dalis. Matmenys ir kontaktų vieta. Pirmasis leidimas, 1999 m.
- ISO/IEC 7816-3 Informacinė technologija. Identifikacijos kortelės. Kortelės su integriniu grandynu (integriniais grandynais) ir kontaktais. 3 dalis. Elektroniniai signalai ir siuntimo protokolai. 2 leidimas, 1997 m.
- ISO/IEC 10373 Identifikacijos kortelės. Testų metodai. Pirmasis leidimas, 1993 m.

2. TRANSPORTO PRIEMONĖS BLOKO FUNKCINIAI BANDYMAI

Nr.	Bandymas	Aprašymas	Susiję reikalavimai
1.	Administracinis patikrinimas		
1.1.	Dokumentacija	Dokumentacijos teisingumas	
1.2.	Gamintojo bandymų rezultatai	Įdiegimo metu gamintojo atliktų bandymų rezultatai. Įrodymai popieriuje.	070, 071, 073
2.	Vizualus patikrinimas		
2.1.	Atitiktis su dokumentacija		
2.2.	Identifikacija (ženklėjimas)		168, 169
2.3.	Medžiagos		nuo 163 iki 167
2.4.	Sandarinimas		251
2.5.	Išoriniai paviršiai		
3.	Funkciniai bandymai		
3.1.	Suteikiamos funkcijos		002, 004, 244
3.2.	Darbo režimai		006*, 007*, 008*, 009*, 106, 107
3.3.	Prieigos prie funkcijų ir duomenų teisės		010*, 011*, 240, 246, 247
3.4.	Kortelės įkišimo ir ištraukimo stebėseną		013, 014, 015*, 016*, 106
3.5.	Greičio ir atstumo matavimas		nuo 017 iki 026
3.6.	Laiko matavimas (bandymas atliekamas 20 °C temperatūroje)		nuo 027 iki 032
3.7.	Vairuotojo veiklos stebėseną		nuo 033 iki 043, 106
3.8.	Važiavimo būsenos stebėseną		044, 045, 106
3.9.	Rankomis daromi įrašai		nuo 046 iki 050b
3.10.	Įmonės užraktų valdymas		nuo 051 iki 055
3.11.	Kontrolės veiklos stebėseną		056, 057
3.12.	Įvykių ir (arba) gedimų aptikimas		nuo 059 iki 069, 106

Nr.	Bandymas	Aprašymas	Susiję reikalavimai
3.13.	Įrangos identifikacijos duomenys		075*, 076*, 079
3.14.	Duomenys apie vairuotojo kortelės įkišimą ir ištraukimą		nuo 081* iki 083*
3.15.	Duomenys apie vairuotojo veiklą		nuo 084* iki 086*
3.16.	Duomenys apie vietas		nuo 087* iki 089*
3.17.	Hodometro duomenys		nuo 090* iki 092*
3.18.	Išsamūs duomenys apie greitį		093*
3.19.	Duomenys apie įvykius		094*, 095
3.20.	Duomenys apie gedimus		096*
3.21.	Duomenys apie kalibravimą		097*, 098*
3.22.	Duomenys apie laiko koregavimą		100*, 101*
3.23.	Duomenys apie kontrolės veiklą		102*, 103*
3.24.	Duomenys apie įmonės užraktus		104*
3.25.	Duomenys apie duomenų perkėlimo veiklą		105*
3.26.	Duomenys apie ypatingas būsenas		105a*, 105b*
3.27.	Registravimas ir įrašymas į tachografo kortelių atmintį		108, 109*, 109a*, 110*, 111, 112
3.28.	Rodymas ekrane		072, 106, nuo 113 iki 128, PIC_001, DIS_001
3.29.	Spausdinimas		072, 106, nuo 129 iki 138, PIC_001, nuo PRT_001 iki PRT_112
3.30.	Perspėjimas		106, nuo 139 iki 148, PIC_001
3.31.	Duomenų perkėlimas į išorines laikmenas		072, 106, nuo 149 iki 151
3.32.	Duomenys, išvedami į papildomus išorinius įrenginius		152, 153
3.33.	Kalibravimas		154*, 155*, 156*, 245
3.34.	Laiko koregavimas		157*, 158*
3.35.	Papildomų funkcijų netrukdytas		003, 269

Nr.	Bandymas	Aprašymas	Susiję reikalavimai
4.	Aplinkos poveikio bandymai		
4.1.	Temperatūra	Funkcionalumas tikrinamas taip: — IEC 68-2-1, Ad bandymas, trunkantis 72 valandas žemoje temperatūroje (-20°C), 1 valandą – veikiant, 1 valandą – neveikiant, — IEC 68-2-2, Bd bandymas, trunkantis 72 valandas aukštoje temperatūroje ($+70^{\circ}\text{C}$), 1 valandą – veikiant, 1 valandą – neveikiant. Temperatūros ciklai: IEC 68-2-14 bandymu Na, 20 ciklų, kiekvieno ciklo metu keičiant temperatūrą nuo žemos (-20°C) iki aukštos ($+70^{\circ}\text{C}$) ir išlaikant po 2 valandas tiek žemoje, tiek aukštoje temperatūroje, patikrinama, ar transporto priemonės blokas gali išlaikyti staigius aplinkos temperatūros pokyčius. Žemoje, aukštoje temperatūroje ir temperatūros ciklų metu galima atlikti mažesnę bandymų rinkinį (iš nurodytųjų šios lentelės 3 skyriuje).	159
4.2.	Drėgnis	IEC 68-2-30 Db bandymu, atliekant šešis 24 val. trukmės ciklus, kiekvieno jų metu keičiant temperatūrą nuo $+25^{\circ}\text{C}$ iki $+55^{\circ}\text{C}$, o santykiniam drėgmeniui esant 97 % (kai temperatūra yra $+25^{\circ}\text{C}$) ir 93 % (kai temperatūra yra $+55^{\circ}\text{C}$), ar transporto priemonės blokas gali išlaikyti ciklišką drėgmės poveikį (karščio bandymą).	160
4.3.	Vibracija	1. Sinusoidinės vibracijos: patikrinama, ar transporto priemonės blokas gali išlaikyti tokias sinusoidines vibracijas: nuolat kintančias nuo 5 iki 11 Hz: 10 mm pikas nuolatinis pagreitis nuo 11 iki 300 Hz: 5 g Šis reikalavimas patikrinamas IEC 68-2-6 Fc bandymu, trunkančiu ne trumpiau kaip 3×12 valandų (po 12 valandų išilgai kiekvienos koordinačių ašies). 2. Atsitiktinės vibracijos: patikrinama, ar transporto priemonės blokas gali išlaikyti tokias atsitiktines vibracijas: dažnis: 5–150 Hz, lygis: $0,02 \text{ g}^2/\text{Hz}$ Šis reikalavimas patikrinamas IEC 68-2-35 Ffda bandymu, trunkančiu ne trumpiau kaip 3×12 valandų (po 12 valandų išilgai kiekvienos koordinačių ašies), 1 valandą – veikiant, 1 valandą – neveikiant. Abu pirmiau nurodyti bandymai atliekami su dviem skirtingais bandomo įrangos tipo pavyzdžiais.	163
4.4.	Apsauga nuo vandens ir svetimkūnių	Patikrinama, ar darbinės būklės transporto priemonėje sumontuoto transporto priemonės bloko apsaugos indeksas pagal IEC 529 yra ne mažesnis kaip IP 40.	164, 165
4.5.	Apsauga nuo viršįtampio	Patikrinama, ar transporto priemonės blokas gali išlaikyti maitinimą tokiomis sąlygomis: 24 V modeliai: 34 V, $+40^{\circ}\text{C}$ temperatūroje 1 valandą 12 V modeliai: 17 V, $+40^{\circ}\text{C}$ temperatūroje 1 valandą	161
4.6.	Apsauga nuo polių sukeitimo vietomis	Patikrinama, ar transporto priemonės blokas gali išlaikyti jo maitinimo polių sukeitimą vietomis.	161

Nr.	Bandymas	Aprašymas	Susiję reikalavimai
4.7.	Apsauga nuo trumpojo jungimo	Patikrinama, ar įvesties ir išvesties signalai apsaugoti nuo trumpojo jungimo su maitinimo ir žeminimo linijomis.	161
5.	EMS bandymai		
5.1.	Spinduliuotė ir imlumas	Atitiktis Direktyvos 95/54/EEB reikalavimams	162
5.2.	Elektrostatinė iškrova	Atitiktis IEC 61000-4-2, ± 2 kV (1 lygis) reikalavimams	162
5.3.	Imlumas trumpalaikiam laidumui per maitinimo linijas	24 V modeliams: atitiktis ISO 7637-2: 1a impulsas: $V_s = -100$ V, $R_i = 10$ omų 2 impulsas: $V_s = +100$ V, $R_i = 10$ omų 3a impulsas: $V_s = -100$ V, $R_i = 50$ omų 3b impulsas: $V_s = +100$ V, $R_i = 50$ omų 4 impulsas: $V_s = -16$ V, $V_a = -12$ V, $t_6 = 100$ ms 5 impulsas: $V_s = +120$ V, $R_i = 2,2$ omo, $t_d = 250$ ms 12 V modeliams: atitiktis ISO 7637-1: 1 impulsas: $V_s = -100$ V, $R_i = 10$ omų 2 impulsas: $V_s = +100$ V, $R_i = 10$ omų 3a impulsas: $V_s = -100$ V, $R_i = 50$ omų 3b impulsas: $V_s = +100$ V, $R_i = 50$ omų 4 impulsas: $V_s = -6$ V, $V_a = -5$ V, $t_6 = 15$ ms 5 impulsas: $V_s = +65$ V, $R_i = 3$ omai, $t_d = 100$ ms 5 impulsas turi būti bandomas tik jei transporto priemonės blokas skirtas įrengti transporto priemonėje, kurioje nenaudojama jokia įprasta išorinė apsauga nuo susikaupusio krūvio.	162

3. JUDESIO JUTIKLIO FUNKCINIAI BANDYMAI

Nr.	Bandymas	Aprašymas	Susiję reikalavimai
1.	Administracinis patikrinimas		
1.1.	Dokumentacija	Dokumentacijos teisingumas	
2.	Vizualus patikrinimas		
2.1.	Atitiktis su dokumentacija		
2.2.	Identifikacija (ženklinimas)		169, 170
2.3.	Medžiagos		nuo 163 iki 167
2.4.	Sandarinimas		251
3.	Funkciniai bandymai		
3.1.	Jutiklio identifikacijos duomenys		077*
3.2.	Judesio jutiklio ir transporto priemonės bloko sujungimas		099*, 155
3.3.	Judėjimo aptikimas		
	Judėjimo matavimo tikslumas		nuo 022 iki 026

Nr.	Bandymas	Aprašymas	Susiję reikalavimai
4.	Aplinkos poveikio bandymai		
4.1.	Darbinė temperatūra	Funkcionalumas tikrinamas (kaip nurodyta bandyme Nr. 3.3.) temperatūroje nuo -40°C iki $+135^{\circ}\text{C}$ taip: — IEC 68-2-1, Ad bandymas, trunkantis 96 valandas žemiausioje temperatūroje $T_{\min}$, — IEC 68-2-2, Bd bandymas, trunkantis 96 valandas aukščiausioje temperatūroje $T_{\max}$.	159
4.2.	Temperatūros ciklai	Funkcionalumas tikrinamas (kaip nurodyta bandyme Nr. 3.3.) IEC 68-2-14 bandymu Na, 20 ciklų, kiekvieno ciklo metu keičiant temperatūrą nuo žemos (-40°C) iki aukštos ($+135^{\circ}\text{C}$) ir išlaikant po 2 valandas tiek žemoje, tiek aukštoje temperatūroje. Žemoje, aukštoje temperatūroje ir temperatūros ciklų metu galima atlikti mažesnę bandymų rinkinį (iš nurodytųjų 3.3 bandyme).	159
4.3.	Drėgnio ciklai	Funkcionalumas tikrinamas (kaip nurodyta bandyme Nr. 3.3.) IEC 68-2-30 Db bandymu, atliekant šešis 24 val. trukmės ciklus, kiekvieno jų metu keičiant temperatūrą nuo $+25^{\circ}\text{C}$ iki $+55^{\circ}\text{C}$, o santykiniam drėgmeniui esant 97 % (kai temperatūra yra $+25^{\circ}\text{C}$) ir 93 % (kai temperatūra yra $+55^{\circ}\text{C}$).	160
4.4.	Vibracija	Funkcionalumas tikrinamas (kaip nurodyta bandyme Nr. 3.3.) IEC 68-2-6 Fc bandymu, atliekant 100 dažnio ciklų: dažnis nuolat kinta nuo 10 iki 57 Hz: 1,5 mm pikas nuolatinis pagreitis nuo 57 iki 500 Hz: 20 g	163
4.5.	Mechaninis smūgis	Funkcionalumas tikrinamas (kaip nurodyta bandyme Nr. 3.3.) IEC 68-2-27 Ea bandymu, smūgiuojant 3 smūgius abiem kryptimis išilgai statmenų viena kitai ašių.	163
4.6.	Apsauga nuo vandens ir svetimkūnių	Patikrinama, ar darbinės būklės transporto priemonėje sumontuoto judesio jutiklio apsaugos indeksas pagal IEC 529 yra ne mažesnis kaip IP 64.	165
4.7.	Apsauga nuo polių sukeitimo vietomis	Patikrinama, ar judesio jutiklis gali išlaikyti jo maitinimo polių sukeitimą vietomis.	161
4.8.	Apsauga nuo trumpojo jungimo	Patikrinama, ar įvesties ir išvesties signalai apsaugoti nuo trumpojo jungimo su maitinimo ir žeminimo linijomis.	161
5.	EMC		
5.1.	Spinduliuotė ir imlumas	Atitiktis Direktyvos 95/54/EEB reikalavimams	162
5.2.	Elektrostatinė iškrova	Atitiktis IEC 61000-4-2, $\pm 2\text{ kV}$ (1 lygis) reikalavimams	162
5.3.	Imlumas trumpalaikiam laidumui per duomenų perdavimo linijas	Atitiktis ISO 7637-3 (III lygis)	162

4. TACHOGRAFO KORTELIŲ FUNKCINIAI BANDYMAI

Nr.	Bandymas	Aprašymas	Susiję reikalavimai
1.	Administracinis patikrinimas		
1.1.	Dokumentacija	Dokumentacijos teisingumas	
2.	Vizualus patikrinimas		
2.1.		Patikrinama, ar visos apsaugos priemonės ir matomi duomenys ant kortelės išspausdinti teisingai ir atitinka reikalavimus.	nuo 171 iki 181
3.	Fiziniai bandymai		
3.1.		Patikrinami kortelės matmenys ir kontaktų vieta.	184 ISO/IEC 7816-1 ISO/IEC 7816-2
4.	Protokolo bandymai		
4.1.	ATR	Patikrinama, ar ATR atitinka reikalavimus.	ISO/IEC 7816-3, TCS 304, 307, 308
4.2.	T=0	Patikrinama, ar protokolas T=0 atitinka reikalavimus.	ISO/IEC 7816-3, TCS 302, 303, 305
4.3.	PTS	Patikrinama, ar komanda PTS atitinka reikalavimus nustatant T=1 iš T=0.	ISO/IEC 7816-3, nuo TCS 309 iki TCS 311
4.4.	T=1	Patikrinama, ar protokolas T=1 atitinka reikalavimus.	ISO/IEC 7816-3, TCS 303, 306
5.	Kortelės struktūra		
5.1.		Išbandoma, ar kortelės struktūra atitinka reikalavimus – ar kortelėje yra privalomosios rinkmenos ir jų prieigos sąlygos.	TCS 312 TCS 400*, 401, 402, 403*, 404, 405*, 406, 407, 408*, 409, 410*, 411, 412, 413*, 414, 415*, 416, 417, 418*, 419
6.	Funkciniai bandymai		
6.1.	Įprastas apdorojimas	Bent po kartą išbandoma kiekviena leistina komanda (pvz., komanda UPDATE_BINARY išbandoma su CLA = „00“, CLA = „0C“ ir su skirtingais parametrais P1, P2 ir Lc). Patikrinama, ar operacijos kortelėje atliekamos iš tikrųjų (pvz., nuskaitant rinkmeną, su kuria komanda buvo atlikta).	nuo TCS 313 iki TCS 379
6.2.	Pranešimai apie klaidas	Bent po kartą išbandomas kiekvienos komandos kiekvienas pranešimas apie klaidą (kaip nurodyta 2 priedėlyje). Bent po kartą išbandoma kiekviena bendroji klaida (išskyrus nepažeistumo klaidas „6400“, kurios patikrinamos atliekant apsaugotumo atestaciją).	
7.	Aplinkos poveikio bandymai		
7.1.		Patikrinama, ar kortelės veikia ISO/IEC 10373 apibrėžtomis sąlygomis	nuo 185 iki 188 ISO/IEC 7816-1

5. FUNKCINIO SUDERINAMUMO BANDYMAI

Nr.	Bandymas	Aprašymas
1.	Abipusis autentiškumo patvirtinimas	Patikrinama, ar abipusis autentiškumo patvirtinimas tarp transporto priemonės bloko ir tachografo kortelės vyksta tinkamai.
2.	Rašymo ir nuskaitymo bandymai	Atliekamas transporto priemonės bloko būdingos veiklos patikrinimas. Veiklos scenarijus turi būti suderintas su bandomu kortelės tipu, o į kortelę turi būti įrašoma kiek įmanoma daugiau EF. Perkeliant duomenis iš kortelės patikrinama, ar tinkamai įrašyti visi reikiami įrašai. Išspausdinant kasdienį spaudinį iš kortelės patikrinama, ar visus reikiamus įrašus galima tinkamai nuskaityti.

10 priedėlis

BENDRIEJI APSAUGOS TIKSLAI

Šiame priedėlyje nurodyti būtinausi reikalaujami judesio jutiklio, transporto priemonės bloko ir tachografo kortelių apsaugos tikslai.

Tam, kad gamintojai suformuluotų apsaugos tikslus, kuriais remdamiesi galėtų siekti sertifikuoti apsaugotumą, jie turi patobulinti ir užpildyti reikiamus dokumentus, nepakeisdami ir neišbraukdami esamų pavojų, reikalavimų, procedūrinių priemonių ir apsaugos užtikrinimo funkcijų specifikacijų.

TURINYS

Judesio jutiklio bendrieji apsaugos tikslai

1.	Įvadas	482
2.	Santrumpos, apibrėžimai ir nuorodos	482
2.1.	Santrumpos	482
2.2.	Apibrėžimai	482
2.3.	Nuorodos	483
3.	Gaminio apibūdinimas	483
3.1.	Judesio jutiklio aprašymas ir naudojimo būdas	483
3.2.	Judesio jutiklio gyvavimo ciklas	484
3.3.	Pavojai	484
3.3.1.	Pavojai prieigos kontrolei	484
3.3.2.	Su konstrukcija susiję pavojai	485
3.3.3.	Su eksploatacija susiję pavojai	485
3.4.	Apsaugos tikslai	485
3.5.	Informacinės technologijos apsaugos tikslai	485
3.6.	Fizinės, personalo arba procedūrinės priemonės	486
3.6.1.	Įrangos konstrukcija	486
3.6.2.	Įrangos tiekimas	486
3.6.3.	Apsauginių duomenų sukūrimas ir pateikimas	486
3.6.4.	Tachografų įrengimas, kalibravimas ir patikra	486
3.6.5.	Teisės aktų vykdymo kontrolė	486
3.6.6.	Programinės įrangos tobulinimas	486
4.	Apsaugos užtikrinimo funkcijos	486
4.1.	Identifikacija ir autentiškumo patvirtinimas	486
4.2.	Prieigos kontrolė	487
4.2.1.	Prieigos kontrolės strategija	487
4.2.2.	Prieigos prie duomenų teisės	487
4.2.3.	Rinkmenų struktūra ir prieigos sąlygos	487
4.3.	Atskaitomybė	487

4.4.	Auditas	488
4.5.	Tikslumas	488
4.5.1.	Informacijos srauto valdymo strategija	488
4.5.2.	Vidinis duomenų perdavimas	488
4.5.3.	Atmintyje laikomų duomenų nepažeistumas	488
4.6.	Eksplotacinis patikimumas	488
4.6.1.	Bandymai	488
4.6.2.	Programinė įranga	489
4.6.3.	Fizinė apsauga	489
4.6.4.	Maitinimo nutūkimas	489
4.6.5.	Perkrovimo sąlygos	489
4.6.6.	Duomenų prieinamumas	489
4.6.7.	Daugiafunkciškumas	489
4.7.	Keitimasis duomenimis	489
4.8.	Kriptografinė geba	489
5.	Apsaugos mechanizmų apibrėžimas	490
6.	Būtiniausias apsaugos mechanizmų neįveikiamumas	490
7.	Užtikrinimo lygis	490
8.	Apibūdinimas	490

Transporto priemonės bloko bendrieji apsaugos tikslai

1.	Įvadas	492
2.	Santrumpos, apibrėžimai ir nuorodos	492
2.1.	Santrumpos	492
2.2.	Apibrėžimai	492
2.3.	Nuorodos	492
3.	Gaminio apibūdinimas	492
3.1.	Transporto priemonės bloko aprašymas ir naudojimo būdas	492
3.2.	Transporto priemonės bloko gyvavimo ciklas	494
3.3.	Pavojai	494
3.3.1.	Pavojai identifikacijos ir prieigos kontrolės strategijai	494
3.3.2.	Su konstrukcija susiję pavojai	495
3.3.3.	Su eksploatacija susiję pavojai	495
3.4.	Apsaugos tikslai	495
3.5.	Informacinės technologijos apsaugos tikslai	496
3.6.	Fizinės, personalo arba procedūrinės priemonės	496
3.6.1.	Įrangos konstrukcija	496
3.6.2.	Įrangos tiekimas	496

3.6.3. Apsauginių duomenų sukūrimas ir pateikimas	496
3.6.4. Kortelių pateikimas	497
3.6.5. Tachografų įrengimas, kalibravimas ir patikra	497
3.6.6. Įrangos naudojimas	497
3.6.7. Teisės aktų vykdymo kontrolė	497
3.6.8. Programinės įrangos tobulinimas	497
4. Apsaugos užtikrinimo funkcijos	497
4.1. Identifikacija ir autentiškumo patvirtinimas	497
4.1.1. Judesio jutiklio identifikacija ir autentiškumo tikrinimas	497
4.1.2. Naudotojo identifikacija ir autentiškumo tikrinimas	498
4.1.3. Nuotoliniu būdu prisijungusios įmonės identifikacija ir autentiškumo tikrinimas	499
4.1.4. Valdymo įrenginių identifikacija ir autentiškumo tikrinimas	499
4.2. Prieigos kontrolė	499
4.2.1. Prieigos kontrolės strategija	499
4.2.2. Prieigos prie funkcijų teisės	499
4.2.3. Prieigos prie duomenų teisės	499
4.2.4. Rinkmenų struktūra ir prieigos sąlygos	500
4.3. Atskaitomybė	500
4.4. Auditas	500
4.5. Objektų pakartotinis naudojimas	501
4.6. Tikslumas	501
4.6.1. Informacijos srauto valdymo strategija	501
4.6.2. Vidinis duomenų perdavimas	501
4.6.3. Atmintyje laikomų duomenų nepažeistumas	501
4.7. Eksploatacinis patikimumas	501
4.7.1. Bandymai	501
4.7.2. Programinė įranga	502
4.7.3. Fizinė apsauga	502
4.7.4. Maitinimo nutrūkimas	502
4.7.5. Perkrovimo sąlygos	502
4.7.6. Duomenų prieinamumas	502
4.7.7. Daugiafunkciškumas	502
4.8. Keitimasis duomenimis	502
4.8.1. Duomenų keitimasis su judesio jutikliu	502
4.8.2. Duomenų keitimasis su tachografo kortelėmis	503
4.8.3. Duomenų keitimasis su išorinėmis laikmenomis (duomenų perkėlimo funkcija)	503
4.9. Kriptografinė geba	503

5.	Apsaugos mechanizmų apibrėžimas	503
6.	Būtiniausias apsaugos mechanizmų neįveikiamumas	503
7.	Užtikrinimo lygis	503
8.	Apibūdinimas	504

Tachografo kortelės bendrieji apsaugos tikslai

1.	Įvadas	508
2.	Santrumpos, apibrėžimai ir nuorodos	508
2.1.	Santrumpos	508
2.2.	Apibrėžimai	508
2.3.	Nuorodos	509
3.	Gaminio apibūdinimas	509
3.1.	Tachografo kortelės aprašymas ir naudojimo būdas	509
3.2.	Tachografo kortelės gyvavimo ciklas	509
3.3.	Pavojai	510
3.3.1.	Pavojai identifikacijos ir prieigos kontrolės strategijai	510
3.3.2.	Kenkimo būdai	510
3.4.	Apsaugos tikslai	510
3.5.	Informacinės technologijos apsaugos tikslai	510
3.6.	Fizinės, personalo arba procedūrinės priemonės	510
4.	Apsaugos užtikrinimo funkcijos	511
4.1.	Atitiktis apsaugos profiliams	511
4.2.	Naudotojo identifikacija ir autentiškumo patvirtinimas	511
4.2.1.	Naudotojo identifikacija	511
4.2.2.	Naudotojo autentiškumo tikrinimas	511
4.2.3.	Autentiškumo tikrinimo nepavykimas	511
4.3.	Prieigos kontrolė	512
4.3.1.	Prieigos kontrolės strategija	512
4.3.2.	Prieigos kontrolės funkcijos	512
4.4.	Atskaitomybė	512
4.5.	Auditas	512
4.6.	Tikslumas	512
4.6.1.	Atmintyje laikomų duomenų nepažeistumas	512
4.6.2.	Pagrindinis duomenų autentiškumo tikrinimas	512
4.7.	Ekspluatacinis patikimumas	513
4.7.1.	Bandymai	513
4.7.2.	Programinė įranga	513
4.7.3.	Maitinimo nutūkimas	513

4.7.4. Perkrovimo sąlygos	513
4.8. Keitimasis duomenimis	513
4.8.1. Duomenų keitimasis su transporto priemonės bloku	513
4.8.2. Duomenų eksportas ne į transporto priemonės bloką (duomenų perkėlimo funkcija)	513
4.9. Kriptografinė geba	513
5. Apsaugos mechanizmų apibrėžimas	513
6. Būtiniausias apsaugos mechanizmų neįveikiamumas	514
7. Užtikrinimo lygis	514
8. Apibūdinimas	514

JUDESIO JUTIKLIO BENDRIEJI APSAUGOS TIKSLAI

1. Įvadas

Šiame dokumente aprašytas judesio jutiklis, pavojai, kuriuos jis turi gebėti įveikti, ir apsaugos reikalavimai, kuriuos jis turi atitikti. Čia nurodytos reikiamos apsaugos užtikrinimo funkcijos, reikalaujamas apsaugos mechanizmų neįveikiamumas ir reikiamas tobulinimo bei vertinimo užtikrinimo lygis.

Šiame dokumente nurodyti reikalavimai iš I priedo B dalies teksto. Kad būtų aiškiau skaityti, kartais I priedo B dalies teksto reikalavimai ir apsaugos tikslų reikalavimai kartojami. Jei apsaugos tikslų reikalavimas ir tame reikalavime nurodytas I priedo B dalies teksto reikalavimas nesutampa, pirmenybę turi I priedo B dalies teksto reikalavimas.

Apsaugos tikslų nenurodyti I priedo B dalies teksto reikalavimai su apsaugos užtikrinimo funkcijomis nėra susiję.

Tam, kad pavojus, reikalavimus, procedūrines priemones ir SEF specifikacijas galima būtų rasti patobulinimų ir įvertinimo dokumentacijoje, jiems priskirti unikalūs žymekliai.

2. Santrumpos, apibrėžimai ir nuorodos**2.1. Santrumpos**

ROM	pastovioji atmintis;
SEF	apsaugą užtikrinanti funkcija;
TBD	nustatyтина;
TOE	įvertinimo tikslas;
VU	transporto priemonės blokas.

2.2. Apibrėžimai

Skaitmeninis tachografas	Tachografas
Objektas	Su judesio jutikliu sujungtas įrenginys
Duomenys apie judėjimą	Duomenys, kuriais keičiamasi su TPB, nurodantys greitį ir nuvažiuotą atstumą
Fiziškai atskirtos dalys	Judesio jutiklio fiziniai komponentai, išdėstyti transporto priemonėje (priešpriešinant judesio jutiklio korpuse esantiems fiziniams komponentams)
Apsauginiai duomenys	Ypatingi duomenys, reikalingi apsaugos užtikrinimo funkcijai veikti (pvz., kriptografiniai raktai)
Sistema	Įranga, žmonės ar organizacijos, kaip nors susiję su tachografu
Naudotojas	Judesį jutiklį naudojantis asmuo (kai nevartojama junginyje „duomenys apie naudotoją“)
Duomenys apie naudotoją	Visi judesio jutiklio atmintyje įrašyti ir laikomi duomenys, išskyrus duomenis apie judėjimą ir apsauginius duomenis.

2.3. Nuorodos

ITSEC Informacinės technologijos apsaugos vertinimo kriterijai, 1991 m.

3. Gaminio apibūdinimas

3.1. Judesio jutiklio aprašymas ir naudojimo būdas

Judesio jutiklis skirtas montuoti į kelių transporto priemones. Jo paskirtis – suteikti transporto priemonės blokui apsaugotą informaciją apie transporto priemonės greitį ir nuvažiuotą atstumą.

Judesio jutiklis mechaniškai sujungiamas su judančia transporto priemonės dalimi, kurios judėjimas atitinka transporto priemonės greitį arba nuvažiuotą atstumą. Jis gali būti transporto priemonės pavarų dėžėje arba bet kurioje kitoje dalyje.

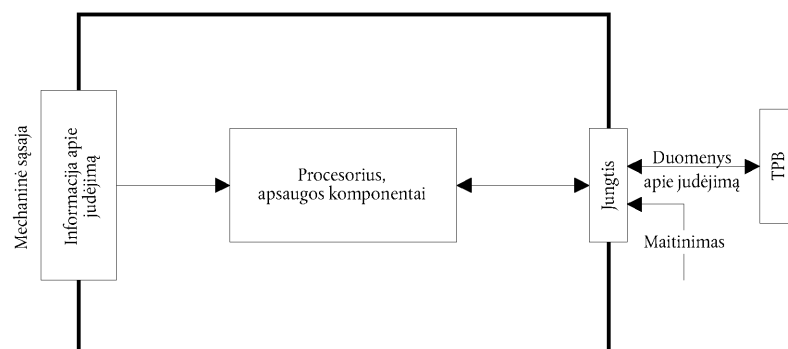
Darbo režimu judesio jutiklis yra sujungtas su TPB.

Valdymo tikslais jis taip pat gali būti sujungtas su specialiąja įranga (nustato gamintojas).

Tipinis judesio jutiklis apibūdintas toliau pateikiamame paveikslėlyje:

1 paveikslėlis

Tipinis judesio jutiklis

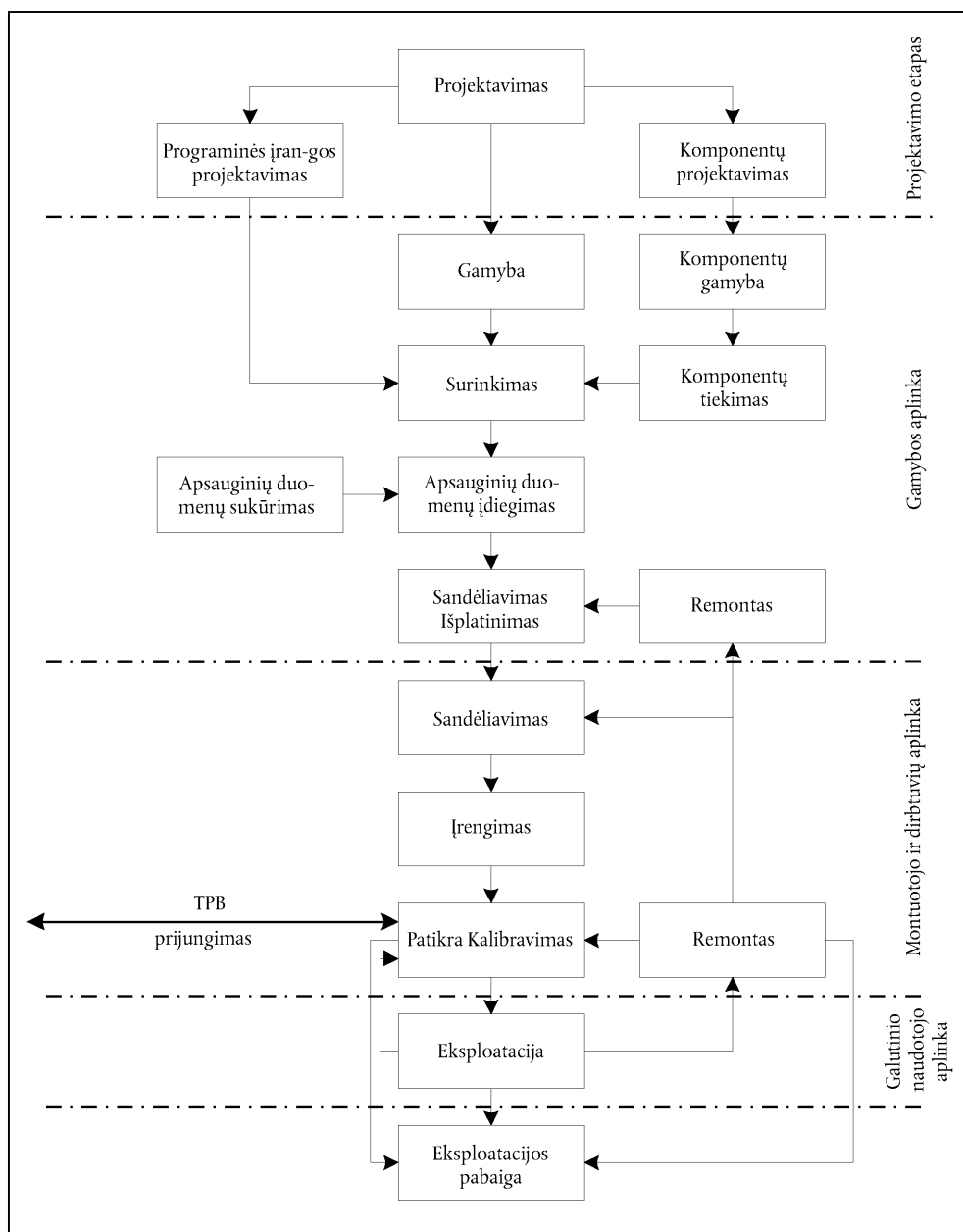


3.2. Judesio jutiklio gyvavimo ciklas

Tipinis judesio jutiklio gyvavimo ciklas pavaizduotas toliau pateikiamame paveikslėlyje:

2 paveikslėlis

Tipinis judesio jutiklio gyvavimo ciklas



3.3. Pavojai

Šiame poskyryje aprašyti judesio jutikliui galintys kilti pavojai.

3.3.1. Pavojai prieigos kontrolei

T.Access

Naudotojai gali mėginti pasinaudoti jiems neleistinomis funkcijomis.

3.3.2. Su konstrukcija susiję pavojai

T.Faults	Dėl techninės, programinės įrangos, ryšio procedūrų sutrikimų gali sumažėti judesio jutiklio apsaugotumas.
T.Tests	Taikant neleistinus bandymų metodus arba galimas kontrolės išvengimo galimybės gali sumažėti judesio jutiklio apsaugotumas.
T.Design	Naudotojai gali mėginti neleistinai susipažinti su konstrukcija iš gamintojo medžiagos (ji gali būti pavagiama, gaunama už kyšius ir kt.) arba naudodamiesi inžinerine analize.

3.3.3. Su eksploatacija susiję pavojai

T.Environment	Naudotojai gali sumažinti judesio jutiklio apsaugotumą aplinkos poveikiu (terminiu, elektromagnetiniu, optiniu, cheminiu, mechaniniu ir kt.).
T.Hardware	Naudotojai gali mėginti pakeisti judesio jutiklio techninę įrangą.
T.Mechanical_Origin	Naudotojai gali mėginti pakeisti judesio jutiklio įvestį (pvz., nusukti jo korpusą nuo pavarų dėžės ir kt.).
T.Motion_Data	Naudotojai gali mėginti pakeisti duomenis apie transporto priemonės judėjimą (papildydami, pakeisdami, panaikindami, pakartodami signalą).
T.Power_Supply	Naudotojai gali mėginti susidoroti su judesio jutiklio apsauga –pakeisti jo maitinimą (jį nutraukti, sumažinti ar padidinti).
T.Security_Data	Naudotojai gali mėginti neleistinai susipažinti su apsauginiais duomenimis juos generuojant, perkeltant arba sandėliuojant įrangą.
T.Software	Naudotojai gali mėginti pakeisti judesio jutiklio programinę įrangą.
T.Stored_Data	Naudotojai gali mėginti pakeisti į atmintį įrašytus duomenis (apsauginius arba duomenis apie naudotoją).

3.4. Apsaugos tikslai

Pagrindinis skaitmeninės tachografo sistemos apsaugos tikslas yra toks:

O.Main	Kontrolės institucijų tikrinami duomenys turi būti prieinami. Jie visiškai tiksliai turi apibūdinti kontroliuojamų vairuotojų ir transporto priemonių veiklą: vairavimo, darbo, buvimo pasirengus dirbti ir poilsio laikotarpius, transporto priemonės greitį.
---------------	--

Todėl judesio jutiklio apsaugos tikslas, kuris prisideda prie bendrojo apsaugos tikslo:

O.Sensor_Main	Judesio jutiklio duomenys turi būti prieinami TPB taip, kad pastarasis visiškai ir tiksliai galėtų nustatyti transporto priemonės greitį ir nuvažiuotą atstumą.
----------------------	---

3.5. Informacinės technologijos apsaugos tikslai

Specifiniai judesio jutiklio IT apsaugos tikslai, prisidedantys prie pagrindinio apsaugos tikslo, yra tokie:

O.Access	Judesio jutiklis turi kontroliuoti prijungto objekto prieigą prie funkcijų ir duomenų.
O.Audit	Judesio jutiklis turi kontroliuoti bandymus pažeisti jo apsaugą ir atsekti juos iki susijusių objektų.
O.Authentication	Judesio jutiklis turi tvirtinti prijungtų objektų autentiškumą.

O.Processing	Judesio jutiklis turi užtikrinti, kad įvesties duomenys būtų tiksliai paverčiami duomenimis apie judėjimą.
O.Reliability	Judesio jutiklis turi patikimai dirbti.
O.Secured_Data_Exchange	Judesio jutiklis turi apsaugoti keitimąsi duomenimis su TPB.

3.6. Fizinės, personalo arba procedūrinės priemonės

Šiame poskyryje aprašyti fiziniai, personalo arba procedūriniai reikalavimai, kurie didina judesio jutiklio apsaugą.

3.6.1. Įrangos konstrukcija

M.Development	Judesio jutiklių projektuotojai turi užtikrinti, kad projektuojant atsakomybė būtų paskirstyta taip, jog būtų užtikrinta IT apsauga.
M.Manufacturing	Judesio jutiklių gamintojai turi užtikrinti, kad gaminant atsakomybė būtų paskirstyta taip, jog būtų užtikrinta IT apsauga ir gamybos proceso metu judesio jutikliai būtų apsaugoti nuo fizinio poveikio, kuris galėtų sumažinti IT apsaugą.

3.6.2. Įrangos tiekimas

M.Delivery	Judesio jutiklių gamintojai, transporto priemonių gamintojai ir montuotojai arba dirbtuvės turi užtikrinti, kad judesio jutikliais būtų disponuojama taip, jog būtų užtikrinta IT apsauga.
-------------------	--

3.6.3. Apsauginių duomenų sukūrimas ir pateikimas

M.Sec_Data_Generation	Apsauginių duomenų generavimo algoritmai turi būti prieinami tik įgaliotiems ir patikimiems asmenims.
M.Sec_Data_Transport	Apsauginiai duomenys turi būti generuojami, perkeliama ir įdiegiami į judesio jutiklį užtikrinant reikiamą jų konfidencialumą ir nepažeistumą.

3.6.4. Tachografų įrengimas, kalibravimas ir patikra

M.Approved_Workshops	Tachografus turi įrengti, kalibruoti ir remontuoti patikimi ir patvirtinti montuotojai ar dirbtuvės.
M.Mechanical_Interface	Turi būti priemonės aptikti fizinius bandymų panaudoti mechaninę sąsają ne pagal paskirtį požymius (pvz., plombos).
M.Regular_Inpections	Tachografai turi būti reguliariai tikrinami ir kalibruojami.

3.6.5. Teisės aktų vykdymo kontrolė

M.Controls	Turi būti reguliariai ir atsitiktine tvarka atliekamas teisės aktų vykdymo auditas, kurio metu tikrinamas ir apsaugotumas.
-------------------	--

3.6.6. Programinės įrangos tobulinimas

M.Software_Upgrade	Prieš diegiant naujas programinės įrangos versijas į judesio jutiklius, joms turi būti suteiktas apsaugotumo pažymėjimas.
---------------------------	---

4. Apsaugos užtikrinimo funkcijos

4.1. Identifikacija ir autentiškumo patvirtinimas

UIA_101 Judesio jutiklis per kiekvieną sąveiką turi gebėti nustatyti bet kurio objekto, prie kurio jis prijungtas, tapatybę.

UIA_102 Prijungto objekto tapatybę turi sudaryti:

- tapatybės grupė:
 - TPB,
 - valdymo įtaisas,
 - kita,
- objekto ID (tik TPB).

UIA_103 Prijungto TPB objekto ID turi sudaryti TPB patvirtinimo numeris ir TPB serijos numeris.

UIA_104 Judesio jutiklis turi gebėti patikrinti bet kurio TPB arba valdymo įrenginio, prie kurio jis prijungtas, autentiškumą:

- prijungiant objektą,
- vėl atsiradus maitinimui.

UIA_105 Judesio jutiklis turi gebėti periodiškai pakartotinai tikrinti TPB, prie kurio jis prijungtas, autentiškumą.

UIA_106 Judesio jutiklis turi aptikti ir neleisti naudotis autentiškumo tikrinimo duomenimis, kurie yra nukopijuoti ir siunčiami pakartotinai.

UIA_107 Aptikusi (ne daugiau kaip 20; nustato gamintojas) iš eilės nesėkmingų mėginimų patvirtinti autentiškumą, SEF turi:

- užregistruoti įvykį audito įrašų,
- perspėti objektą,
- toliau siųsti duomenis apie judėjimą neapsaugotu režimu.

4.2. **Prieigos kontrolė**

Prieigos kontrolė užtikrina, kad informaciją nuskaityti, sukurti ar keisti TOE galėtų tik tie, kam leidžiama tai daryti.

4.2.1. *Prieigos kontrolės strategija*

ACC_101 Judesio jutiklis turi kontroliuoti prieigos prie funkcijų ir duomenų teises.

4.2.2. *Prieigos prie duomenų teisės*

ACC_102 Judesio jutiklis turi užtikrinti, kad jo identifikacijos duomenis būtų galima įrašyti tik vieną kartą (078 reikalavimas).

ACC_103 Judesio jutiklis turi priimti ir (arba) įrašyti į atmintį duomenis tik iš objektų, kurių autentiškumas patvirtintas.

ACC_104 Judesio jutiklis turi taikyti atitinkamas apsauginių duomenų nuskaitymo ir įrašymo prieigos teises.

4.2.3. *Rinkmenų struktūra ir prieigos sąlygos*

ACC_105 Programos ir duomenų rinkmenų struktūra turi būti sudaryta gamybos proceso metu ir užblokuota taip, kad daugiau jos nebebūtų galima keisti ar panaikinti.

4.3. **Atskaitomybė**

ACT_101 Judesio jutiklis turi laikyti savo atmintyje savo identifikacijos duomenis (077 reikalavimas).

ACT_102 Judesio jutiklis turi laikyti savo atmintyje duomenis apie įdiegimą (099 reikalavimas).

ACT_103 Judesio jutiklis turi gebėti išvesti atskaitomybės duomenis patvirtinto autentiškumo objektams, kai šie to pareikalauja.

4.4. **Auditas**

AUD_101 Judesio jutiklis turi generuoti audito įrašus apie jo apsaugą mažinančius įvykius.

AUD_102 Judesio jutiklio apsaugą mažina tokie įvykiai:

- bandymai pažeisti apsaugą,
- nepavykęs autentiškumo tikrinimas,
- atmintyje laikomų duomenų nepažeistumo klaida,
- vidinio duomenų perdavimo klaida,
- neleistinas korpuso atidarymas,
- kenkimas techninei įrangai,
- jutiklio gedimas.

AUD_103 Audito įrašuose turi būti tokie duomenys:

- įvykio data ir laikas,
- įvykio rūšis,
- prijungto objekto tapatybė.

Kai reikalaujamų duomenų negalima gauti, turi būti pateikta atitinkama numatytoji nuoroda (nustato gamintojas).

AUD_104 Judesio jutiklis turi siųsti sugeneruotus audito įrašus į TPB jų sukūrimo momentu ir taip pat gali laikyti juos atmintyje.

AUD_105 Jei judesio jutiklis įrašo audito įrašus į atmintį, joje turi būti išlaikyti 20 audito įrašų (neatsižvelgiant į tam skirtos talpos išnaudojimą) ir šiuos įrašus turi būti galima išvesti į patvirtinto autentiškumo objektus jų reikalavimu.

4.5. **Tikslumas**

4.5.1. *Informacijos srauto valdymo strategija*

ACR_101 Judesio jutiklis turi užtikrinti, kad duomenys būtų apdorojami ir gaunami tik jutiklio mechanine įvestimi.

4.5.2. *Vidinis duomenų perdavimas*

Šio punkto reikalavimai taikomi tik judesio jutikliams, kurie naudoja fiziškai atskirtas dalis.

ACR_102 Jei duomenys perduodami tarp fiziškai atskirtų judesio jutiklio dalių, jie turi būti apsaugoti nuo galimybės juos pakeisti.

ACR_103 Aptikus duomenų vidinio perdavimo klaidą turi būti bandoma siųsti iš naujo, o SEF turi sugeneruoti apie šį įvykį audito įrašą.

4.5.3. *Atmintyje laikomų duomenų nepažeistumas*

ACR_104 Judesio jutiklis turi tikrinti, ar jo atmintyje laikomuose duomenyse apie naudotoją nėra nepažeistumo klaidų.

ACR_105 Aptikus atmintyje laikomuose duomenyse apie naudotoją nepažeistumo klaidų SEF turi sugeneruoti audito įrašą.

4.6. **Eksplloatacinis patikimumas**

4.6.1. *Bandymai*

RLB_101 Visos bandymams gamyboje reikalingos komandos, veikimo rūšys ar bandymų vietos turi būti dezaktyvuotos arba pašalintos iki gamybos pabaigos. Jų turi būti nebeįmanoma vėliau vėl panaudoti.

RLB_102 Pradinio paleidimo ir įprasto veikimo metu judesio jutiklis pats tikrinti, ar veikia tinkamai. Judesio jutiklio savitikra turi aprėpti apsauginių duomenų ir atmintyje laikomo vykdomojo kodo (jei jis nėra įrašytas į ROM) nepažeistumo tikrinimą.

RLB_103 Savitiktros metu aptikusi vidinį gedimą, SEF turi sugeneruoti audito įrašą (jutiklio gedimas).

4.6.2. Programinė įranga

RLB_104 Neturi būti galimybių vietoje analizuoti judesio jutiklio programinę įrangą arba ją perprogramuoti.

RLB_105 Įvestis iš išorinių šaltinių neturi būti priimama kaip vykdomasis kodas.

4.6.3. Fizinė apsauga

RLB_106 Jei judesio jutiklio konstrukcija leidžia jį atidaryti, jis turi aptikti bet koki korpuso atidarymą net ir nesant išorinio maitinimo ne mažiau kaip 6 mėnesius. Tokiu atveju SEF turi sugeneruoti audito įrašą apie įvykį (leidžiama, kad audito įrašas būtų sugeneruotas ir įrašytas į atmintį atsiradus maitinimui).

Jei judesio jutiklio negalima atidaryti, jo konstrukcija turi būti tokia, kad būtų lengvai matyti bandymo tai padaryti fiziniai požymiai (pvz., apžiūrėjus).

RLB_107 Judesio jutiklis turi aptikti nustatytos rūšies (nustato gamintojas) kenkimą techninei įrangai.

RLB_108 Pirmiau nurodytu atveju SEF turi sugeneruoti audito įrašą, o judesio jutiklis – (nustato gamintojas).

4.6.4. Maitinimo nutrūkimas

RLB_109 Nutrūkus arba kintant maitinimo įtampai judesio jutiklio būseną turi likti apsaugota.

4.6.5. Perkrovimo sąlygos

RLB_110 Nutrūkus maitinimui, sustabdžius operaciją jai nesibaigus arba bet kuriomis kitomis perkrovimo sąlygomis judesio jutiklis turi būti perkrautas tinkamai.

4.6.6. Duomenų prieinamumas

RLB_111 Judesio jutiklis turi užtikrinti, kad prie sistemos elementų galima būtų prieiti, kai to reikia, ir kad to nebūtų reikalaujama ir nuo to nebūtų sulaikoma be reikalo.

4.6.7. Daugifunkciškumas

RLB_112 Jei judesio jutiklis be tachografo funkcijų atlieka ir kitas funkcijas, visos jos turi būti fiziškai ir (arba) logiškai atskirtos viena nuo kitos. Šių funkcijų apsauginiai duomenys turi būti skirtingi. Vienu metu gali būti atliekama tik viena užduotis.

4.7. Keitimasis duomenimis

DEX_101 Judesio jutiklis turi eksportuoti duomenis apie judėjimą į TPB su atitinkamais apsaugos objektais taip, kad TPB galėtų patikrinti jų nepažeistumą ir autentiškumą.

4.8. Kriptografinė geba

Šio poskyrio reikalavimai taikomi tik tuomet, kai reikia, atsižvelgiant į naudojamus apsaugos mechanizmus ir gamintojo sprendimu.

CSP_101 Visos judesio jutiklio atliekamos kriptografinės operacijos turi būti pagal nustatytą algoritmą ir rakto dydį.

CSP_102 Jei judesio jutiklis generuoja kriptografinius raktus, tai turi būti daroma pagal nustatytus kriptografinių raktų kūrimo algoritmus ir raktų dydį.

CSP_103 Jei judesio jutiklis platina kriptografinius raktus, tai turi būti daroma nustatytais kriptografinių raktų platinimo būdais.

CSP_104 Jei judesio jutiklis priima kriptografinius raktus, tai turi būti daroma nustatytais kriptografinių raktų priėmimo būdais.

CSP_105 Jei judesio jutiklis naikina kriptografinius raktus, tai turi būti daroma nustatytais kriptografinių raktų naikinimo būdais.

5. Apsaugos mechanizmų apibrėžimas

Apsaugos mechanizmus, kurie atlieka judesio jutiklio apsaugos užtikrinimo funkcijas, nustato judesio jutiklio gamintojai.

6. Būtiniausias apsaugos mechanizmų neįveikiamumas

Judesio jutiklio apsaugos mechanizmų neįveikiamumas turi būti ne mažesnis kaip aukštas, kaip apibrėžta ITSEC.

7. Užtikrinimo lygis

Judesio jutiklio užtikrinimo lygis yra lygis E3 pagal ITSEC.

8. Apibūdinimas

Toliau esančiose lentelėse pateiktas SEF apibūdinimas, nurodantis:

- kurios SEF ar priemonės kovoja su pavojais,
- kurios SEF atitinka kuriuos IT apsaugos tikslus.

	Pavojai												IT reikalavimai					
	Access [priėga]	Faults [gedimai]	Tests [bandymai]	Design [konstrukcija]	Environment [aplinka]	Hardware [techninė įranga]	Mechanical_Origin [mechaninės kilmės]	Motion_Data [duomenys apie judėjimą]	Power_Supply [maitinimas]	Security_Data [apsauginiai duomenys]	Software [programinė įranga]	Stored Data [atmintyje laikomi duomenys]	Access [priėga]	Audit [auditas]	Authentication [autentiškumo tikrinimas]	Processing [apdorojimas]	Reliability [patikimumas]	Secured_Data_Exchange [keitimasis apsaugotais duomenimis]
Fizinės, personalo, procedūrinės priemonės																		
Projektavimas		x	x	x														
Gamyba			x	x														
Tiekimas						x						x	x					
Apsauginių duomenų kūrimas										x								
Apsauginių duomenų perdavimas										x								
Patvirtintos dirbtuvės							x											
Mechaninė sąsaja							x											
Reguliari patikra						x	x		x		x							
Teisės aktų vykdymo kontrolė					x	x	x		x	x	x							
Programinės įrangos tobulinimas											x							
Apsaugos užtikrinimo funkcijos																		
Identifikacija ir autentiškumo tikrinimas																		
UIA_101 Objektų identifikacija	x							x					x		x			x
UIA_102 Objektų tapatybė	x												x		x			
UIA_103 TPB tapatybė														x				
UIA_104 Objektų autentiškumo tikrinimas	x							x					x		x			x
UIA_105 Pakartotinis autentiškumo tikrinimas	x							x					x		x			x
UIA_106 Nesuklastojamas autentiškumo tikrinimas	x							x					x		x			
UIA_107 Autentiškumo tikrinimo nepavykimas								x						x			x	
Prieigos kontrolė																		
ACC_101 Prieigos kontrolės strategija	x									x		x	x					
ACC_102 Judesio jutiklio ID												x	x					

[illegible]

TRANSPORTO PRIEMONĖS BLOKO BENDRIEJI APSAUGOS TIKSLAI

1. Įvadas

Šiame dokumente aprašytas transporto priemonės blokas, pavojai, kuriuos jis turi gebėti įveikti, ir apsaugos tikslai, kuriuos jis turi atitikti. Čia nurodytos reikiamos apsaugos užtikrinimo funkcijos, reikalaujamas apsaugos mechanizmų neišvengiamumas ir reikiamas tobulinimo bei vertinimo užtikrinimo lygis.

Šiame dokumente nurodyti reikalavimai iš I priedo B dalies teksto. Kad būtų aiškiau skaityti, kartais I priedo B dalies teksto reikalavimai ir apsaugos tikslų reikalavimai kartojami. Jei apsaugos tikslo reikalavimas ir tame reikalavime nurodytas I priedo B dalies teksto reikalavimas nesutampa, pirmenybę turi I priedo B dalies teksto reikalavimas.

Apsaugos tikslų nenurodyti I priedo B dalies teksto reikalavimai su apsaugos užtikrinimo funkcijomis nėra susiję.

Tam, kad pavojus, tikslus, procedūrines priemones ir SEF specifikacijas galima būtų rasti patobulinimų ir įvertinimo dokumentacijoje, jiems priskirti unikalūs žymekliai.

2. Santrumpos, apibrėžimai ir nuorodos

2.1. Santrumpos

PIN	asmeninės identifikacijos numeris;
ROM	pastovioji atmintis;
SEF	apsaugą užtikrinanti funkcija;
TBD	nustatyta;
TOE	įvertinimo tikslas;
VU	transporto priemonės blokas.

2.2. Apibrėžimai

Skaitmeninis tachografas	Tachografas
Duomenys apie judėjimą	Duomenys, kuriais keičiamasi su TPB, nurodantys greitį ir nuvažiuotą atstumą
Fiziškai atskirtos dalys	Judesio jutiklio fiziniai komponentai, išdėstyti transporto priemonėje (priešpriešinant judesio jutiklio korpuse esantiems fiziniams komponentams)
Apsauginiai duomenys	Ypatingi duomenys, reikalingi apsaugos užtikrinimo funkcijai veikti (pvz., kriptografiniai raktai)
Sistema	Įranga, žmonės ar organizacijos, kaip nors susiję su tachografu
Naudotojas	TPB naudojantis asmuo (kai nevartojama junginyje „duomenys apie naudotoją“)
Duomenys apie naudotoją	Visi TPB atmintyje įrašyti ir laikomi duomenys, išskyrus apsauginius, nurodyti III skyriaus 12 poskyryje

2.3. Nuorodos

ITSEC Informacinės technologijos apsaugos vertinimo kriterijai, 1991 m.

3. Gaminio apibūdinimas

3.1. Transporto priemonės bloko aprašymas ir naudojimo būdas

Transporto priemonės blokas skirtas montuoti į kelių transporto priemones. Jo paskirtis – įrašyti, laikyti atmintyje, rodyti ekrane, spausdinti ir išvesti duomenis apie vairuotojo veiklą.

Jis sujungiamas su judesio jutikliu, su kuriuo keičiasi duomenimis apie transporto priemonės judėjimą.

Naudotojai identifikuoja save TPB naudodami tachografo korteles.

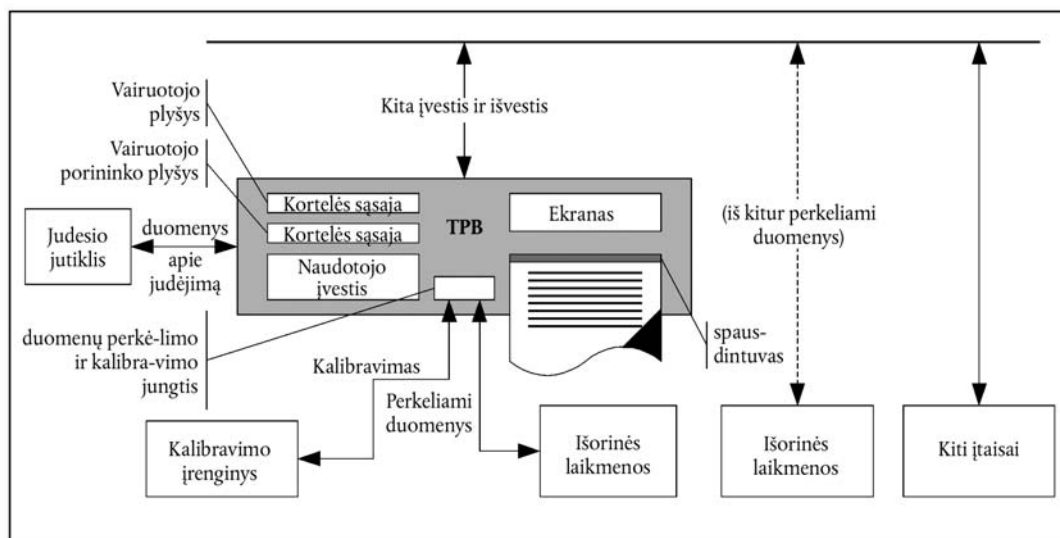
TPB įrašo ir laiko duomenis apie naudotojų veiklą savo atmintyje ir įrašo tuos duomenis į tachografo korteles.

TPB išveda duomenis į ekraną, spausdintuvą ir išorinius įrenginius.

Transporto priemonės bloko darbo aplinka įrengus jį transporto priemonėje pavaizduota toliau pateikiamame paveikslėlyje:

1 paveikslėlis

TPB darbo aplinka



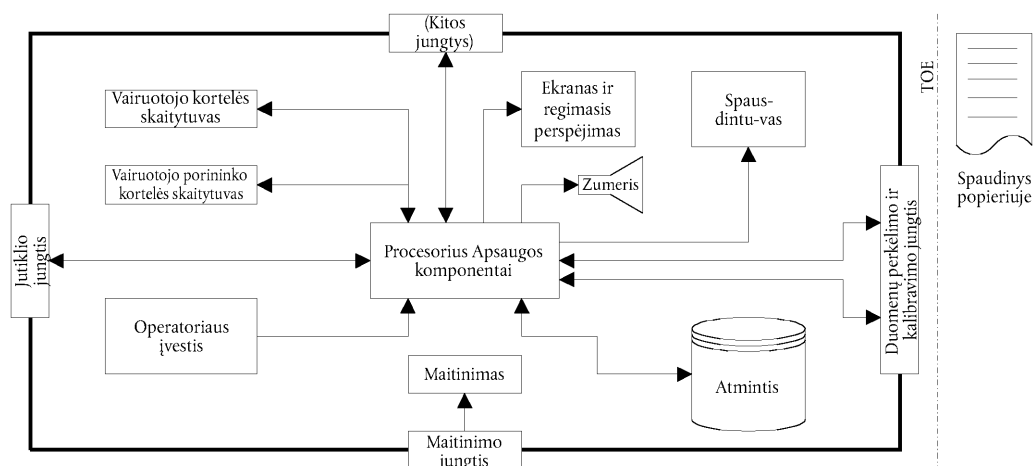
TPB bendrosios savybės, funkcijos ir darbo režimai aprašyti I priedo B dalies II skyriuje.

TPB funkciniai reikalavimai nurodyti I priedo B dalies III skyriuje.

Tipinis TPB pavaizduotas toliau pateikiamame paveikslėlyje.

2 paveikslėlis

Tipinis TPB (...) neprivalomas



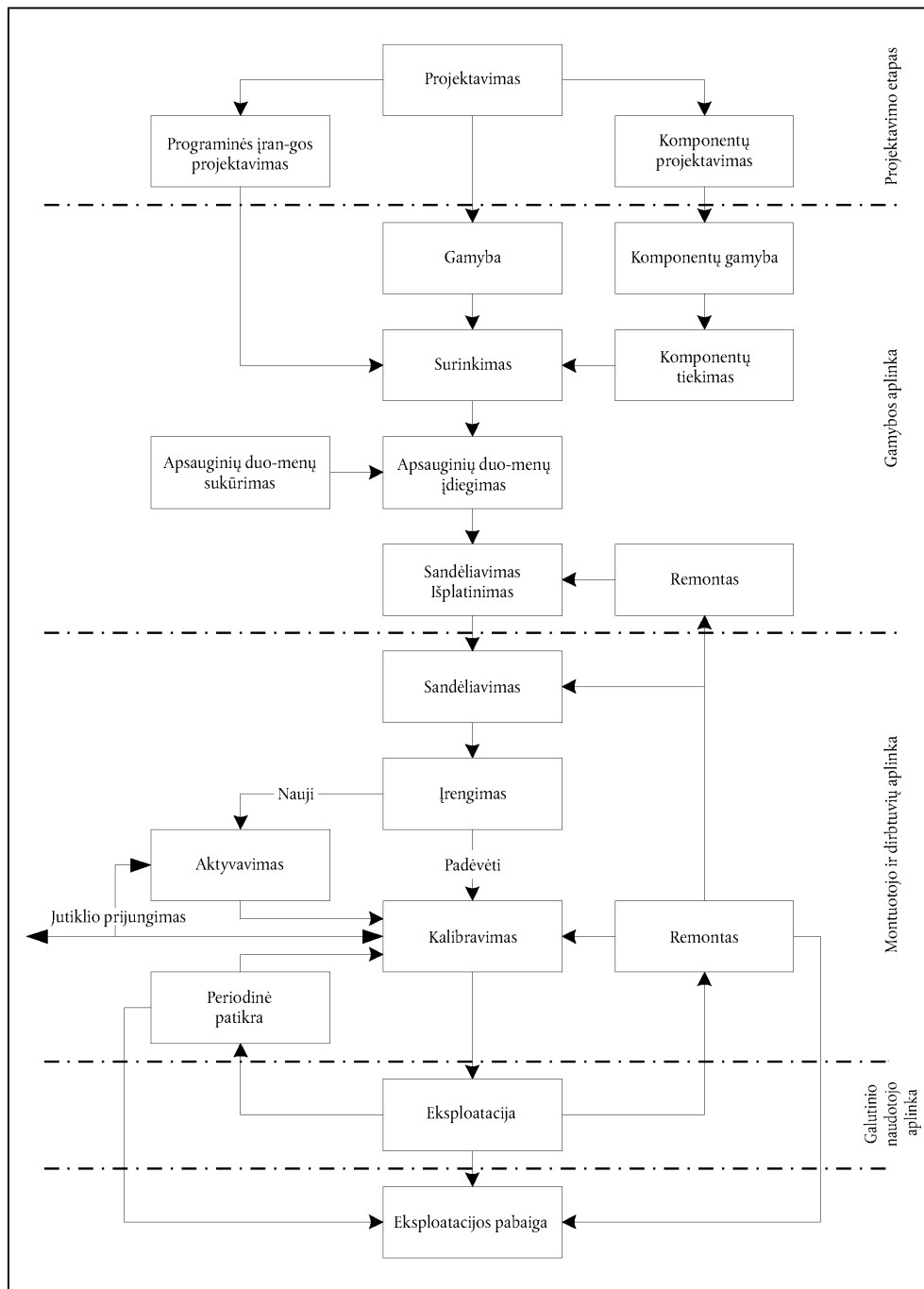
Reikia atkreipti dėmesį į tai, kad nors spausdintuvo mechanizmas yra TOE dalis, išspausdintas dokumentas – jau nebe.

3.2. Transporto priemonės bloko gyvavimo ciklas

Tipinis transporto priemonės bloko gyvavimo ciklas pavaizduotas toliau pateikiamame paveikslėlyje:

3 paveikslėlis

Tipinis transporto priemonės bloko gyvavimo ciklas



3.3. Pavojai

Šiame poskyryje aprašyti TPB galintys kilti pavojai.

3.3.1. Pavojai identifikacijos ir prieigos kontrolės strategijai

T.Access

Naudotojai gali mėginti pasinaudoti jiems neleistinomis funkcijomis (pvz., vairuotojai gali naudotis kalibravimo funkcija).

T.Identification

Naudotojai gali mėginti naudoti keletą identifikacijų arba jokios identifikacijos.

3.3.2. Su konstrukcija susiję pavojai

T.Faults	Dėl techninės, programinės įrangos, ryšio procedūrų sutrikimų gali sumažėti TPB apsaugotumas.
T.Tests	Taikant neleistinus bandymų metodus arba galimas kontrolės išvengimo galimybes gali sumažėti TPB apsaugotumas.
T.Design	Naudotojai gali mėginti neleistinai susipažinti su konstrukcija iš gamintojo medžiagos (ji gali būti pavagiama, gaunama už kyšius ir kt.) arba naudodamiesi inžinerine analize.

3.3.3. Su eksploatacija susiję pavojai

T.Calibration_Parameters	Naudotojai gali mėginti naudoti neteisingai sukalibruotą įrangą (pakeisti kalibravimo duomenis arba pasinaudoti organizacijos trūkumais).
T.Card_Data_Exchange	Naudotojai gali mėginti pakeisti duomenis keičiantis jais tarp TPB ir tachografo kortelių (juos papildyti, pakeisti, panaikinti, pakartoti signalą).
T.Clock	Naudotojai gali mėginti pakeisti vidinį laikrodį.
T.Environment	Naudotojai gali sumažinti TPB apsaugotumą aplinkos poveikiu (terminiu, elektromagnetiniu, optiniu, cheminiu, mechaniniu ir kt.).
T.Fake_Devices	Naudotojai gali mėginti prijungti prie TPB suklastotus įtaisus (judesio jutiklį, korteles su mikroschema).
T.Hardware	Naudotojai gali mėginti pakeisti TPB techninę įrangą.
T.Motion_Data	Naudotojai gali mėginti pakeisti duomenis apie transporto priemonės judėjimą (juos papildyti, pakeisti, panaikinti, pakartoti signalą).
T.Non_Activated	Naudotojai gali naudoti neaktyvuotą įrangą.
T.Output_Data	Naudotojai gali mėginti pakeisti išvedamus duomenis (spaudinius, rodinius ar perkeltamus duomenis).
T.Power_Supply	Naudotojai gali mėginti susidoroti su TPB apsauga – pakeisti jo maitinimą (jį nutraukti, sumažinti ar padidinti).
T.Security_Data	Naudotojai gali mėginti neleistinai susipažinti su apsauginiais duomenimis juos kuriant, perkeltiant arba sandėliuojant įrangą.
T.Software	Naudotojai gali mėginti pakeisti TPB programinę įrangą.
T.Stored_Data	Naudotojai gali mėginti pakeisti į atmintį įrašytus duomenis (apsauginius arba duomenis apie naudotoją).

3.4. Apsaugos tikslai

Pagrindinis skaitmeninės tachografo sistemos apsaugos tikslas yra toks:

O.Main	Kontrolės institucijų tikrinami duomenys turi būti prieinami. Jie visiškai tiksliai turi apibūdinti kontroliuojamų vairuotojų ir transporto priemonių veiklą: vairavimo, darbo, buvimo pasirengus dirbti ir poilsio laikotarpius, transporto priemonės greitį.
---------------	--

Todėl TPB apsaugos tikslas, kuris prisideda prie bendrojo apsaugos tikslo:

O.VU_Main Išmatuoti, užregistruoti ir kontrolės institucijų tikrinami duomenys turi būti prieinami. Jie visiškai tiksliai turi apibūdinti kontroliuojamų vairuotojų ir transporto priemonių veiklą: vairavimo, darbo, buvimo pasirengus dirbti ir poilsio laikotarpius, transporto priemonės greitį.

O.VU_Export TPB turi gebėti eksportuoti duomenis į išorines laikmenas taip, kad galima būtų patikrinti duomenų nepažeistumą ir autentiškumą.

3.5. Informacinės technologijos apsaugos tikslai

Specifiniai TPB IT apsaugos tikslai, prisidedantys prie pagrindinio apsaugos tikslo, yra tokie:

O.Access TPB turi kontroliuoti prijungto objekto prieigą prie funkcijų ir duomenų.

O.Accountability TPB turi kaupti tikslus atskaitomybės duomenis.

O.Audit TPB turi kontroliuoti bandymus pažeisti jo apsaugą ir atsekti juos iki susijusių objektų.

O.Authentication TPB turi tvirtinti naudotojų ir prijungtų objektų autentiškumą (kai tarp objektų reikia nustatyti patikimą maršrutą).

O.Integrity TPB turi išsaugoti atmintyje laikomų duomenų nepažeistumą.

O.Output TPB turi užtikrinti, kad išvedami duomenys tiksliai atitiktų išmatuotus ar į atmintį įrašytus duomenis.

O.Processing TPB turi užtikrinti, kad įvesties duomenys būtų tiksliai paverčiami duomenimis apie naudotoją.

O.Reliability TPB turi patikimai dirbti.

O.Secured_Data_Exchange TPB turi apsaugoti keitimąsi duomenimis su tachografo kortelėmis.

3.6. Fizinės, personalo arba procedūrinės priemonės

E bekezdés azon fizikai, személyzeti és eljárás követelményeket írja le, amelyek hozzájárulnak a JE biztonságához.

3.6.1. Įrangos konstrukcija

M.Development TPB projektuotojai turi užtikrinti, kad projektuojant atsakomybė būtų paskirstyta taip, jog būtų užtikrinta IT apsauga.

M.Manufacturing TPB gamintojai turi užtikrinti, kad gaminant atsakomybė būtų paskirstyta taip, jog būtų užtikrinta IT apsauga ir gamybos proceso metu judesio jutikliai būtų apsaugoti nuo fizinio poveikio, kuris galėtų sumažinti IT apsaugą.

3.6.2. Įrangos tiekimas

M.Delivery TPB gamintojai, transporto priemonių gamintojai ir montuotojai arba dirbtuvės turi užtikrinti, kad neaktyvuotais TPB būtų disponuojama taip, jog būtų užtikrinta IT apsauga.

M.Activation Transporto priemonių gamintojai ir montuotojai arba dirbtuvės turi aktyvuoti įrengtus TPB iki transporto priemonės išvykstant iš montavimo patalpų.

3.6.3. Apsauginių duomenų sukūrimas ir pateikimas

M.Sec_Data_Generation Apsauginių duomenų algoritmai turi būti prieinami tik įgaliotiems ir patikimiems asmenims.

M.Sec_Data_Transport Apsauginiai duomenys turi būti kuriami, perkelti ir įdiegiami į TPB užtikrinant reikiamą jų konfidencialumą ir nepažeistumą.

3.6.4. Kortelių pateikimas

M.Card_Availability	Tachografo kortelės turi būti prieinamos ir pateikiamos tik įgaliotiems asmenims.
M.Driver_Card_Uniqueness	Vairuotojai vienu metu gali turėti tik po vieną galiojančią vairuotojo kortelę.
M.Card_Traceability	Kortelių suteikimą turi būti galima atsekti (baltieji sąrašai, juodieji sąrašai), o atliekant apsaugotumo auditą turi būti naudojamos juodaisiais sąrašais.

3.6.5. Tachografų įrengimas, kalibravimas ir patikra

M.Approved_Workshops	Tachografus turi įrengti, kalibruoti ir remontuoti patikimi ir patvirtinti montuotojai ar dirbtuvės.
M.Regular_Inspections	Tachografai turi būti reguliariai tikrinami ir kalibruojami.
M.Faithful_Calibration	Kalibruodami patvirtinti montuotojai ir dirbtuvės turi įvesti į tachografą tinkamus transporto priemonės parametrus.

3.6.6. Įrangos naudojimas

M.Faithful_Drivers	Vairuotojai turi elgtis pagal taisyklės ir atsakingai (pvz., naudoti nuosavas vairuotojo korteles, tinkamai nurodyti rankomis įvedamus duomenis apie veiklą ir kt.).
---------------------------	--

3.6.7. Teisės aktų vykdymo kontrolė

M.Controls	Turi būti reguliariai ir atsitiktine tvarka atliekami teisės aktų vykdymo patikrinimai, kurių metu tikrinamas ir apsaugotumas.
-------------------	--

3.6.8. Programinės įrangos tobulinimas

M.Software_Upgrade	Prieš diegiant naujas programinės įrangos versijas į TPB, joms turi būti suteiktas apsaugotumo pažymėjimas.
---------------------------	---

4. Apsaugos užtikrinimo funkcijos

4.1. Identifikacija ir autentiškumo patvirtinimas

4.1.1. Judesio jutiklio identifikacija ir autentiškumo tikrinimas

UIA_201 TPB per kiekvieną sąveiką turi gebėti nustatyti bet kurio judesio jutiklio, prie kurio jis prijungtas, tapatybę.

UIA_202 Judesio jutiklio tapatybę turi sudaryti jutiklio patvirtinimo numeris ir serijos numeris.

UIA_203 TPB turi patikrinti judesio jutiklio, prie kurio jis prijungtas, autentiškumą:

- prijungiant judesio jutiklį,
- kiekvienąsyk kalibruojant tachografą,
- vėl atsiradus maitinimui.

Autentiškumo tikrinimas turi būti abipusis ir jį turi inicijuoti TPB.

UIA_204 TPB turi periodiškai (dažnumą nustato gamintojas; dažniau kaip kartą per valandą) pakartotinai tikrinti judesio jutiklio, prie kurio jis prijungtas, tapatybę ir autentiškumą, kad patikrintų, ar tachografo paskutinio kalibravimo metu identifikuotas judesio jutiklis nepasikeitė.

UIA_205 TPB turi aptikti ir neleisti naudotis autentiškumo tikrinimo duomenimis, kurie yra nukopijuoti ir siunčiami pakartotinai.

UIA_206 Aptikusi (ne daugiau kaip 20; nustato gamintojas) iš eilės nesėkmingų mėginimų patvirtinti autentiškumą ir (arba) aptikusi, kad judesio jutiklio tapatybė neleistinai (t. y. nekalibruojant tachografo) pasikeitė, SEF turi:

- užregistruoti įvykį audito įrašu,
- perspėti naudotoją,
- toliau priimti ir naudoti judesio jutiklio siunčiamus neapsaugotus duomenis apie judėjimą.

4.1.2. Naudotojo identifikacija ir autentiškumo tikrinimas

UIA_207 TPB turi nuolatos ir atskirai sekti dviejų naudotojų tapatybę, kontroliuodamas tachografo korteles, įkištas atitinkamai į įrangos vairuotojo ir vairuotojo porininko plyšį.

UIA_208 Naudotojo tapatybę turi sudaryti:

- naudotojų grupė:
 - VAIRUOTOJAS (vairuotojo kortelė),
 - KONTROLIERIUS (kontrolės kortelė),
 - DIRBTUVĖS (dirbtuvių kortelė),
 - ĮMONĖ (įmonės kortelė),
 - NEŽINOMA (kortelė neįkišta),
- naudotojo ID, kurią sudaro:
 - kortelę išduodančios valstybės narės kodas ir kortelės numeris,
 - NEŽINOMA, jei naudotojų grupė yra NEŽINOMA.

Tapatybės NEŽINOMA gali būti numanomos arba atvirai žinomos.

UIA_209 TPB turi patikrinti savo naudotojų autentiškumą įkišus kortelę.

UIA_210 TPB turi iš naujo patikrinti savo naudotojų autentiškumą:

- vėl atsiradus maitinimui,
- periodiškai arba įvykus ypatingiems įvykiams (nustato gamintojas – dažniau kaip kartą per dieną).

UIA_211 Autentiškumas turi būti tikrinamas išsiaiškinant, ar įkišta kortelė yra galiojanti tachografo kortelė su apsauginiais duomenimis, kuriuos platinti gali tik sistema. Autentiškumo tikrinimas turi būti abipusis ir inicijuojamas TPB.

UIA_212 Be pirmiau minėtų dalykų, dirbtuvių autentiškumas turi būti sėkmingai patikrintas pagal PIN. PIN turi būti ne trumpesnis kaip 4 rašmenų.

Pastaba: jei PIN perduodamas į TPB iš išorinės įrangos, kuri yra netoli TPB, PIN konfidencialumo perduodant užtikrinti nebūtina.

UIA_213 TPB turi aptikti ir neleisti naudotis autentiškumo tikrinimo duomenimis, kurie yra nukopijuoti ir siunčiami pakartotiniai.

UIA_214 Aptikusi 5 iš eilės nesėkmingus mėginimus patvirtinti autentiškumą, SEF turi:

- užregistruoti įvykį audito įrašu,
- perspėti naudotoją,
- laikyti naudotoją NEŽINOMU, o kortelę – negaliojančia (z apibrėžimas ir 097 reikalavimas).

4.1.3. Nuotoliniu būdu prisijungusios įmonės identifikacija ir autentiškumo tikrinimas

Nuotolinio sujungimo su įmone galimybė yra neprivaloma, todėl šis punktas galioja tik tuomet, jei ši funkcija yra įdiegta.

- UIA_215 Kiekvieną kartą sąveikaudamas su nuotoliniu būdu prisijungusia įmone TPB turi gebėti nustatyti įmonės tapatybę.
- UIA_216 Nuotoliniu būdu prisijungusios įmonės tapatybę turi sudaryti įmonės kortelę išduodančios valstybės narės kodas ir jos įmonės kortelės numeris.
- UIA_217 Prieš leisdamas eksportuoti bet kokius duomenis, TPB turi pavykti patikrinti nuotoliniu būdu prisijungusios įmonės autentiškumą.
- UIA_218 Autentiškumo tikrinimas turi būti atliekamas išsiaiškinant, ar įmonė turi galiojančią įmonės kortelę su apsauginiais duomenimis, kuriuos platinti gali tik sistema. Autentiškumo tikrinimas turi būti abipusis ir inicijuojamas TPB.
- UIA_219 TPB turi aptikti ir neleisti naudotis autentiškumo tikrinimo duomenimis, kurie yra nukopijuoti ir siunčiami pakartotinai.
- UIA_220 Aptikęs 5 iš eilės nesėkmingus mėginimus patvirtinti autentiškumą, TPB turi:

— perspėti nuotoliniu būdu prisijungusią įmonę.

4.1.4. Valdymo įrenginių identifikacija ir autentiškumo tikrinimas

TPB gamintojai gali numatyti specializuotus įrenginius papildomoms TPB valdymo funkcijoms (pvz., programinės įrangos tobulinimui, apsauginių duomenų pakartotiniam perkėlimui ir kt.) atlikti. Šis punktas galioja tik tuomet, jei ši funkcija yra įdiegta.

- UIA_221 Kiekvieną kartą sąveikaudamas su valdymo įrenginiu TPB turi gebėti nustatyti jo tapatybę.
- UIA_222 Prieš leisdamas toliau sąveikauti, TPB turi pavykti patikrinti valdymo įrenginio autentiškumą.
- UIA_223 TPB turi aptikti ir neleisti naudotis autentiškumo tikrinimo duomenimis, kurie yra nukopijuoti ir siunčiami pakartotinai.

4.2. Prieigos kontrolė

Prieigos kontrolė užtikrina, kad informaciją nuskaityti, sukurti ar keisti TOE galėtų tik tie, kam leidžiama tai daryti.

Reikia atkreipti dėmesį į tai, kad TPB užregistruojami duomenys apie naudotoją, nors susiję su asmeniškumo arba komercinio taktiškumo dalykais, nėra konfidencialūs. Todėl su duomenų nuskaitymo prieigos teisėmis susijusiems reikalavimams (011 reikalavimas) netaikomos apsaugą užtikrinančios funkcijos.

4.2.1. Prieigos kontrolės strategija

- ACC_201 TPB turi kontroliuoti prieigos prie funkcijų ir duomenų teises.

4.2.2. Prieigos prie funkcijų teisės

- ACC_202 TPB turi taikyti darbo režimo pasirinkimo taisykles (nuo 006 iki 009 reikalavimai).
- ACC_203 TPB panaudoti darbo režimą prieigos prie funkcijų valdymo taisyklėms taikyti (010 reikalavimas).

4.2.3. Prieigos prie duomenų teisės

- ACC_204 TPB turi taikyti TPB identifikacijos duomenų rašymo prieigos taisykles (076 reikalavimas).
- ACC_205 TPB turi taikyti prijungto judesio jutiklio identifikacijos duomenų rašymo prieigos taisykles (079 ir 155 reikalavimai).
- ACC_206 Po TPB aktyvavimo TPB turi užtikrinti, kad kalibravimo duomenys galėtų būti įvesti į TPB ir įrašyti į jo atmintį tik kalibravimo režimu (154 ir 156 reikalavimai).
- ACC_207 Po TPB aktyvavimo TPB turi taikyti kalibravimo duomenų rašymo ir panaikinimo prieigos taisykles (097 reikalavimas).

ACC_208 Po TPB aktyvavimo TPB turi užtikrinti, kad laiko koregavimo duomenys galėtų būti įvesti į TPB ir įrašyti į jo atmintį tik kalibravimo režimu (šis reikalavimas negalioja nedideliems laiko koregavimams, kuriuos leidžia 157 ir 158 reikalavimai).

ACC_209 Po TPB aktyvavimo TPB turi taikyti laiko koregavimo duomenų rašymo ir panaikinimo prieigos taisykles (100 reikalavimas).

ACC_210 TPB turi taikyti atitinkamas apsauginių duomenų nuskaitymo ir įrašymo prieigos taisykles (080 reikalavimas).

4.2.4. Rinkmenų struktūra ir prieigos sąlygos

ACC_211 Programos ir duomenų rinkmenų struktūra turi būti sudaryta gamybos proceso metu ir užblokuota taip, kad daugiau jos nebebūtų galima keisti ar panaikinti.

4.3. Atskaitomybė

ACT_201 TPB turi užtikrinti vairuotojų atskaitomybę už savo veiklą (081, 084, 087, 105a, 105b, 109 ir 109a reikalavimai).

ACT_202 TPB turi laikyti savo atmintyje nuolatinis identifikacijos duomenis (075 reikalavimas).

ACT_203 TPB turi užtikrinti dirbtuvių atskaitomybę už savo veiklą (098, 101 ir 109 reikalavimai).

ACT_204 TPB turi užtikrinti kontrolierių atskaitomybę už savo veiklą (102, 103 ir 109 reikalavimai).

ACT_205 TPB turi registruoti hodometro duomenis (090 reikalavimas) ir išsamius duomenis apie greitį (093 reikalavimas).

ACT_206 TPB turi užtikrinti, kad duomenys apie naudotoją, susiję su nuo 081 iki 093 ir nuo 102 iki 105b reikalavimais, kartą juos įrašius nebegalėtų būti pakeisti, išskyrus atvejus, kai jie tampa seniausiais užregistruotais duomenimis ir vietoj jų reikia įrašyti naujus duomenis.

ACT_207 TPB turi užtikrinti, kad nekeis tachografo kortelės atmintyje įrašytų duomenų (109 ir 109a reikalavimai), išskyrus seniausių duomenų keitimą naujais duomenimis (110 reikalavimas) arba 1 priedėlio 2.1 poskyrio pastaboje nurodytu atveju.

4.4. Auditas

Audito funkcijos reikalaujamos tik tiems įvykiams, kurie gali nurodyti klastojimą arba bandymą pažeisti apsaugą. Jos nereikalaujamos įprastai naudojantis teisėmis, net jei jos susijusios su apsauga.

AUD_201 TPB turi sugeneruoti audito įrašus apie jo apsaugą mažinančius įvykius (094, 096 ir 109 reikalavimai).

AUD_202 TPB apsaugą mažina tokie įvykiai:

- bandymai pažeisti apsaugą,
 - nepavykęs judesio jutiklio autentiškumo tikrinimas,
 - nepavykęs tachografo kortelės autentiškumo tikrinimas,
 - neleistinas judesio jutiklio pakeitimas,
 - kortelės duomenų įvesties nepažeistumo klaida,
 - atmintyje laikomų duomenų apie naudotoją nepažeistumo klaida,
 - vidinio duomenų perdavimo klaida,
 - neleistinas korpuso atidarymas,
 - kenkimas techninei įrangai,

- netinkamai užbaigta paskutinė kortelės panauda,
- judesio jutiklio klaidos įvykis,
- maitinimo nutrūkimo įvykis,
- TPB vidinis gedimas.

AUD_203 TPB turi taikyti audito įrašų laikymo taisykles (094 ir 096 reikalavimai).

AUD_204 TPB turi įrašyti į savo atmintį judesio jutiklio sukuriamus audito įrašus.

AUD_205 Audito įrašus turi būti galima spausdinti, matyti ekrane ir perkelti.

4.5. *Objektų pakartotinis naudojimas*

REU_201 TPB turi užtikrinti, kad laikinai atmintyje laikomus objektus galima būtų pakartotinai panaudoti nesudarant neleistinų informacijos srautų.

4.6. *Tikslumas*

4.6.1. *Informacijos srauto valdymo strategija*

ACR_201 TPB turi užtikrinti, kad duomenys apie naudotoją, susiję su 081, 084, 087, 090, 093, 102, 104, 105, 105a ir 109 reikalavimais, galėtų būti apdorojami tik gauti iš tinkamų įvesties šaltinių:

- duomenys apie transporto priemonės judėjimą,
- TPB esamojo laiko laikrodis,
- tachografo kalibravimo parametrai,
- tachografo kortelės,
- naudotojo įvestis.

ACR_201a TPB turi užtikrinti, kad galėtų būti įvesti tik laikotarpio nuo paskutinio kortelės ištraukimo iki dabartinio įkišimo duomenys apie naudotoją, susiję su 109a reikalavimu (050a reikalavimas).

4.6.2. *Vidinis duomenų perdavimas*

Šio punkto reikalavimai taikomi tik TPB, kurie naudoja fiziškai atskirtas dalis.

ACR_202 Jei duomenys perduodami tarp fiziškai atskirtų TPB dalių, jie turi būti apsaugoti nuo galimybės juos pakeisti.

ACR_203 Aptikus duomenų vidinio perdavimo klaidą turi būti bandoma siųsti iš naujo, o SEF turi sugeneruoti apie šį įvykį audito įrašą.

4.6.3. *Atmintyje laikomų duomenų nepažeistumas*

ACR_204 TPB turi tikrinti, ar jo atmintyje laikomuose duomenyse apie naudotoją nėra nepažeistumo klaidų.

ACR_205 Aptikusi atmintyje laikomuose duomenyse apie naudotoją nepažeistumo klaidų, SEF turi sugeneruoti audito įrašą.

4.7. *Ekspluatacinis patikimumas*

4.7.1. *Bandymai*

RLB_201 Visos bandymams gamybos etapu reikalingos komandos, veikimo rūšys ar bandymų vietos turi būti dezaktyvuotos arba pašalintos iki TPB aktyvavimo. Jų turi būti nebeįmanoma vėliau vėl panaudoti.

RLB_202 Pradinio paleidimo ir įprasto veikimo metu TPB pats tikrinti, ar veikia tinkamai. TPB savitakra turi aprępti apsauginių duomenų ir atmintyje laikomo vykdomojo kodo (jei jis nėra įrašytas į ROM) nepažeistumo tikrinimą.

RLB_203 Savitikros metu aptikusi vidinį gedimą, SEF turi:

- sugeneruoti audito įrašą (išskyrus kalibravimo režimu) (TPB vidinis gedimas),
- apsaugoti laikomus duomenis nepažeistus.

4.7.2. Programinė įranga

RLB_204 Neturi būti galimybių po TPB aktyvavimo vietoje analizuoti arba perprogramuoti programinę įrangą.

RLB_205 Įvestis iš išorinių šaltinių neturi būti priimama kaip vykdomasis kodas.

4.7.3. Fizinė apsauga

RLB_206 Jei TPB konstrukcija leidžia ją atidaryti, jis turi aptikti bet kokią korpuso atidarymą net ir nesant išorinio maitinimo ne mažiau kaip 6 mėnesius (išskyrus kalibravimo režimu). Tokiu atveju SEF turi sugeneruoti audito įrašą apie įvykį (leidžiama, kad audito įrašas būtų sugeneruotas ir įrašytas į atmintį atsiradus maitinimui).

Jei TPB negalima atidaryti, jo konstrukcija turi būti tokia, kad būtų lengvai matyti bandymo tai padaryti fiziniai požymiai (pvz., apžiūrėjus).

RLB_207 Po aktyvavimo TPB turi aptikti nustatytos rūšies (nustato gamintojas) kenkimą techninei įrangai.

RLB_208 Pirmiau nurodytu atveju SEF turi sugeneruoti audito įrašą, o TPB – (nustato gamintojas).

4.7.4. Maitinimo nutrūkimas

RLB_209 TPB turi aptikti nustatytų maitinimo parametrų pokyčius ir maitinimo nutrūkimą.

RLB_210 Pirmiau nurodytais atvejais SEF turi:

- sugeneruoti audito įrašą (išskyrus kalibravimo režimu),
- išlaikyti apsaugotą TPB būseną,
- gebėti naudoti apsaugines funkcijas, susijusias su tebeveikiančiais komponentais ar tebevykstančiais procesais,
- apsaugoti įrašytus duomenis.

4.7.5. Perkrovimo sąlygos

RLB_211 Nutrūkus maitinimui, sustabdžius operaciją jai nesibaigus arba bet kuriomis kitomis perkrovimo sąlygomis TPB turi būti perkrautas tinkamai.

4.7.6. Duomenų prieinamumas

RLB_212 TPB turi užtikrinti, kad prie sistemos elementų galima būtų prieiti, kai to reikia, ir kad to nebūtų reikalaujama ir nuo to nebūtų sulaikoma be reikalo.

RLB_213 TPB turi užtikrinti, kad kortelės negalėtų būti išvestos nebaigus rašyti į jas reikiamų duomenų (015 ir 016 reikalavimai).

RLB_214 Pirmiau nurodytu atveju SEF turi sugeneruoti audito įrašą.

4.7.7. Daugiafunkciškumas

RLB_215 Jei TPB be tachografo funkcijų atlieka ir kitas funkcijas, visos jos turi būti fiziškai ir (arba) logiškai atskirtos viena nuo kitos. Šių funkcijų apsauginiai duomenys turi būti skirtingi. Viena metu gali būti atliekama tik viena užduotis.

4.8. Keitimasis duomenimis

Šiame poskyryje aprašytas duomenų keitimasis tarp TPB ir prie jo prijungtų įrenginių.

4.8.1. Duomenų keitimasis su judesio jutikliu

DEX_201 TPB turi tikrinti iš judesio jutiklio importuotų duomenų nepažeistumą ir autentiškumą.

DEX_202 Aptikusi duomenų apie judėjimą nepažeistumo arba autentiškumo klaidą, SEF turi:

- sugeneruoti audito įrašą,
- toliau naudoti importuotus duomenis.

4.8.2. Duomenų keitimasis su tachografo kortelėmis

DEX_203 TPB turi tikrinti iš tachografo kortelių importuotų duomenų nepažeistumą ir autentiškumą.

DEX_204 Aptikusi duomenų apie judėjimą nepažeistumo arba autentiškumo klaidą, SEF turi:

- sugeneruoti audito įrašą,
- nenaudoti importuotų duomenų.

DEX_205 TPB turi eksportuoti duomenis apie judėjimą į tachografo korteles su atitinkamais apsaugos elementais taip, kad kortelės galėtų patikrinti jų nepažeistumą ir autentiškumą.

4.8.3. Duomenų keitimasis su išorinėmis laikmenomis (duomenų perkėlimo funkcija)

DEX_206 TPB turi sugeneruoti į išorines laikmenas perkeltų duomenų kilmės įrodymą.

DEX_207 TPB turi suteikti gavėjui galimybę patikrinti perkeltų duomenų kilmės įrodymą.

DEX_208 TPB turi perkelti duomenis į išorines laikmenas su atitinkamais apsaugos elementais taip, kad galima būtų patikrinti jų nepažeistumą ir autentiškumą.

4.9. Kriptografinė geba

Šio poskyrio reikalavimai taikomi tik tuomet, kai reikia, atsižvelgiant į naudojamus apsaugos mechanizmus ir gamintojo sprendimu.

CSP_201 Visos TPB atliekamos kriptografinės operacijos turi būti pagal nustatytą algoritmą ir rakto dydį.

CSP_202 Jei TPB generuoja kriptografinius raktus, tai turi būti daroma pagal nustatytus kriptografinių raktų kūrimo algoritmus ir raktų dydį.

CSP_203 Jei TPB platina kriptografinius raktus, tai turi būti daroma nustatytais kriptografinių raktų platinimo būdais.

CSP_204 Jei TPB priima kriptografinius raktus, tai turi būti daroma nustatytais kriptografinių raktų priėmimo būdais.

CSP_205 Jei TPB naikina kriptografinius raktus, tai turi būti daroma nustatytais kriptografinių raktų naikinimo būdais.

5. Apsaugos mechanizmų apibrėžimas

Reikalaujami apsaugos mechanizmai nustatyti 11 priedėlyje.

Visus kitus apsaugos mechanizmus nustato gamintojai.

6. Būtiniausias apsaugos mechanizmų neveikiamumas

TPB apsaugos mechanizmų neveikiamumas turi būti ne mažesnis kaip aukštas, kaip apibrėžta ITSEC.

7. Užtikrinimo lygis

TPB užtikrinimo lygis yra lygis E3 pagal ITSEC.

8. Apibūdinimas

Toliau esančiose lentelėse pateiktas SEF apibūdinimas, nurodantis:

- kurios SEF ar priemonės kovoja su pavojais,
- kurios SEF atitinka kuriuos IT apsaugos tikslus.

	Pavojai																		IT reikalavimai								
	Access [prieiga]	Identification [identifikacija]	Faults [gedimai]	Tests [bandymai]	Design [konstrukcija]	Calibration_Parameters [kalibravimo parametrai]	Card_Data_Exchange [keitimasis duomenimis su kortele]	Clock [laikrodis]	Environment [aplinka]	Fake_Devices [suklastoti įtaisai]	Hardware [techninė įranga]	Motion_Data [duomenys apie judėjimą]	Non_Activated [neaktyvuota]	Output_Data [išvesties duomenys]	Power_Supply [maitinimas]	Security_Data [apsauginiai duomenys]	Software [programinė įranga]	Stored Data [atmintvie laikomi duomenys]	Access [prieiga]	Accountability [atskaitomybė]	Audit [auditas]	Authentication [autentiškumo tikrinimas]	Integrity [nepažeistumas]	Output [išvestis]	Processing [apdorojimas]	Reliability [patikimumas]	Secured Data_Exchange [keitimasis apsaugotais duomenimis]
Fizinės, personalo, procedūrinės priemonės																											
Projektavimas			x	x	x																						
Gamyba				x	x																						
Tiekimas												x															
Aktyvavimas	x											x															
Apsauginių duomenų kūrimas																	x										
Apsauginių duomenų perdavimas																	x										
Kortelės pateikimas		x																									
Vieno vairuotojo kortelė		x																									
Kortelės atsekamumas		x																									
Patvirtintos dirbtuvės						x		x																			
Reguliari patikra ir kalibravimas						x		x				x	x			x											
Patikimo dirbtuvės						x		x																			
Patikimi vairuotojai		x																									
Teisės aktų vykdymo kontrolė		x				x		x	x		x		x		x		x	x									
Programinės įrangos tobulinimas																		x									
Apsaugos užtikrinimo funkcijos																											
Identifikacija ir autentiškumo tikrinimas																											
UIA_201 Jutiklio identifikacija										x	x											x					x
UIA_202 Jutiklio tapatybė										x	x											x					x
UIA_203 Jutiklio autentiškumo tikrinimas										x	x											x					x
UIA_204 Pakartotinė jutiklio identifikacija autentiškumo tikrinimas										x	x											x					x
UIA_205 Nesuklastojamas autentiškumo tikrinimas										x	x											x					
UIA_206 Autentiškumo tikrinimo nepavykimas										x	x											x				x	
UIA_207 Naudotojų identifikacija	x	x								x									x			x					x
UIA_208 Naudotojo tapatybė	x	x								x									x			x					x
UIA_209 Naudotojo autentiškumo tikrinimas	x	x								x									x			x					x
UIA_210 Pakartotinė jutiklio identifikacija autentiškumo tikrinimas	x	x								x									x			x					x
UIA_211 Autentiškumo tikrinimo priemonės	x	x								x									x			x					
UIA_212 PIN patikrinimai	x	x				x		x											x			x					
UIA_213 Nesuklastojamas autentiškumo tikrinimas	x	x								x									x			x					

	Pavojai																	IT reikalavimai									
	Access [priega]	Identification [identifikacija]	Faults [gedimai]	Tests [bandymai]	Design [konstrukcija]	Calibration_Parameters [kalibravimo parametrai]	Card_Data_Exchange [keitimasis duomenimis su kortele]	Clock [laikrodis]	Environment [aplinka]	Fake_Devices [suklastoti įtaisai]	Hardware [techninė įranga]	Motion_Data [duomenys apie judėjimą]	Non_Activated [neaktyvuota]	Output_Data [išvesties duomenys]	Power_Supply [maitinimas]	Security_Data [apsauginiai duomenys]	Software [programinė įranga]	Stored Data [atminties laikomi duomenys]	Access [priega]	Accountability [atskaitomybė]	Audit [auditas]	Authentication [autentiškumo tikrinimas]	Integrity [nepažeistumas]	Output [išvestis]	Processing [apdorojimas]	Reliability [patikimumas]	Secured Data_Exchange [keitimasis apsaugotais duomenimis]
UIA_214 Autentiškumo tikrinimo nepavykimas	x	x							x												x						
UIA_215 Nutolusiojo naudotojo identifikacija	x	x																	x			x					x
UIA_216 Nutolusiojo naudotojo tapatybė	x	x																	x			x					
UIA_217 Nutolusiojo naudotojo autentiškumo tikrinimas	x	x																	x			x					x
UIA_218 Autentiškumo tikrinimo priemonės	x	x																	x			x					
UIA_219 Nesuklastojamas autentiškumo tikrinimas	x	x																	x			x					
UIA_220 Autentiškumo tikrinimo nepavykimas	x	x																									
UIA_221 Valdymo įrenginio identifikacija	x	x																	x			x					
UIA_222 Valdymo įrenginio autentiškumo tikrinimas	x	x																	x			x					
UIA_223 Nesuklastojamas autentiškumo tikrinimas	x	x																	x			x					
Prieigos kontrolė																											
ACC_201 Prieigos kontrolės strategija	x					x	x										x		x	x							
ACC_202 Prieigos prie funkcijų teisės	x					x	x													x							
ACC_203 Prieigos prie funkcijų teisės	x					x	x													x							
ACC_204 TPB ID																			x	x							
ACC_205 Prijungto jutiklio ID									x										x	x							
ACC_206 Kalibravimo duomenys	x					x													x	x							
ACC_207 Kalibravimo duomenys						x													x	x							
ACC_208 Duomenys apie laiko koregavimą							x												x	x							
ACC_209 Duomenys apie laiko koregavimą							x												x	x							
ACC_210 Apsauginiai duomenys																	x		x	x							
ACC_211 Rinkmenų struktūra ir prieigos sąlygos	x					x											x		x	x							
Atskaitomybė																											
ACT_201 Viruotojo atskaitomybė																				x							
ACT_202 TPB ID duomenys																				x	x						
ACT_203 Dirbtuvių atskaitomybė																				x							
ACT_204 Įmonės atskaitomybė																				x							
ACT_205 Transporto priemonės judėjimo atskaitomybė																				x							
ACT_206 Atskaitomybės duomenų keitimas																			x				x			x	
ACT_207 Atskaitomybės duomenų keitimas																			x				x			x	

	Pavojai																IT reikalavimai										
	Access [priega]	Identification [identifikacija]	Faults [gedimai]	Tests [bandymai]	Design [konstrukcija]	Calibration_Parameters [kalibravimo parametrai]	Card_Data_Exchange [keitimasis duomenimis su kortele]	Clock [laikrodis]	Environment [aplinka]	Fake_Devices [suklastoti įtaisai]	Hardware [techninė įranga]	Motion_Data [duomenys apie judėjimą]	Non_Activated [neaktyvuota]	Output_Data [išvesties duomenys]	Power_Supply [maitinimas]	Security_Data [apsauginiai duomenys]	Software [programinė įranga]	Stored Data [atmintvie laikomi duomenys]	Access [priega]	Accountability [atskaitomybė]	Audit [auditas]	Authentication [autentiškumo tikrinimas]	Integrity [nepažeistumas]	Output [išvestis]	Processing [apdorojimas]	Reliability [patikimumas]	Secured Data Exchange [keitimasis apsaugotais duomenimis]
Auditas																											
AUD_201 Audito įrašai																					x						
AUD_202 Audito įvykių sąrašas	x					x				x	x			x	x			x			x						
AUD_203 Audito įrašų laikymo taisyklės																					x						
AUD_204 Jutiklio audito įrašai																					x						
AUD_205 Audito priemonės																					x						
Pakartotinis naudojimas																											
REU_201 Pakartotinis naudojimas																x										x	x
Tikslumas																											
ACR_201 Informacijos srauto valdymo strategija						x			x		x														x	x	
ACR_202 Vidinis perdavimas														x										x	x	x	
ACR_203 Vidinis perdavimas														x													
ACR_204 Laikomų duomenų nepažeistumas																		x					x			x	
ACR_205 Laikomų duomenų nepažeistumas																		x			x						
Patikimumas																											
RLB_201 Gamybos bandymai				x	x																					x	
RLB_202 Savitikra			x								x				x		x									x	
RLB_203 Savitikra											x				x		x				x						
RLB_204 Programinės įrangos analizė						x												x								x	
RLB_205 Programinės įrangos įvestis																		x					x	x	x		
RLB_206 Korpuso atidarymas					x			x	x			x				x	x	x					x			x	
RLB_207 Kenkimas techninei įrangai											x															x	
RLB_208 Kenkimas techninei įrangai											x										x						
RLB_209 Maitinimo nutrūkimas															x											x	
RLB_210 Maitinimo nutrūkimas															x						x						
RLB_211 Perkrovimas			x																							x	
RLB_212 Duomenų prieinamumas																								x	x		
RLB_213 Kortelės išvedimas																										x	
RLB_214 Kortelės panauda pabaigta netinkamai																						x					
RLB_215 Daugiafunkciškumas																										x	
Keitimasis duomenimis																											
DEX_201 Apsaugotų duomenų apie judėjimą importas												x															x
DEX_202 Apsaugotų duomenų apie judėjimą importas												x						x									
DEX_203 Apsaugotų duomenų iš kortelės importas						x																					x

TACHOGRAFO KORTELĖS BENDRIEJI APSAUGOS TIKSLAI

1. Įvadas

Šiame dokumente aprašyta tachografo kortelė, pavojai, kuriuos ji turi gebėti įveikti, ir apsaugos tikslai, kuriuos ji turi atitikti. Čia nurodytos reikiamos apsaugos užtikrinimo funkcijos, reikalaujamas apsaugos mechanizmų neįveikiamumas ir reikiamas tobulinimo bei vertinimo užtikrinimo lygis.

Šiame dokumente nurodyti reikalavimai iš I priedo B dalies teksto. Kad būtų aiškiau skaityti, kartais I priedo B dalies teksto reikalavimai ir apsaugos tikslų reikalavimai kartojami. Jei apsaugos tikslų reikalavimas ir tame reikalavime nurodytas I priedo B dalies teksto reikalavimas nesutampa, pirmenybę turi I priedo B dalies teksto reikalavimas.

Apsaugos tikslų reikalavimų nenurodyti I priedo B dalies teksto reikalavimai su apsaugos užtikrinimo funkcijomis nėra susiję.

Tachografo kortelė yra standartinė kortelė su mikroschema, turinti naudojimo su tachografu paskirtį. Ji turi atitikti tokioms kortelėms taikomus naujausius funkcinis ir apsaugos užtikrinimo reikalavimus. Todėl šiame skyriuje nurodyti tik papildomi apsaugos reikalavimai, kurių, atsižvelgiant šią paskirtį, reikia.

Tam, kad pavojus, reikalavimus, procedūrinės priemonės ir SEF specifikacijas galima būtų rasti patobulinimų ir įvertinimo dokumentacijoje, jiems priskirti unikalūs žymekliai.

2. Santrumpos, apibrėžimai ir nuorodos**2.1. Santrumpos**

IC	integrinis grandynas (elektroninis komponentas, skirtas duomenų apdorojimo ir (arba) atminties funkcijoms atlikti);
OS	operacinė sistema;
PIN	asmeninės identifikacijos numeris;
ROM	pastovioji atmintis;
SFP	apsauginių funkcijų strategija;
TBD	nustatytina;
TOE	įvertinimo tikslas;
TSF	TOE apsauginė funkcija;
TPB	transporto priemonės blokas.

2.2. Apibrėžimai

Skaitmeninis tachografas	Tachografas.
Svarbūs duomenys	Tachografo kortelės atmintyje laikomi duomenys, kuriuos reikia saugoti nuo pažeidimo, neleistino pakeitimo ir dėl konfidencialumo (kai taikytina – dėl apsauginių duomenų). Svarbius duomenis sudaro apsauginiai duomenys ir duomenys apie naudotoją.
Apsauginiai duomenys	Ypatingi duomenys, reikalingi apsaugos užtikrinimo funkcijai veikti (pvz., kriptografiniai raktai).
Sistema	Įranga, žmonės ar organizacijos, kaip nors susiję su tachografu.
Naudotojas	Bet koks TOE nepriklausantis ir su juo sąveikaujantis subjektas (žmogus arba išorinis IT subjektas) (kai nevertinama junginyje „duomenys apie naudotoją“).

Duomenys apie naudotoją	Tachografo kortelės atmintyje laikomi svarbūs duomenys, išskyrus apsauginius. Duomenis apie naudotoją sudaro identifikacijos duomenys ir duomenys apie veiklą.
Identifikacijos duomenys	Identifikacijos duomenis sudaro kortelės identifikacijos duomenys ir kortelės turėtojo identifikacijos duomenys.
Kortelės identifikacijos duomenys	Duomenys apie naudotoją, susiję su kortelės identifikacija, kaip apibrėžta 190, 191, 192, 194, 215, 231 ir 235 reikalavimuose.
Kortelės turėtojo identifikacijos duomenys	Duomenys apie naudotoją, susiję su kortelės turėtojo identifikacija, kaip apibrėžta 195, 196, 216, 232 ir 236 reikalavimuose.
Duomenys apie veiklą	Duomenis apie veiklą sudaro duomenys apie kortelės turėtojo veiklą, įvykius bei gedimus ir kontrolės veiklą.
Duomenys apie kortelės turėtojo veiklą	Duomenys apie naudotoją, susiję su kortelės turėtojo vykdoma veikla, kaip apibrėžta 197, 199, 202, 212, 212a, 217, 219, 221, 226, 227, 229, 230a, 233 ir 237 reikalavimuose.
Duomenys apie įvykius ir gedimus	Duomenys apie naudotoją, susiję su įvykiais ir gedimais, kaip apibrėžta 204, 205, 207, 208 ir 223 reikalavimuose.
Duomenys apie kontrolės veiklą	Duomenys apie naudotoją, susiję su teisės aktų vykdymo kontrole, kaip apibrėžta 210 ir 225 reikalavimuose.

2.3. Nuorodos

ITSEC	Informacinės technologijos apsaugos vertinimo kriterijai, 1991 m.
IC PP	Kortelių integrinių grandynų apsaugos profilis. 2.0 versija, 1998 m. rugsėjo mėnesio leidimas. Užregistruota Prancūzijos sertifikavimo institucijoje numeriu PP/9806.
ES PP	Kortelių integrinių grandynų su įdiegta programine įranga apsaugos profilis. 2.0 versija, 1999 m. birželio mėnesio leidimas. Užregistruota Prancūzijos sertifikavimo institucijoje numeriu PP/9911.

3. Gaminio apibūdinimas

3.1. Tachografo kortelės aprašymas ir naudojimo būdas

Tachografo kortelė yra kortelė su mikroschema, kaip aprašyta IC PP ir ES PP, su programa, skirta naudoti tachografuose.

Pagrindinės tachografo kortelės funkcijos yra tokios:

- laikyti kortelės ir kortelės turėtojo identifikacijos duomenis. Šiuos duomenis transporto priemonės blokas naudoja kortelės turėtojiui identifikuoti, prieigos prie atitinkamų funkcijų ir duomenų teisėms suteikti ir kortelės atskaitomybei už savo veiksmus užtikrinti;
- laikyti duomenis apie kortelės turėtojo veiklą, įvykius bei gedimus ir kontrolės veiklą, susijusius su kortelės turėtoju.

Taigi tachografo kortelė yra skirta transporto priemonės bloko sąsajos įtaisui. Ją taip pat gali naudoti bet koks kortelių nuskaitymo įrenginys (pvz., asmeninis kompiuteris), kuris turi turėti visas nuskaitymo prieigos teises visiems duomenims apie naudotoją.

Tachografo kortelės gyvavimo ciklo galutinio naudojimo etapu (7 gyvavimo ciklo etapas, kaip aprašyta ES PP), transporto priemonės blokai gali rašyti į kortelę tik duomenis apie naudotoją.

Tachografo kortelės funkciniai reikalavimai nustatyti I priedo B dalies tekste ir 2 priedėlyje.

3.2. Tachografo kortelės gyvavimo ciklas

Tachografo kortelės gyvavimo ciklas atitinka ES PP aprašytą kortelių su mikroschema gyvavimo ciklą.

3.3. Pavojai

Be ES PP ir IC PP išvardytų bendrųjų kortelių su mikroschema pavojų, tachografo kortelei gali kilti dar tokie pavojai:

3.3.1. Pavojai identifikacijos ir prieigos kontrolės strategijai

Text Missing!!!

T.Ident_Data	Sėkmingai pakeitus TOE turimus identifikacijos duomenis (pvz., kortelės rūšį, kortelės galiojimo pabaigos datą arba kortelės turėtojo identifikacijos duomenis) galima būtų apgaulingai naudoti TOE ir tai keltų didelį pavojų bendrajam sistemos apsaugotumui.
T.Activity_Data	Sėkmingas TOE laikomų duomenų apie veiklą pakeitimas keltų pavojų TOE apsaugotumui.
T.Data_Exchange	Sėkmingas duomenų apie veiklą pakeitimas (papildymas, panaikinimas, pakeitimas) juos importuojant arba eksportuojant keltų pavojų TOE apsaugotumui.

3.3.2. Kenkimo būdai

TOE gali būti pakenkta:

- bandant nelegaliai susipažinti su TOE technine ir programine įranga, ypač – su apsauginėmis funkcijomis ir apsauginiais duomenimis. Nelegalios žinios gali būti įgyjamos iš projektuotojo arba gamintojo medžiagos (jos gali būti pavagiamos, gaunamos už kyšius ir kt.) arba tiesiogiai ištyrus TOE (fiziniais bandymais, išvadine analize ir kt.),
- naudojantis TOE konstrukcijos arba pagaminimo trūkumais (techninės, programinės įrangos klaidomis, siuntimo sutrikimais, dėl aplinkos poveikio TOE atsiradusiomis klaidomis, apsaugos funkcijų – autentiškumo tikrinimo procedūrų, duomenų prieigos kontrolės, kriptografinių operacijų ir kt. – trūkumais),
- pakeitus TOE arba jo apsaugos funkcijas fizinėmis, elektroninėmis arba loginėmis priemonėmis ar jų deriniu.

3.4. Apsaugos tikslai

Pagrindinis skaitmeninės tachografo sistemos apsaugos tikslas yra toks:

O.Main	Kontrolės institucijų tikrinami duomenys turi būti prieinami. Jie visiškai tiksliai turi apibūdinti kontroliuojamų vairuotojų ir transporto priemonių veiklą: vairavimo, darbo, buvimo pasirengus dirbti ir poilsio laikotarpius, transporto priemonės greitį.
---------------	--

Todėl pagrindinis TOE apsaugos tikslas, kuris prisideda prie bendrojo apsaugos tikslo, yra toks:

O.Card_Identification_Data	TOE turi apsaugoti kortelės suasmeninimo proceso metu joje įrašytus kortelės ir kortelės turėtojo identifikacijos duomenis.
O.Card_Activity_Storage	TOE turi apsaugoti kortelės atmintyje transporto priemonės blokų įrašytus duomenis apie naudotoją.

3.5. Informacinės technologijos apsaugos tikslai

Be ES PP ir IC PP išvardytų bendrųjų kortelių su mikroschema apsaugos tikslų, specifiniai TOE IT apsaugos tikslai, prisidedantys prie pagrindinio apsaugos tikslo, gyvavimo ciklo galutinio naudojimo etapu yra tokie:

O.Data_Access	TOE turi suteikti duomenų įrašymo teises tik tiems transporto priemonių blokam, kurių autentiškumas patikrintas.
O.Secure_Communications	TOE turi gebėti naudoti saugaus ryšio protokolus ir procedūras tarp kortelės ir kortelės sąsajos įtaiso, kai to reikia programai.

3.6. Fizinės, personalo arba procedūrinės priemonės

Fiziniai, personalo arba procedūriniai reikalavimai, kurie didina TOE apsaugą, išvardyti ES PP ir IC PP (skyriuose apie apsaugos nuo aplinkos poveikio reikalavimus).

4. Apsaugos užtikrinimo funkcijos

Šiame skyriuje išsamiau aprašytos kai kurios leistinos operacijos, pvz., paskyrimo ar pasirinkimo pagal ES PP, ir nurodyti papildomi SEF funkciniai reikalavimai.

4.1. Atitiktis apsaugos profiliams

CPP_301 TOE turi atitikti IC PP.

CPP_302 TOE turi atitikti ES PP kaip išsamiau aprašyta toliau.

4.2. Naudotojo identifikacija ir autentiškumo patvirtinimas

Kortelė turi identifikuoti objektą, į kurį yra įkišta, ir nustatyti, ar tai yra patvirtinto autentiškumo transporto priemonės blokas, ar ne. Kortelė gali eksportuoti bet kokius duomenis į objektą, prie kurio ji yra prijungta, išskyrus kontrolės kortelę, kuri gali eksportuoti kortelės turėtojo identifikacijos duomenis tik į patvirtinto autentiškumo transporto priemonės blokus (kad kontrolierius būtų užtikrintas, jog transporto priemonės blokas nėra suklaidintas, matydamas jo pavadinimą ekrane ir spaudiniuose).

4.2.1. Naudotojo identifikacija

Užduotis (FIA_UID.1.1) *Veiksmų, atliekamų per TSF, sąrašas:* nė vieno.

Užduotis (FIA_ATD.1.1) *Apsaugos atributų sąrašas:*

USER_GROUP VEHICLE_UNIT, NON_VEHICLE_UNIT,

USER_ID transporto priemonės registracijos numeris (TPRN) ir valstybės narės kodas (USER_ID žinomas tik tuomet, kai USER_GROUP = VEHICLE_UNIT).

4.2.2. Naudotojo autentiškumo tikrinimas

Užduotis (FIA_UAU.1.1) *Veiksmų, atliekamų per TSF, sąrašas:*

- vairuotojo ir dirbtuvių kortelės: duomenų apie naudotoją su apsaugos atributais eksportas (duomenų iš kortelės perkėlimo funkcija),
- kontrolės kortelė: duomenų apie naudotoją be apsaugos (išskyrus kortelės turėtojo identifikacijos duomenis) atributų eksportas.

UIA_301 Transporto priemonės bloko autentiškumas turi būti tikrinamas išsiaiškinant, ar jis turi apsauginius duomenis, kuriuos platinti gali tik sistema.

Pasirinkimas (FIA_UAU.3.1 ir FIA_UAU.3.2): apsaugoti.

Užduotis (FIA_UAU.4.1) *Identifikuotas autentiškumo tikrinimo mechanizmas (-ai):* bet koks autentiškumo tikrinimo mechanizmas.

UIA_302 Dirbtuvių kortelė turi suteikti papildomą autentiškumo tikrinimo mechanizmą patikrindama PIN kodą (šis mechanizmas skirtas transporto priemonės blokui, kad jis nustatytų kortelės turėtojo tapatybę – jis neskirtas dirbtuvių kortelės turiniui apsaugoti).

4.2.3. Autentiškumo tikrinimo nepavykimas

Toliau nurodytos užduotys apibūdina kortelės reakciją į kiekvieną nepavykusį naudotojo autentiškumo tikrinimą.

Užduotis (FIA_AFL.1.1) *Numeris: 1, autentiškumo tikrinimo įvykių sąrašas:* kortelės sąsajos įtaiso autentiškumo tikrinimas.

Užduotis (FIA_AFL.1.2) *Veiksmų sąrašas:*

- perspėti prijungtą objektą,
- laikyti naudotoją NON_VEHICLE_UNIT.

Toliau nurodytos užduotys apibūdina kortelės reakciją į nepavykusį autentiškumo tikrinimą pagal UIA_302 reikalaujamą papildomą autentiškumo tikrinimo mechanizmą.

Užduotis (FIA_AFL.1.1) *Numeris: 5, autentiškumo tikrinimo įvykių sąrašas:* PIN patikrinimas (dirbtuvių kortelė).

Užduotis (FIA_AFL.1.2) *Veiksmų sąrašas:*

- perspėti prijungtą objektą,
- užblokuoti PIN tikrinimo procedūrą taip, kad kitas PIN tikrinimo mėginimas nepavyktų,
- gebėti nurodyti vėlesniems naudotojams užblokavimo priežastį.

4.3. **Prieigos kontrolė**

4.3.1. *Prieigos kontrolės strategija*

Tachografo kortelei jos gyvavimo ciklo galutinio naudojimo etapu taikoma viena prieigos kontrolė pagal apsauginės funkcijos strategiją (SFP), vadinama AC_SFP.

Užduotis (FDP_ACC.2.1) *Prieigos kontrolė SFP:* AC_SFP.

4.3.2. *Prieigos kontrolės funkcijos*

Užduotis (FDP_ACF.1.1) *Prieigos kontrolė SFP:* AC_SFP.

Užduotis (FDP_ACF.1.1) *A biztonsígi attrib/tumok megnevezett csoportja:* USER_GROUP.

Užduotis (FDP_ACF.1.2) *Prieigos tarp kontroliuojamų subjektų ir objektų, naudojant kontroliuojamas operacijas su kontroliuojamais objektais, taisyklės::*

GENERAL_READ: Duomenis apie naudotoją iš TOE gali nuskaityti bet kuris naudotojas (išskyrus kortelės turėtojo identifikacijos duomenis, kuriuos iš kontrolės kortelių gali nuskaityti tik VEHICLE_UNIT).

IDENTIF_WRITE: Identifikacijos duomenys gali būti įrašyti tik kartą ir iki kortelės gyvavimo ciklo 6-ojo etapo. Jokie naudotojai negali įrašyti ar keisti identifikacijos duomenų kortelės gyvavimo ciklo galutinio naudojimo etapu.

ACTIVITY_WRITE: Duomenis apie veiklą į TOE gali įrašyti tik VEHICLE_UNIT.

SOFT_UPGRADE: Joks naudotojas negali atnaujinti TOE programinės įrangos.

FILE_STRUCTURE: Rinkmenų struktūra ir prieigos sąlygos turi būti sukurtos iki TOE gyvavimo ciklo 6-ojo etapo pabaigos ir užblokuotos, kad vėliau jų negalėtų pakeisti ar panaikinti joks naudotojas.

4.4. **Atskaitomybė**

ACT_301 TOE turi laikyti savo atmintyje nuolatinius identifikacijos duomenis.

ACT_302 Turi būti nurodyta TOE suasmeninimo data ir laikas. Tokia nuoroda turi būti nepakeičiama.

4.5. **Auditas**

TOE turi stebėti įvykius, kurie nurodo galimą apsaugos pažeidimą.

Užduotis (FAU_SAA.1.2) *Nustatytų kontroliuotinių įvykių poaibis:*

- nepavykęs kortelės turėtojo autentiškumo tikrinimas (5 iš eilės nesėkmingi PIN patikrinimai),
- savitikros klaida,
- atmintyje laikomų duomenų nepažeistumo klaida,
- duomenų apie veiklą įvesties klaida.

4.6. **Tikslumas**

4.6.1. *Atmintyje laikomų duomenų nepažeistumas*

Užduotis (FDP_SDL.2.2) *Veiksmai, kurių turi būti imtasi:* perspėti prijungtą objektą.

4.6.2. *Pagrindinis duomenų autentiškumo tikrinimas*

Užduotis (FDP_DAU.1.1) *Objektų arba informacijos rūšių sąrašas:* duomenys apie veiklą.

Užduotis (FDP_DAU.1.2) *Objektų sąrašas:* bet kokie.

4.7. *Eksplotacinis patikimumas*

4.7.1. *Bandymai*

Pasirinkimas (FPT_TST.1.1): pradinio paleidimo metu, periodiškai įprasto veikimo metu.

Pastaba: „pradinio paleidimo metu“ reiškia iki kodas yra įvykdomas (ir nebūtinai per atsakymo į perkrovimą procedūrą).

RLB_301 TOE savitakra turi būti patikrintas bet kokio ne ROM laikomo programinės įrangos kodo nepažeistumas.

RLB_302 Aptikusi savitikros klaidą, TSF turi perspėti prijungtą objektą.

RLB_303 Pabaigus OS tikrinimą visos su bandymais susiję komandos ir veikimo rūšys turi būti dezaktyvuotos arba pašalintos. Šių valdymo priemonių turi būti nebeįmanoma panaikinti arba atkurti. Vien su tam tikru gyvavimo ciklo etapu susijusi komanda turi būti nebepasiekama kitu etapu.

4.7.2. *Programinė įranga*

RLB_304 Neturi būti galimybių vietoje analizuoti, perprogramuoti arba pakeisti TOE programinę įrangą.

RLB_305 Įvestis iš išorinių šaltinių neturi būti priimama kaip vykdomasis kodas.

4.7.3. *Maitinimo nutrūkimas*

RLB_306 Nutrūkus arba kintant maitinimui TOE turi išlaikyti saugią būseną.

4.7.4. *Perkrovimo sąlygos*

RLB_307 Nutrūkus TOE maitinimui (arba kintant įtampai), sustabdžius operaciją jai nesibaigus arba bet kuriomis kitomis perkrovimo sąlygomis TOE turi būti perkrautas tinkamai.

4.8. *Keitimasis duomenimis*

4.8.1. *Duomenų keitimasis su transporto priemonės bloku*

DEX_301 TPB turi tikrinti iš transporto priemonės bloko importuotų duomenų nepažeistumą ir autentiškumą.

DEX_302 Aptikus importuotų duomenų nepažeistumo klaidą, TOE turi:

— perspėti duomenis siunčiantį objektą,

— nenaudoti duomenų.

DEX_303 TOE turi eksportuoti duomenis apie naudotoją su apsaugos elementais į transporto priemonės bloką taip, kad jis galėtų patikrinti gautų duomenų nepažeistumą ir autentiškumą.

4.8.2. *Duomenų eksportas ne į transporto priemonės bloką (duomenų perkėlimo funkcija)*

DEX_304 TOE turi gebėti sukurti į išorines laikmenas perkeltų duomenų kilmės įrodymą.

DEX_305 TOE turi gebėti suteikti gavėjui galimybę patikrinti perkeltų duomenų kilmės įrodymą.

DEX_306 TOE turi gebėti perkelti duomenis į išorines laikmenas su atitinkamais apsaugos elementais taip, kad galima būtų patikrinti jų nepažeistumą ir autentiškumą.

4.9. *Kriptografinė geba*

CSP_301 Jei TSF generuoja kriptografinius raktus, tai turi būti daroma pagal nustatytus kriptografinių raktų kūrimo algoritmus ir raktų dydį. Sugeneruoti kriptografinio seanso raktai turi turėti ribotas naudojimo galimybes (jų skaičių nustato gamintojas – ne daugiau kaip 240).

CSP_302 Jei TSF platina kriptografinius raktus, tai turi būti daroma nustatytais kriptografinių raktų platinimo būdais.

5. *Apsaugos mechanizmų apibrėžimas*

Reikalaujami apsaugos mechanizmai nustatyti 11 priedėlyje.

Visus kitus apsaugos mechanizmus nustato TOE gamintojas.

6. Būtiniausias apsaugos mechanizmų neįveikiamumas

Tachografo kortelės apsaugos mechanizmų neįveikiamumas turi būti ne mažesnis kaip aukštas, kaip apibrėžta ITSEC.

7. Užtikrinimo lygis

Tachografo kortelės užtikrinimo lygis yra lygis E3 pagal ITSEC.

8. Apibūdinimas

Toliau esančiose lentelėse pateiktas SEF apibūdinimas, nurodantis:

- kurios SEF ar priemonės kovoja su pavojais,
- kurios SEF atitinka kuriuos IT apsaugos tikslus.

	Pavojai											IT reikalavimai								
	T.CLON*	T.DIS_ES2	T.T_ES	T.T_CMD	T.MOD_SOFT*	T.MOD_LOAD	T.MOD_EXE	T.MOD_SHARE	Ident_Data [identifikacijos duomenys]	Activity_Data [duomenys apie veiklą]	Data_Exchange [keitimasis duomenimis]	O.TAMPER_ES	O.CLON*	O.OPERATE*	O.FLAW*	O.DJS_MECHANISM2	O.DJS_MEMORY*	O.MOD_MEMORY*	Data_Access [prieiga prie duomenų]	Secured_Communications [apsaugotas ryšys]
UIA_301 Autentiškumo tikrinimo priemonės																			x	
UIA_302 PIN tikrinimas																			x	
ACT_301 Identifikacijos duomenys																				
ACT_302 Suasmeninimo data																				
RLB_301 Programinės įrangos nepažeistumas												x		x						
RLB_302 Savitikra												x		x						
RLB_303 Gamybos bandymai					x	x						x		x						
RLB_304 Programinės įrangos analizė					x		x	x				x		x						
RLB_305 Programinės įrangos įvestis					x	x		x				x		x						
RLB_306 Maitinimas									x	x		x		x						
RLB_307 Perkrovimas												x		x						
DEX_301 Apsaugotų duomenų importas											x									x
DEX_302 Apsaugotų duomenų importas											x									x
DEX_303 Apsaugotų duomenų eksportas į TPB											x									x
DEX_304 Kilmės įrodymas											x									x
DEX_305 Kilmės įrodymas											x									x
DEX_306 Saugus eksportas į išorines laikmenas											x									x
CSP_301 Raktų generavimas												x								x
CSP_302 Raktų platinimas												x								x

11 priedėlis

BENDRIEJI APSAUGOS MECHANIZMAI

TURINYS

1.	Bendroji dalis	516
1.1.	Nuorodos	516
1.2.	Santrumpos ir žymenys	517
2.	Kriptografinės sistemos ir algoritmai	518
2.1.	Kriptografinės sistemos	518
2.2.	Kriptografiniai algoritmai	518
2.2.1.	RSA algoritmas	518
2.2.2.	Maišos algoritmas	518
2.2.3.	Duomenų kodavimo algoritmas	518
3.	Raktai ir pažymėjimai	518
3.1.	Raktų generavimas ir platinimas	518
3.1.1.	RSA raktų generavimas ir platinimas	518
3.1.2.	RSA bandymų raktai	520
3.1.3.	Judesio jutiklio raktai	520
3.1.4.	T-DES panaudos raktų generavimas ir platinimas	520
3.2.	Raktai	520
3.3.	Pažymėjimai	520
3.3.1.	Pažymėjimų turinys	521
3.3.2.	Išduodami pažymėjimai	522
3.3.3.	Pažymėjimo tikrinimas ir išnagrinėjimas	523
4.	Abipusio autentiškumo tikrinimo mechanizmas	523
5.	Duomenų perdavimo tarp tpb ir kortelių konfidencialumo, nepažeistumo ir autentiškumo tikrinimo mechanizmai	526
5.1.	Saugusis keitimasis pranešimais	526
5.2.	Saugiojo keitimosi pranešimais klaidų tvarkymas	527
5.3.	Kriptografinių sumų apskaičiavimo algoritmas	528
5.4.	Kriptogramų konfidencialumo DO skaičiavimo algoritmas	528
6.	Duomenų perkėlimo skaitmeninio parašo mechanizmai	529
6.1.	Parašų generavimas	529
6.2.	Parašo tikrinimas	529

1. BENDROJI DALIS

Šiame priedėlyje nurodyti apsaugos mechanizmai, kurie užtikrina:

- abipusį autentiškumo tikrinimą tarp TPB ir tachografo kortelių, įskaitant sutartį dėl seanso rakto,
- duomenų, kuriais keičiasi TPB ir tachografo kortelės, konfidencialumą, nepažeistumą ir autentiškumą,
- iš TPB į išorines laikmenas perkeliamų duomenų nepažeistumą ir autentiškumą,
- iš tachografo kortelių į išorines laikmenas perkeliamų duomenų nepažeistumą ir autentiškumą.

1.1. Nuorodos

Šiame priedėlyje naudoti tokie šaltiniai:

SHA-1	Nacionalinis standartų ir technologijos institutas (NIST). FIPS leidinys 180-1: Saugios maišos standartas, 1995 m. balandžio mėn.
PKCS1	RSA laboratorijos. PKCS # 1: RSA kodavimo standartas. 2.0 versija, 1998 m. spalio mėn.
TDES	Nacionalinis standartų ir technologijos institutas (NIST). FIPS leidinys 46-3: duomenų kodavimo standartas, 1999 m. projektas.
TDES-OP	ANSI X9.52. Trigubo duomenų kodavimo algoritmo naudojimo režimai, 1998 m.
ISO/IEC 7816-4	Informacinė technologija. Identifikacijos kortelės. Kortelės su integriniais grandynais ir kontaktais. 4 dalis. Tarpusavio keitimosi tarpšakinės komandos. Pirmasis leidimas: 1995 m. + 1 pataisa: 1997 m.
ISO/IEC 7816-6	Informacinė technologija. Identifikacijos kortelės. Kortelės su integriniais grandynais ir kontaktais. 6 dalis. Tarpšakiniai duomenų elementai. Pirmasis leidimas: 1996 m. + 1 pataisa: 1998 m.
ISO/IEC 7816-8	Informacinė technologija. Identifikacijos kortelės. Kortelės su integriniais grandynais ir kontaktais. 8 dalis. Apsauginės tarpšakinės komandos. Pirmasis leidimas: 1999 m.
ISO/IEC 9796-2	Informacinė technologija. Apsaugos metodika. Skaitmeninio parašo sistemos pranešimams atkurti. 2 dalis. Maišos funkcijų naudojantys mechanizmai. Pirmasis leidimas: 1997 m.
ISO/IEC 9798-3	Informacinė technologija. Apsaugos metodika. Objekto autentiškumo tikrinimo mechanizmai. 3 dalis. Objekto autentiškumo tikrinimas naudojant atvirojo rakto algoritmą. Antrasis leidimas: 1998 m.
ISO 16844-3	Kelių transporto priemonės. Tachografų sistemos. 3 dalis. Judesio jutiklio sąsaja.

1.2. Santrumpos ir žymenys

Šiame priedėlyje naudotos tokios santrumpos ir žymenys:

(K_a, K_b, K_c)	raktų rinkinys, skirtas naudoti trigubo duomenų kodavimo algoritme;
CA	sertifikavimo institucija;
CAR	sertifikavimo institucijos žymuo;
CC	kriptografinė kontrolinė suma;
CG	kriptograma;
CH	komandos antraštė;
CHA	pažymėjimo turėtojo įgaliojimas;
CHR	pažymėjimo turėtojo žymuo;
D()	dekodavimas naudojant DES;
DE	duomenų elementas;
DO	duomenų objektas;
d	RSA slaptasis raktas, slaptoji eksponentė;
e	RSA atvirasis raktas, atviroji eksponentė;
E()	kodavimas naudojant DES;
EQT	įranga;
Hash()	maišos vertė, hash išvestis;
Hash	maišos funkcija;
KID	rakto vardas;
Km	TDES raktas. Pagrindinis raktas, apibrėžtas ISO 16844-3;
Km_{vu}	transporto priemonės bloke įdiegtas TDES raktas;
Km_{wc}	dirbtuvių kortelėse įdiegtas TDES raktas;
m	pranešimas, nurodantis sveikąjį skaičių nuo 0 iki $n-1$;
n	RSA raktai, modulis;
PB	išplėtimo baitai;
PI	išplėtimo indikacinis baitas (skirtas naudoti konfidencialumo DO kriptogramoje);
PV	paprastoji vertė
s	parašo simbolis, sveikasis skaičius nuo 0 iki $n-1$;
SSC	siuntimo sekos skaitiklis;
SM	saugusis keitimasis pranešimais;
TCBC	TDEA skaitmenų blokų jungimo režimas;
TDEA	trigubo duomenų kodavimo algoritmas;
TLV	žymenos ilgio vertė;
VU	transporto priemonės blokas
X.C	sertifikavimo institucijos išduotas naudotojo X pažymėjimas;
X.CA	naudotojo X sertifikavimo institucija;
X.CA.PK _o X.C	pažymėjimo išnagrinėjimo operacija atvirajam raktui išskirti. Tai yra intarpinė funkcija, kurios kairysis operandas yra sertifikavimo institucijos atvirasis raktas, o dešinysis operandas – tos sertifikavimo institucijos išduotas pažymėjimas. Rezultatas – naudotojo X, kurio pažymėjimas yra dešinysis operandas, atvirasis raktas;

X.PK	naudotojo X atvirasis raktas;
X.PK[I]	tam tikros informacijos I šifruotė RSA, gauta naudojant naudotojo X atvirąjį raktą;
X.SK	naudotojo X slaptasis RSA raktas;
X.SK[I]	tam tikros informacijos I šifruotė RSA, gauta naudojant naudotojo X atvirąjį raktą;
„xx“	šešioliktainė vertė;
	sąryšio ženklas.

2. KRIPTOGRAFINĖS SISTEMOS IR ALGORITMAI

2.1. Kriptografinės sistemos

CSM_001 Transporto priemonės blokai ir tachografo kortelės turi naudoti klasikinę RSA atvirojo rakto kriptografinę sistemą tokiems apsaugos mechanizms sudaryti:

- autentiškumo tikrinimas tarp transporto priemonės blokų ir kortelių,
- trigubo DES panaudų raktų perdavimas tarp transporto priemonės blokų ir kortelių,
- iš transporto priemonės blokų arba tachografų kortelių į išorines laikmenas perkeliama duomenų skaitmeninis parašas.

CSM_002 Transporto priemonės blokai ir tachografo kortelės turi naudoti trigubo DES simetrinę kriptografinę sudaryti duomenų nepažeistumo apsaugos mechanizms keičiantis duomenimis apie naudotoją tarp transporto priemonės blokų ir tachografo kortelių ir (kai taikytina) sudaryti konfidencialumui keičiantis duomenimis tarp transporto priemonės blokų ir tachografo kortelių.

2.2. Kriptografiniai algoritmai

2.2.1. RSA algoritmas

CSM_003 RSA algoritmą visiškai apibūdina tokios lygtys:

$$\begin{aligned} X.SK[m] &= s = m^d \bmod n \\ X.PK[s] &= m = s^e \bmod n \end{aligned}$$

Išsamesnis RSA funkcijos apibūdinimas pateiktas šaltinyje (PKCS1).

RSA skaičiavimuose naudojama atviroji eksponentė e visuose sugeneruotuose RSA raktuose nėra lygi 2.

2.2.2. Maišos algoritmas

CSM_004 Skaitmeninio parašo mechanizmuose turi būti naudojamas maišos algoritmas SHA-1, nurodytas šaltinyje (SHA-1).

2.2.3. Duomenų kodavimo algoritmas

CSM_005 DES paremti algoritmai turi būti naudojami skaitmenų blokų jungimo režimu.

3. RAKTAI IR PAŽYMĖJIMAI

3.1. Raktų generavimas ir platinimas

3.1.1. RSA raktų generavimas ir platinimas

CSM_006 RSA raktai turi būti kuriami trimis funkcinės hierarchijos lygiais:

- europiniu lygiu,
- valstybės narės lygiu,
- įrangos lygiu.

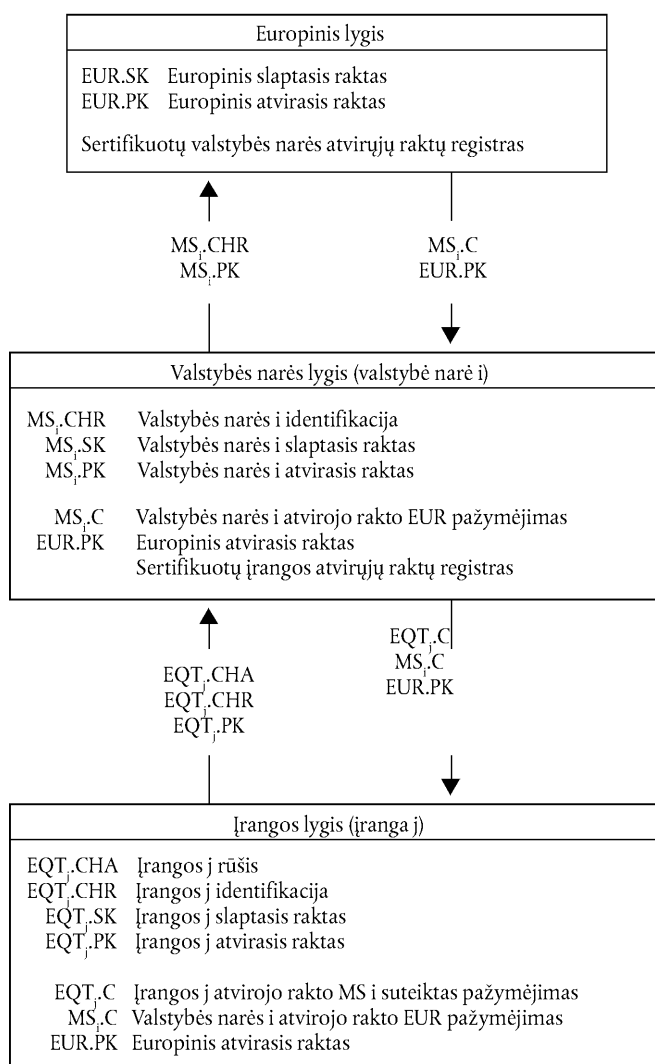
CSM_007 Europiniu lygiu sugeneruojama viena europinių raktų pora (EUR.SK ir EUR.PK). Europinis slaptasis raktas naudojamas valstybių narių atviresiems raktams sertifikuoti. Turi būti laikomi visų sertifikuotų raktų registrai. Tai daro Europos sertifikavimo institucija, prižiūrima už tai atsakančios Europos Komisijos.

CSM_008 Valstybės narės lygiu sugeneruojama valstybės narės raktų pora (MS.SK ir MS.PK). Valstybių narių atviresiems raktus sertifikuoja Europos sertifikavimo institucija. Valstybės narės slaptasis raktas naudojamas sertifikuoti atviresiems raktams, įdiegtiniams į įrangą (transporto priemonės bloką arba tachografo kortelę). Turi būti laikomi visų sertifikuotų atvirųjų raktų registrai, kuriuose nurodyta įrangos, kurioje jie įdiegti, identifikacija. Tai daro valstybės narės sertifikavimo institucija. Valstybė narė gali reguliariai keisti savo raktų porą.

CSM_009 Įrangos lygiu sugeneruojama ir įdiegiama į įrangą viena raktų pora (EQT.SK ir EQT.PK). Įrangos atviresiems raktus sertifikuoja Europos sertifikavimo institucija. Tai gali daryti įrangos gamintojai, suasmenintojai arba valstybės narės institucijos. Ši raktų pora naudojama autentiškumo tikrinimo, skaitmeninio parašo ir šifravimo paslaugoms.

CSM_010 Slaptųjų raktų konfidencialumas turi būti išlaikomas generuojant, perduodant (jei reikia) ir laikant juos.

Toliau esančioje schemoje pavaizduotas šio proceso duomenų srautas:



3.1.2. **RSA bandymų raktai**

CSM_011 Įrangos bandymams (įskaitant funkcinio suderinamumo bandymus) Europos sertifikavimo institucija turi sugeneruoti vieną europinių bandymų raktų porą ir ne mažiau kaip dvi valstybių narių bandymų raktų poras, kurių slaptieji raktai sertifikuojami europiniu slaptuoju bandymų raktu. Į įrangą, kuria atliekami tipo patvirtinimo bandymai, gamintojai turi įdiegti bandymų raktus, sertifikuotus vienu iš šių valstybių narių bandymų raktu.

3.1.3. **Judesio jutiklio raktai**

Toliau aprašytų trijų TDES raktų konfidencialumas turi būti reikiamai išlaikytas generuojant, perduodant (jei reikia) ir laikant juos.

Tam, kad paremtų ISO 16844 atitinkančius tachografus, Europos sertifikavimo institucija ir valstybių narių sertifikavimo institucijos papildomai turi užtikrinti:

CSM_036 Europos sertifikavimo institucija generuoja du nepriklausomus ir unikalius trigubo DES raktus — $K_{m_{VU}}$ ir $K_{m_{WC}}$ ir K_m :

$$K_m = K_{m_{VU}} \text{ XOR } K_{m_{WC}}$$

Šiuos raktus valstybių narių prašymu Europos sertifikavimo institucija atitinkamos apsaugos tvarka perduoda tų šalių sertifikavimo institucijoms.

CSM_037 Valstybių narių sertifikavimo institucijos:

- naudoja K_m judesio jutiklio gamintojų pareikalautiems duomenims apie judesio jutiklį užkoduoti (K_m koduojami duomenys apibrėžti ISO 16844-3),
- atitinkamos apsaugos tvarka perduoda $K_{m_{VU}}$ transporto priemonės blokų gamintojams įdiegti į transporto priemonės blokus,
- užtikrina, kad suasmeninant korteles $K_{m_{WC}}$ būtų įdiegtas į visas dirbtuvių korteles (*SensorInstallationSecData* elementariojoje rinkmenoje *Sensor_Installation_Data*).

3.1.4. **T-DES panaudos raktų generavimas ir platinimas**

CSM_012 Transporto priemonės blokai ir tachografo kortelės abipusio autentiškumo tikrinimo proceso metu turi generuoti ir keisti būtinais duomenimis bendrajam trigubo DES panaudos raktui detalizuoti. Šio keitimosi duomenimis konfidencialumas turi būti apsaugotas RSA šifravimo mechanizmu.

CSM_013 Šis raktas turi būti naudojamas visose tolesnėse kriptografinėse operacijose naudojant saugųjį keitimąsi pranešimais. Jo galiojimas turi baigtis pasibaigus panaudai (ištraukus kortelę arba perkrovus ją) ir (arba) po 240 panaudojimų (vienas rakto panaudojimas = viena saugiojo keitimosi pranešimais būdu į kortelę nusiųsta komanda ir atsakymas į ją).

3.2. **Raktai**

CSM_014 RSA raktų (bet kurio lygio) ilgis yra toks: modulis n — 1024 bitai, atviroji eksponentė e — ne daugiau kaip 64 bitai, slaptoji eksponentė d — 1024 bitai.

CSM_015 Trigubo DES raktai turi būti formos (K_a, K_b, K_d) , ahol K_a ir K_b yra nepriklausomi 64 bitų ilgio raktai. Lyginumo klaidos aptikimo bitai nenustatomi.

3.3. **Pažymėjimai**

CSM_016 RSA atvirųjų raktų pažymėjimai turi būti „ne save apibūdinantieji“ „kortele patikrintini“ pažymėjimai (ISO/IEC 7816-8).

3.3.1. **Pažymėjimų turinys**

CSM_017 RSA atvirųjų raktų pažymėjimus sudaro tokie duomenys, išdėstyti nurodyta tvarka:

Duomenys	Formatas	Baitai	Obs
CPI	INTEGER	1	Pažymėjimo profilio vardas (šios versijos — „01“)
CAR	OCTET STRING	8	Sertifikavimo institucijos žymuo
CHA	OCTET STRING	7	Pažymėjimo turėtojo autentiškumo patvirtinimas
EOV	TimeReal	4	Pažymėjimo galiojimo pabaiga. Neprivaloma, jei nenaudojama, užpildoma „FF“.
CHR	OCTET STRING	8	Pažymėjimo turėtojo žymuo
<i>n</i>	OCTET STRING	128	Atvirasis raktas (modulis)
<i>e</i>	OCTET STRING	8	Atvirasis raktas (atviroji eksponentė)
		164	

Pastabos:

1. Pažymėjimo profilio vardas (CPI) apibrėžia tikslią autentiškumo patvirtinimo pažymėjimo struktūrą. Jį galima naudoti kaip įrangos atitinkamų antraščių sąrašo vidinį vardą, apibūdinantį duomenų elementų sąryšį pažymėjime.

Su pažymėjimo turiniu susijęs antraščių sąrašas yra toks:

'4D'	'16'	'5F 29'	'01'	'42'	'08'	'5F 4B'	'07'	'5F 24'	'04'	'5F 20'	'08'	'7F 49'	'05'	'81'	'81 80'	'82'	'08'
Išplėsto antraščių sąrašo žymena	Antraščių sąrašo ilgis	CPI žymena	CPI ilgis	CAR žymena	CAR ilgis	CHA žymena	CHA ilgis	EOV žymena	EOV ilgis	CHR žymena	CHR ilgis	Atvirojo rakto žymena (sudaryta)	Paskesnių DO ilgis	modulio žymena	modulio ilgis	atvirojos eksponentės žymena	atvirojos eksponentės ilgis

2. „Sertifikavimo institucijos žymuo“ (CAR) identifikuoja pažymėjimą išduodančią CA taip, kad duomenų elementą galima naudoti kartu su institucijos rakto vardu sertifikavimo institucijos atvirajam raktui nurodyti (apie kodavimą žr. punkte „rakto vardas“).
3. „Pažymėjimo turėtojo autentiškumo patvirtinimas“ (CHA) naudojamas pažymėjimo turėtojo teisėms identifikuoti. Jį sudaro tachografo programos įrangos rūšies, kuriai pažymėjimas skirtas, identifikacija (pagal duomenų elementą **EquipmentType**; valstybės narės — „00“).
4. „Pažymėjimo turėtojo žymuo“ (CHR) skirtas vienam pažymėjimo turėtojui identifikuoti taip, kad duomenų elementą galima naudoti kartu su subjekto rakto vardu pažymėjimo turėtojo atvirajam raktui nurodyti.
5. Raktų vardai identifikuoja atskirą pažymėjimo turėtoją arba sertifikavimo instituciją. Jie koduojami taip:

5.1. Įranga (TPB arba kortelė):

Duomenys	Įrangos serijos numeris	Data	Rūšis	Gamintojas
Ilgis	4 baitai	2 baitai	1 baitas	1 baitas
Vertė	Sveikasis skaičius	mm yy BCD kodu	Nustato gamintojas	Gamintojo kodas

Kalbant apie TPB, prašydamas pažymėjimų gamintojas gali žinoti įrangos, į kurią raktai bus įdiegti, identifikaciją arba jos nežinoti.

Pirmuoju atveju gamintojas siunčia įrangos identifikaciją su atviruoju raktu savo valstybės narės institucijai sertifikuoti. Tuomet pažymėjime bus įrangos identifikacija, o gamintojas privalo užtikrinti, kad raktai ir pažymėjimas būtų įdiegti į jiems skirtą įrangą. Rakto vardo forma yra tokia, kaip nurodyta pirmiau.

Antruoju atveju gamintojas turi priskirti unikalią identifikaciją kiekvienam pažymėjimo prašymui ir nusiųsti tą identifikaciją su atviruoju raktu savo valstybės narės institucijai sertifikuoti. Pažymėjime bus nurodyta prašyme nurodyta identifikacija. Įdiegęs raktą į rangą, gamintojas turi pranešti valstybės narės institucijai apie rakto priskyrimą įrangai (t. y. pažymėjimo prašymo identifikacija, įrangos identifikacija). Rakto vardas yra tokios formos:

Duomenys	Pažymėjimo prašymo serijos numeris	Data	Rūšis	Gamintojas
Ilgis	4 baitai	2 baitai	1 baitas	1 baitas
Vertė	BCD kodas	mm yy BCD kodu	!!!!	Gamintojo kodas

5.2. Sertifikavimo institucija:

Duomenys	Institucijos identifikacija	Rakto serijos numeris	Papildoma informacija	Vardas
Ilgis	4 baitai	1 baitas	2 baitai	1 baitas
Vertė	1 baito šalies skaitmeninis kodas 3 baitų šalies raidinis kodas	Sveikasis skaičius	papildomas kodas (pagal CA) jei nenaudojama – !!!! FF FF !!!	'01'

Rakto serijos numeris naudojamas skirtingiems valstybės narės raktams atskirti, jei raktas būtų pakeistas.

- Pažymėjimų tikrintojai turi besąlygiškai žinoti, kad sertifikuotas atvirasis raktas yra RSA raktas yra tiesiogiai susijęs su autentiškumo tikrinimu, skaitmeninio parašo tikrinimu ir užšifravimo konfidencialumo paslaugoms (pažymėjime nėra tai nurodančių objektų vardų).

3.3.2. Išduodami pažymėjimai

CSM_018 Išduodamas pažymėjimas yra skaitmeninis parašas su iš dalies atkartotu pažymėjimo turiniu pagal ISO/IEC 9796-2 ir su pridėtu „sertifikavimo institucijos žymeniu“.

$$X.C = X.CA.SK['6A' || C_r || Hash(Cc) || 'BC'] || C_n || X.CAR$$

Pažymėjimo turinys toks: $= Cc = \begin{matrix} C_r \\ 106 \text{ baitai} \end{matrix} || \begin{matrix} C_n \\ 58 \text{ baitai} \end{matrix}$

Pastabos:

- Šis pažymėjimas yra 194 baitų ilgio.
- CAR, kurį slepia parašas, taip pat pridedamas prie parašo, kad sertifikavimo institucijos atvirąjį raktą galima būtų pasirinkti pažymėjimui patikrinti.
- Pažymėjimo tikrintojas turi besąlygiškai žinoti algoritmą, kurį sertifikavimo institucija naudojo pažymėjimui pasirašyti.

4. Su išduotu pažymėjimu susijęs antraščių sąrašas yra toks:

'7F 21'	'09'	'5F 37'	'81 80'	'5F 38'	'3A'	'42'	'08'
CV pažymėjimo žymena (sudaryta)	Paskesnių DO ilgis	Parašo žymena	Parašo ilgis	Likusios dalies žymena	Likusios dalies ilgis	CAR žymena	CAR ilgis

3.3.3. Pažymėjimo tikrinimas ir išnagrinėjimas

Pažymėjimo tikrinimas ir išnagrinėjimas susideda iš parašo tikrinimo pagal ISO/IEC 9796-2, pažymėjimo turinio ir įdiegto atvirojo rakto išrinkimo: $X.PK = X.CA.PK_o.X.C$ ir pažymėjimo galiojimo tikrinimo.

CSM_019 Procesą sudaro tokie žingsniai:

parašo tikrinimas ir turinio išrinkimas:

- iš $X.C$ išrenkamas Ženklas, C_n' ir CAR' :
- iš CAR' pasirenkamas atitinkamas sertifikavimo institucijos atvirasis raktas (jei tai nepadaryta anksčiau kitais būdais),
- Ženklas atidaromas CA atviruoju raktu: $Sr' = X.CA.PK$ [Ženklas],
- patikrinama, ar Sr' prasideda '6A', o baigiasi 'BC',
- apskaičiuojami Cr' ir H' :
- atkuriamas pažymėjimo turinys $C' = C_r' || C_n'$,
- patikrinamas $Hash(C') = H'$.

Jei patikrinimų rezultatai tinkami, pažymėjimas yra nesuklastotas, jo turinys yra C' .

Patikrinamas galiojimas. Pagal C' :

- jei taikytina, patikrinama galiojimo pabaigos data.

Iš C' išrenkamas ir įrašomas atvirasis raktas, rakto vardas, pažymėjimo turėtojo autentiškumo patvirtinimas ir pažymėjimo galiojimo pabaigos data:

- $X.PK = n || e$,
- $X.KID = CHR$,
- $X.CHA = CHA$,
- $X.EOV = EOV$.

4. ABIPUSIO AUTENTIŠKUMO TIKRINIMO MECHANIZMAS

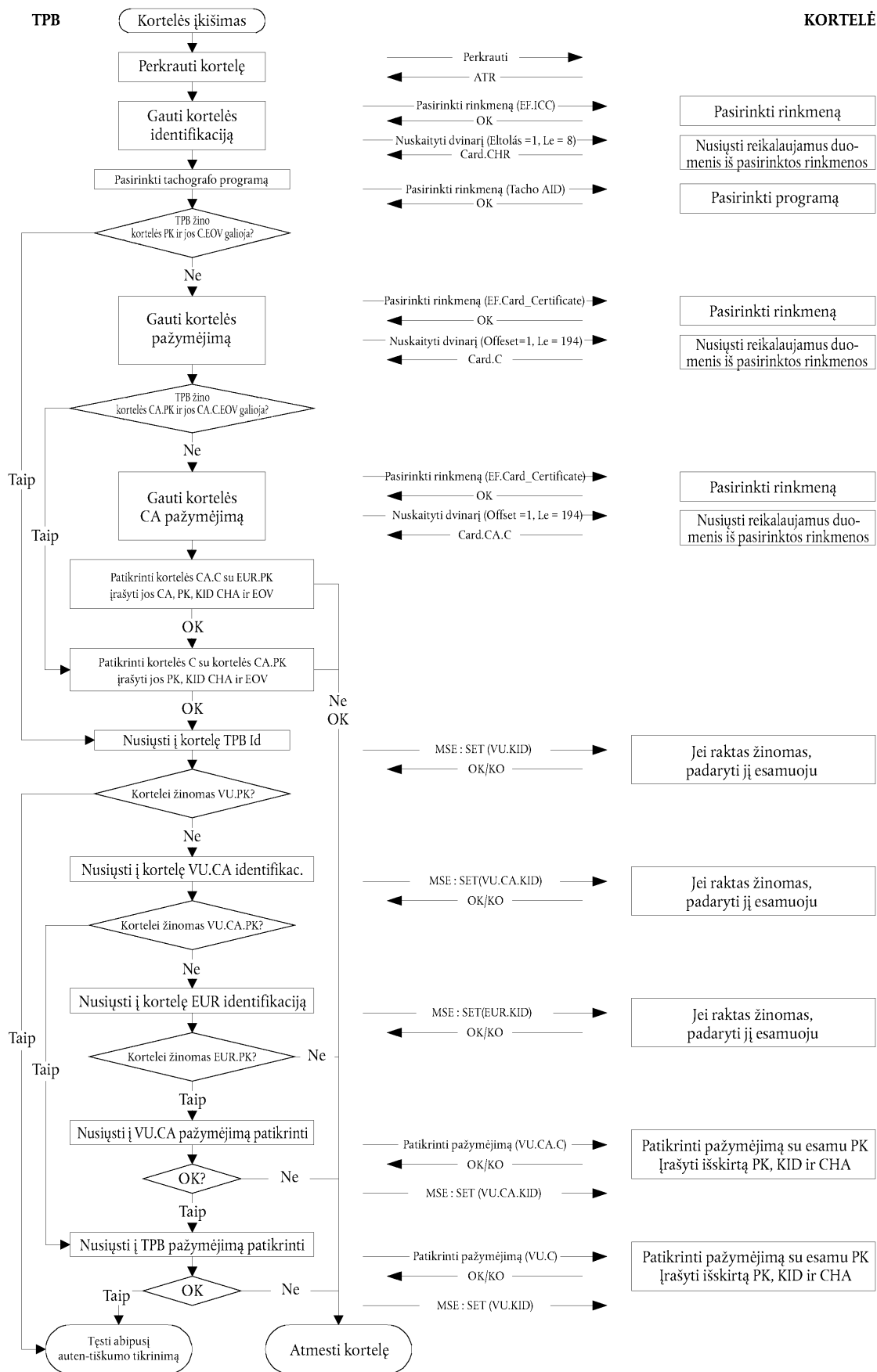
Abipusis autentiškumo tikrinimas tarp tachografo kortelių ir TPB remiasi tokiu principu:

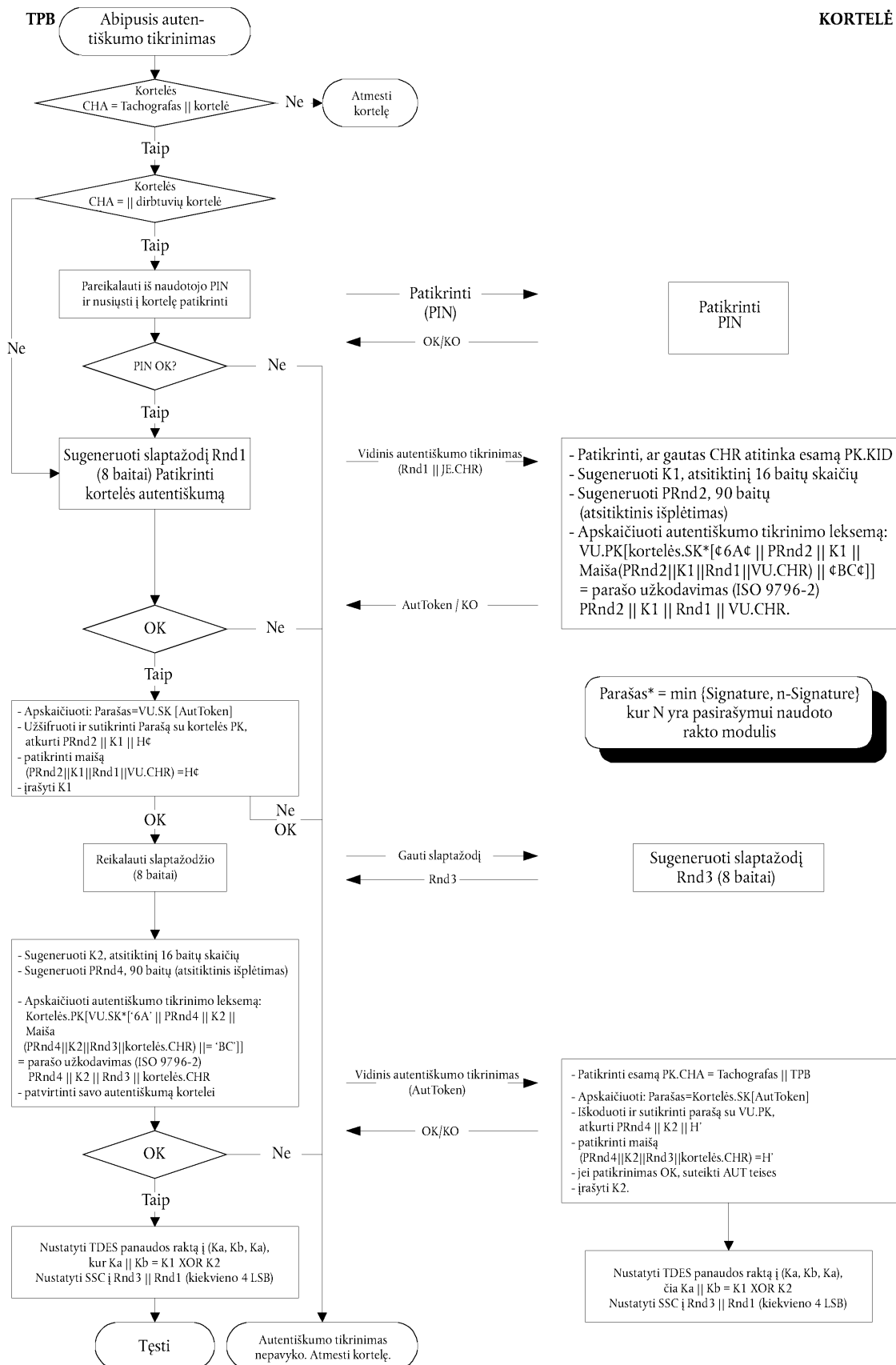
Kiekvienas subjektas turi įrodyti kitam, kad jis turi galiojančių raktų porą, kurios atvirasis raktas yra sertifikuotas valstybės narės sertifikavimo institucijos, kurią savo ruožtu sertifikavo Europos sertifikavimo institucija.

Įrodoma slaptauoju raktu pasirašant kito subjekto atsiųstą atsitiktinį skaičių, kuris turi atkurti tą skaičių tikrindamas parašą.

Mechanizmą TPB aktyvuoja įkišus kortelę. Jis prasideda pažymėjimų pasikeitimu ir atvirųjų raktų išrinkimu, o baigiasi — panaudos rakto nustatymu.

CSM_020 Turi būti naudojamas toliau pavaizduotas protokolas (rodyklėmis pavaizduotos komandos ir duomenys, kuriais keičiamasi (žr. 2 priedėlį)):





5. DUOMENŲ PERDAVIMO TARP TPB IR KORTELIŲ KONFIDENCIALUMO, NEPAŽEISTUMO IR AUTENTIŠKUMO TIKRINIMO MECHANIZMAI

5.1. Saugusis keitimasis pranešimais

- CSM_021 Duomenų perdavimo tarp TPB ir kortelių nepažeistumas turi būti apsaugotas saugiojo keitimosi pranešimais būdu, kaip nurodyta ISO/IEC 7816-4 ir ISO/IEC 7816-8.
- CSM_022 Kai siunčiant duomenis jų apsaugoti nereikia, prie duomenų objektų, siunčiamų su komanda arba atsakymu, pridedama kriptografinė kontrolinė suma. Gavėjas turi patikrinti kriptografinę kontrolinę sumą.
- CSM_023 Su komanda siunčiamų duomenų kriptografinė kontrolinė suma turi sujungti komandos antraštę ir visus siunčiamus duomenų objektus ($\Rightarrow$ CLA = '0C', o visi duomenų objektai turi būti su žymenomis, kurių $b_1 = 1$).
- CSM_024 Atsakymo būsenos ir informacijos baitai turi būti apsaugoti kriptografinė kontrolinė suma, kai atsakyme nėra duomenų laukelio.
- CSM_025 Kriptografinės kontrolinės sumos turi būti keturių baitų ilgio.

Naudojant saugųjį keitimąsi pranešimais komandų ir atsakymų struktūra yra tokia:

Naudojami DO yra ISO/IEC 7816-4 aprašytų saugiojo keitimosi pranešimais DO dalinė imtis:

Žymena	Mnemoninis žymuo	Reikšmė
'81'	T_{PV}	Paprastoji vertė, BER-TLV neužkoduoti duomenys (turi būti apsaugota CC)
'97'	T_{LE}	Le vertė neapsaugotoje komandoje (turi būti apsaugota CC)
'99'	T_{SW}	Informacija apie būseną (turi būti apsaugota CC)
'8E'	T_{CC}	Kriptografinė kontrolinė suma
'87'	$T_{PI\ CG}$	Išplėtimo indikatorinis baitas Kriptograma (Paprastoji vertė, neužkoduota BER-TLV)

Jei neapsaugota atsakymo į komandą pora yra tokia:

Komandos antraštė	Komandos pagrindinė dalis
CLA INS P1 P2	(L_c -laukelis) (Duomenų laukelis) (L_e -laukelis)
keturi baitai	L baitai, pažymėti nuo B_1 iki B_L

Atsakymo pagrindinė dalis	Atsakymo papildymas
(duomenų laukelis)	SW1 SW2
L_r duomenų baitai	du baitai

Atitinkama apsaugota atsakymo į komandą pora yra tokia:

Apsaugota komanda:

Komandos antraštė				Komandos pagrindinė dalis											
CLA	INS	P1	P2	(Naujas L _c laukelis)	(Naujas duomenų laukelis)						(Naujas L _e laukelis)				
'OC'				Naujo duomenų laukelio ilgis	T _{PV}	L _{PV}	PV	T _{LE}	L _{LE}	L _e	T _{CC}	L _{CC}	CC	'00'	
					'81'	L _c	Duo- menų lauke- lis	'97'	'01'	L _e	'8E'	'04'	CC		

I kontrolinę sumą integruojami duomenys = CH || PB || T_{PV} || L_{PV} || PV || T_{LE} || L_{LE} || L_e || PB

PB = išplėtimo baitai (80 .. 00) pagal ISO/IEC 7816-4 ir ISO 9797 1 metodą.

DO PV ir LE yra tik tuomet, kai neapsaugotoje komandoje yra atitinkančių duomenų.

Apsaugotas atsakymas:

1. Atvejis, kai atsakymo duomenų laukelis netuščias ir jo konfidencialumo apsaugoti nereikia:

Atsakymo pagrindinė dalis						Atsakymo papildymas
(Naujas duomenų laukelis)						Nauji SW 1 SW2
T _{PV}	L _{PV}	PV	T _{CC}	L _{CC}	CC	
'81'	L _r	Duomenų laukelis	'8E'	'04'	CC	

I kontrolinę sumą integruojami duomenys = T T_{PV} || L_{PV} || PV || PB

2. Atvejis, kai atsakymo duomenų laukelis netuščias ir jo konfidencialumą reikia apsaugoti:

Atsakymo pagrindinė dalis						Atsakymo papildymas
(Naujas duomenų laukelis)						Nauji SW 1 SW2
T _{PI CG}	L _{PI CG}	PI CG	T _{CC}	L _{CC}	CC	
'87'		PI CG	'8E'	'04'	CC	

Duomenys, kuriuos turi perduoti CG: BER-TLV neužkoduoti duomenys ir išplėtimo baitai.

I kontrolinę sumą integruojami duomenys = T_{PI CG} || L_{PI CG} || PI CG || PB

3. Atvejis, kai atsakymo duomenų laukelis tuščias:

Atsakymo pagrindinė dalis						Atsakymo papildymas
(Naujas duomenų laukelis)						Nauji SW 1 SW2
T _{SW}	L _{SW}	SW	T _{CC}	L _{CC}	CC	
'99'	'02'	nauji SW 1 SW2	'8E'	'04'	CC	

I kontrolinę sumą integruojami duomenys = TSW || LSW || SW || PB.

5.2. Saugiojo keitimosi pranešimais klaidų tvarkymas

CSM_026 Kai tachografo kortelė interpretuodama komandą atpažįsta SM klaidą, tuomet nenaudojant SM turi būti grąžinti būsenos baitai. Pagal ISO/IEC 7816-4 apibrėžti tokie SM klaidas nurodantys būsenos baitai:

'66 88' kriptografinės kontrolinės sumos patikrinimas nepavyko,

'69 87' nėra lauktų SM duomenų objektų,

'69 88' SM duomenų objektai neteisingi.

CSM_027 Kai tachografo kortelė grąžina būsenos baitus be SM DO arba su klaidingais SM DO, TPB turi nutraukti panaudos seansą.

5.3. Kriptografinių sumų apskaičiavimo algoritmas

CSM_028 Kriptografinės sumos sudaromos naudojant mažmeninį MAC pagal ANSI X9.19 pagal DES:

- pradinis etapas: pradinis kontrolinis blokas y_0 yra $E(K_a, SSC)$,
- paskesnis etapas: naudojant K_a apskaičiuojami kontroliniai blokai $y_1, \dots, y_n$,
- galutinis etapas: pagal paskutinį kontrolinį bloką y_n apskaičiuojama kontrolinė suma: $E(K_a, D(K_b, y_n))$.

Čia $E()$ reiškia užkodavimą pagal DES, o $D()$ reiškia iškodavimą pagal DES.

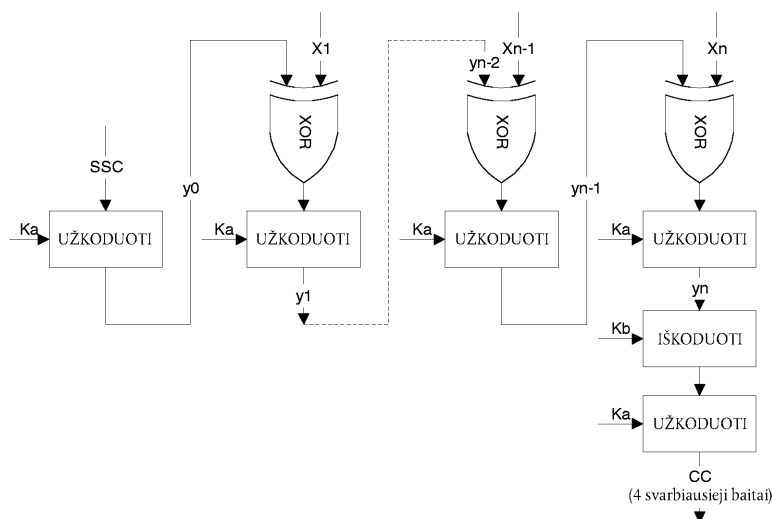
Perduodami keturi svarbiausieji kriptografinės kontrolinės sumos baitai.

CSM_029 Siuntimo sekos skaitiklis (SSC) turi būti aktyvuotas per rakto sutarties procedūrą:

Pradinis SSC: Rnd3 (4 mažiausiai svarbūs baitai) || Rnd1 (4 mažiausiai svarbūs baitai).

CSM_030 Siuntimo sekos skaitiklis turi būti padidintas vienetu prieš apskaičiuojant MAC (t. y. pirmosios komandos SSC yra pradinis SSC + 1, pirmojo atsakymo SSC — pradinis SSC + 2).

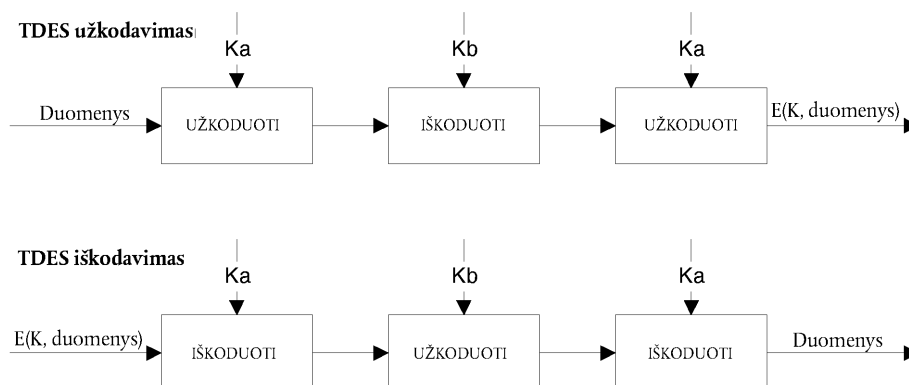
Toliau pateikiamame paveikslėlyje pavaizduota mažmeninio MAC skaičiavimo schema:



5.4. Kriptogramų konfidencialumo DO skaičiavimo algoritmas

CSM_031 Kriptogramas skaičiuojamas darbo režimu TCBC naudojant TDEA, kaip nurodyta TDES ir TDES-OP, o pradinės vertės bloku — nulinių vektorių.

Toliau pateikiamame paveikslėlyje pavaizduota raktų naudojimo TDES schema:



6. DUOMENŲ PERKĖLIMO SKAITMENINIO PARAŠO MECHANIZMAI

CSM_032 Specializuota įranga su mikroprocesoriumi (IDE) įrašo vieno duomenų perkėlimo seanso metu iš įrangos (TPB arba kortelės) gautus duomenis į vieną fizinę rinkmeną. Ši rinkmena turi turėti pažymėjimus MSi.C ir EQT.C. Rinkmenoje yra skaitmeniniai duomenų blokų parašai, kaip nurodyta 7 priedėlyje „Duomenų perkėlimo protokolai“.

CSM_033 Perkeltų duomenų skaitmeniniai parašai turi būti tokios skaitmeninio parašo struktūros su papildymu, kad, jei reikia, perkeltus duomenis galima būtų perskaityti nešifruojant.

6.1. Parašų generavimas

CSM_034 Duomenų parašus įranga turi generuoti pagal parašų su papildymu sistemą, kaip apibrėžta PKCS1, su SHA-1 maišos funkcija:

$$\text{Parašas} = \text{EQT.SK}[\text{'00'} \parallel \text{'01'} \parallel \text{PS} \parallel \text{'00'} \parallel \text{DER}(\text{SHA-1}(\text{Duomenys}))]$$

PS 'FF' išplėtimo oktetų eilutė, kad ilgis sudarytų 128.

DER(SHA-1(M)) yra algoritmo ID užkodavimas maišos funkcijai ir maišos vertės užkodavimas DigestInfo rūšies ASN.1 verte (išskirtinės kodavimo taisyklės):

'30' || '21' || '30' || '09' || '06' || '05' || '2B' || '0E' || '03' || '02' || '1A' || '05' || '00' || '04' || '14' || maišos vertė.

6.2. Parašo tikrinimas

CSM_035 Perkeltų duomenų parašo tikrinimas turi vykti pagal parašų su papildymu sistemą, kaip apibrėžta PKCS1, su SHA-1 maišos funkcija.

Tikrintojas turi pats žinoti europinį atvirąjį raktą EUR.PK (ir pasitikėti).

Toliau esančioje schemoje pavaizduotas protokolai, kurį IDE su kontrolės kortele gali naudoti į ESM (išorines laikmenas) perkeltų ir įrašytų duomenų nepažeistumui tikrinti. Kontrolės kortelė naudojama skaitmeniniam parašams iššifruoti. Tokiu atveju ši funkcija gali būti neįdiegta IDE.

Duomenis persikėlus ir pasirašiusi įranga pažymima EQT.

